TITLE 6—DOMESTIC SECURITY

Chap.		Sec.
1.	**Homeland Security Organization**	**101**
2.	**National Emergency Management**	**701**
3.	**Security and Accountability for Every Port**	**901**
4.	**Transportation Security**	**1101**
5.	**Border Infrastructure and Technology Modernization**	**1401**
6.	**Cybersecurity**	**1500**

EDITORIAL NOTES

PRIOR PROVISIONS

A prior Title 6, Surety Bonds, was enacted by act July 30, 1947, ch. 390, §1, 61 Stat. 646, and was repealed by act Sept. 13, 1982, Pub. L. 97–258, §5(b), 96 Stat. 1068, 1085.

Sections 1 to 5 were repealed by Pub. L. 92–310, title II, §203(1), June 6, 1972, 86 Stat. 202.

Section 1, acts July 30, 1947, ch. 390, 61 Stat. 646; Oct. 31, 1951, ch. 655, §13, 65 Stat. 715, related to custody of official bonds.

Section 2, act July 30, 1947, ch. 390, 61 Stat. 647, directed examination at least once every two years of sufficiency of sureties on official bonds.

Section 3, acts July 30, 1947, ch. 390, 61 Stat. 647; Sept. 3, 1954, ch. 1263, §15, 68 Stat. 1231, related to renewal of bonds and continuance of liability.

Section 4, act July 30, 1947, ch. 390, 61 Stat. 647, related to notice of delinquency of principal. The provisions of the section were reenacted by section 260 of Pub. L. 92–310, which was classified to section 497a of former Title 31. See section 3532 of Title 31, Money and Finance.

Section 5, act July 30, 1947, ch. 390, 61 Stat. 648, related to limitation of actions against sureties.

Sections 6 to 13 were repealed by Pub. L. 97–258, §5(b), Sept. 13, 1982, 96 Stat. 1068, 1085.

Section 6, acts July 30, 1947, ch. 390, 61 Stat. 648; Aug. 9, 1955, ch. 683, §2, 69 Stat. 620; June 6, 1972, Pub. L. 92–310, title II, §203(2), 86 Stat. 202, related to surety companies as sureties. See section 9304 of Title 31, Money and Finance.

Section 7, act July 30, 1947, ch. 390, 61 Stat. 648, related to appointment of agents and service of process with regards to surety companies as sureties. See section 9306 of Title 31.

Section 8, act July 30, 1947, ch. 390, 61 Stat. 649, related to deposit of copy of charter of surety company before transacting business under sections 6 to 13 of this title. See section 9305 of Title 31.

Section 9, act July 30, 1947, ch. 390, 61 Stat. 649, related to quarterly statements of surety companies filed with Secretary of the Treasury. See section 9305 of Title 31.

Section 10, act July 30, 1947, ch. 390, 61 Stat. 649, related to jurisdiction over surety companies with regards to suits on bonds. See section 9307 of Title 31.

Section 11, act July 30, 1947, ch. 390, 61 Stat. 649, provided sanctions for nonpayment of a judgment by surety company. See section 9305 of Title 31.

Section 12, act July 30, 1947, ch. 390, 61 Stat. 649, estopped a surety company to deny its corporate powers, etc. See section 9307 of Title 31.

Section 13, act July 30, 1947, ch. 390, 61 Stat. 650, provided for fining of surety companies for their failure to comply with law. See section 9308 of Title 31.

Section 14, acts July 30, 1947, ch. 390, 61 Stat. 650; Aug. 9, 1955, ch. 683, §1, 69 Stat. 618, which related to purchase of bonds to cover officers and employees of Federal Government, was repealed by Pub. L. 92–310, title II, §203(1), June 6, 1972, 86 Stat. 202.

Section 15, act July 30, 1947, ch. 390, 61 Stat. 650, which related to bonds and notes of United States in lieu of recognizance, stipulation, bond, guarantee, or undertaking and contractors' bonds, was repealed by Pub. L. 97–258, §5(b), Sept. 13, 1982, 96 Stat. 1068, 1085. See sections 9301 and 9303 of Title 31, Money and Finance.

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

Sec.

101. Definitions.

102. Construction; severability.
103. Use of appropriated funds.
103a. Department of Homeland Security Nonrecurring Expenses Fund.
104. National biodefense strategy.
105. Biodefense analysis and budget submission.
106. Update of national biodefense implementation plan.

SUBCHAPTER I—DEPARTMENT OF HOMELAND SECURITY

111. Executive department; mission.
112. Secretary; functions.
113. Other officers.
114. Sensitive Security Information.
115. Trade and customs revenue functions of the Department.

SUBCHAPTER II—INFORMATION ANALYSIS

PART A—INFORMATION AND ANALYSIS; ACCESS TO INFORMATION

121. Information and Analysis.
121a. Homeland Security Intelligence Program.
122. Access to information.
123. Terrorist travel program.
124. Homeland Security Advisory System.
124a. Homeland security information sharing.
124b. Comprehensive information technology network architecture.
124c. Coordination with information sharing environment.
124d. Intelligence components.
124e. Training for employees of intelligence components.
124f. Intelligence training development for State and local government officials.
124g. Information sharing incentives.
124h. Department of Homeland Security State, Local, and Regional Fusion Center Initiative.
124h–1. Threat information sharing.
124i. Homeland Security Information Sharing Fellows Program.
124j. Rural Policing Institute.
124k. Interagency Threat Assessment and Coordination Group.
124*l*. Transferred.
124m. Classified Information Advisory Officer.
124m–1. Departmental coordination on counter threats.
124n. Protection of certain facilities and assets from unmanned aircraft.
124n–1. Penalties.
125. Annual report on intelligence activities of the Department of Homeland Security.
126. Department of Homeland Security data framework.

PART B—INFORMATION SECURITY

131 to 134. Transferred.
141. Procedures for sharing information.
142. Privacy officer.
143 to 145. Transferred.
146. Cybersecurity workforce assessment and strategy.
147 to 151. Transferred.

PART C—OFFICE OF SCIENCE AND TECHNOLOGY

161. Establishment of Office; Director.
162. Mission of Office; duties.
163. Definition of law enforcement technology.
164. Abolishment of Office of Science and Technology of National Institute of Justice; transfer of functions.

165. National Law Enforcement and Corrections Technology Centers.

SUBCHAPTER III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

181. Under Secretary for Science and Technology.
182. Responsibilities and authorities of the Under Secretary for Science and Technology.
183. Functions transferred.
184. Conduct of certain public health-related activities.
185. Federally funded research and development centers.
186. Miscellaneous provisions.
187. Homeland Security Advanced Research Projects Agency.
188. Conduct of research, development, demonstration, testing and evaluation.
189. Utilization of Department of Energy national laboratories and sites in support of homeland security activities.
190. Transfer of Plum Island Animal Disease Center, Department of Agriculture.
191. Homeland Security Science and Technology Advisory Committee.
192. Homeland Security Institute.
193. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security.
194. Enhancement of public safety communications interoperability.
195. Office for Interoperability and Compatibility.
195a. Emergency communications interoperability research and development.
195b. National Biosurveillance Integration Center.
195c. Promoting antiterrorism through international cooperation program.
195d. Social media working group.
195e. Transparency in research and development.
195f. EMP and GMD mitigation research and development and threat assessment, response, and recovery.
195g. Countering Unmanned Aircraft Systems Coordinator.
195h. National Urban Security Technology Laboratory.
195i. Chemical Security Analysis Center.

SUBCHAPTER IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

PART A—BORDER, MARITIME, AND TRANSPORTATION SECURITY RESPONSIBILITIES AND FUNCTIONS

201. Repealed.
202. Border, maritime, and transportation responsibilities.
203. Functions transferred.
204. Surface Transportation Security Advisory Committee.
205. Ombudsman for immigration detention.

PART B—U.S. CUSTOMS AND BORDER PROTECTION

211. Establishment of U.S. Customs and Border Protection; Commissioner, Deputy Commissioner, and operational offices.
212. Retention of Customs revenue functions by Secretary of the Treasury.
213. Preservation of Customs funds.
214. Separate budget request for Customs.
215. Definition.
216. Protection against potential synthetic opioid exposure.
217. Allocation of resources by the Secretary.
218. Asia-Pacific Economic Cooperation Business Travel Cards.
220. Methamphetamine and methamphetamine precursor chemicals.
221. Requirements with respect to administering polygraph examinations to law enforcement personnel of U.S. Customs and Border Protection.
222. Advanced Training Center Revolving Fund.

223. Border security metrics.
224. Other reporting requirements.
225. Reports, evaluations, and research regarding drug interdiction at and between ports of entry.
226. Ensuring timely updates to U.S. Customs and Border Protection field manuals.

PART C—MISCELLANEOUS PROVISIONS

231. Transfer of certain agricultural inspection functions of the Department of Agriculture.
232. Functions of Administrator of General Services.
233. Functions of Transportation Security Administration.
234. Preservation of Transportation Security Administration as a distinct entity.
235. Coordination of information and information technology.
236. Visa issuance.
237. Information on visa denials required to be entered into electronic data system.
238. Office for Domestic Preparedness.
239. Office of Cargo Security Policy.
240. Border Enforcement Security Task Force.
241. Prevention of international child abduction.
242. Department of Homeland Security Blue Campaign.
242a. Department of Homeland Security Center for Countering Human Trafficking.
242b. Reports.
243. Maritime operations coordination plan.
244. Maritime security capabilities assessments.
245. Operational data sharing capability.

PART D—IMMIGRATION ENFORCEMENT FUNCTIONS

251. Transfer of functions.
252. U.S. Immigration and Customs Enforcement.
253. Professional responsibility and quality review.
254. Employee discipline.
255. Report on improving enforcement functions.
256. Sense of Congress regarding construction of fencing near San Diego, California.
257. Report.
258. Homeland Security Investigations Victims Assistance Program.

PART E—CITIZENSHIP AND IMMIGRATION SERVICES

271. Establishment of Bureau of Citizenship and Immigration Services.
272. Citizenship and Immigration Services Ombudsman.
273. Professional responsibility and quality review.
274. Employee discipline.
275. Transition.
276. Report on improving immigration services.
277. Report on responding to fluctuating needs.
278. Application of Internet-based technologies.
279. Children's affairs.

PART F—GENERAL IMMIGRATION PROVISIONS

291. Abolishment of INS.
292. Voluntary separation incentive payments.
293. Authority to conduct a demonstration project relating to disciplinary action.
294. Sense of Congress.
295. Director of Shared Services.
296. Separation of funding.
297. Reports and implementation plans.
298. Immigration functions.

PART G—U.S. CUSTOMS AND BORDER PROTECTION PUBLIC PRIVATE PARTNERSHIPS

301. Fee agreements for certain services at ports of entry.

301a. Port of entry donation authority.
301b. Current and proposed agreements.
301c. Definitions.

SUBCHAPTER V—NATIONAL EMERGENCY MANAGEMENT

311. Definitions.
312. Definition.
313. Federal Emergency Management Agency.
314. Authority and responsibilities.
314a. FEMA programs.
315. Functions transferred.
316. Preserving the Federal Emergency Management Agency.
317. Regional offices.
318. National Advisory Council.
319. National Integration Center.
320. Credentialing and typing.
321. The National Infrastructure Simulation and Analysis Center.
321a. Evacuation plans and exercises.
321b. Disability Coordinator.
321c. Department and Agency officials.
321d. National Operations Center.
321e. Repealed.
321f. Nuclear incident response.
321g. Conduct of certain public health-related activities.
321h. Use of national private sector networks in emergency response.
321i. Use of commercially available technology, goods, and services.
321j. Procurement of security countermeasures for Strategic National Stockpile.
321k. Model standards and guidelines for critical infrastructure workers.
321*l*. Guidance and recommendations.
321m. Voluntary private sector preparedness accreditation and certification program.
321n. Acceptance of gifts.
321*o*. Integrated public alert and warning system modernization.
321o–1. Integrated public alert and warning system.
321p. National planning and education.
321q. Coordination of Department of Homeland Security efforts related to food, agriculture, and veterinary defense against terrorism.
321r. Transfer of equipment during a public health emergency.
322. Continuity of the economy plan.
323. Guidance on how to prevent exposure to and release of PFAS.

SUBCHAPTER VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS

331. Treatment of charitable trusts for members of the Armed Forces of the United States and other governmental organizations.

SUBCHAPTER VII—MANAGEMENT

341. Under Secretary for Management.
342. Chief Financial Officer.
343. Chief Information Officer.
344. Chief Human Capital Officer.
345. Establishment of Officer for Civil Rights and Civil Liberties.
346. Consolidation and co-location of offices.
347. Quadrennial homeland security review.
348. Joint task forces.
349. Office of Strategy, Policy, and Plans.

350. Workforce health and medical support.
351. Employee engagement.
352. Annual employee award program.
353. Acquisition professional career program.

SUBCHAPTER VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

PART A—COORDINATION WITH NON-FEDERAL ENTITIES

361. Office for State and Local Government Coordination.

PART B—INSPECTOR GENERAL

371. Repealed.

PART C—UNITED STATES SECRET SERVICE

381. Functions transferred.
382. Use of proceeds derived from criminal investigations.
383. National Computer Forensics Institute.

PART D—ACQUISITIONS

391. Research and development projects.
392. Personal services.
393. Special streamlined acquisition authority.
394. Unsolicited proposals.
395. Prohibition on contracts with corporate expatriates.
396. Lead system integrator; financial interests.
397. Requirements to buy certain items related to national security interests.

PART E—HUMAN RESOURCES MANAGEMENT

411. Establishment of human resources management system.
412. Labor-management relations.
413. Use of counternarcotics enforcement activities in certain employee performance appraisals.
414. Homeland Security Rotation Program.
415. Homeland Security Education Program.
416. Use of protective equipment or measures by employees.
417. Rotational cybersecurity research program.

PART F—FEDERAL EMERGENCY PROCUREMENT FLEXIBILITY

421. Definition.
422. Procurements for defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack.
423. Increased simplified acquisition threshold for procurements in support of humanitarian or peacekeeping operations or contingency operations.
424. Increased micro-purchase threshold for certain procurements.
425. Application of certain commercial items authorities to certain procurements.
426. Use of streamlined procedures.
427. Review and report by Comptroller General.
428. Identification of new entrants into the Federal marketplace.

PART G—SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES

441. Administration.
442. Litigation management.
443. Risk management.
444. Definitions.

PART H—MISCELLANEOUS PROVISIONS

451. Advisory committees.
452. Reorganization.

453. Use of appropriated funds.
453a. Additional uses of appropriated funds.
453b. Requirement to buy certain items related to national security interests from American sources; exceptions.
453c. Disposition of equines unfit for service.
454. Future Years Homeland Security Program.
455. Miscellaneous authorities.
456. Military activities.
457. Regulatory authority and preemption.
458. Office of Counternarcotics Enforcement.
459. Office of International Affairs.
460. Prohibition of the Terrorism Information and Prevention System.
461. Review of pay and benefit plans.
462. Office of National Capital Region Coordination.
463. Requirement to comply with laws protecting equal employment opportunity and providing whistleblower protections.
464. Federal Law Enforcement Training Centers.
464a. Repealed.
464b. Staffing accreditation function.
464c. Student housing.
464d. Additional funds for training.
464e. Short-term medical services for students.
465. Joint Interagency Task Force.
466. Sense of Congress reaffirming the continued importance and applicability of the Posse Comitatus Act.
467. Coordination with the Department of Health and Human Services under the Public Health Service Act.
468. Preserving Coast Guard mission performance.
469. Fees for credentialing and background investigations in transportation.
469a. Collection of fees from non-Federal participants in meetings.
470. Disclosures regarding homeland security grants.
471. Annual ammunition report.
472. Annual weaponry report.
473. Cyber Crimes Center, Child Exploitation Investigations Unit, Computer Forensics Unit, and Cyber Crimes Unit.
474. Homeland security critical domain research and development.
475. Transnational Criminal Investigative Units.
475a. Mentor-protégé program.

PART I—INFORMATION SHARING

481. Short title; findings; and sense of Congress.
482. Facilitating homeland security information sharing procedures.
483. Report.
484. Authorization of appropriations.
484a. Reciprocal information sharing.
485. Information sharing.
486. Limitation of liability.

PART J—SECURE HANDLING OF AMMONIUM NITRATE

488. Definitions.
488a. Regulation of the sale and transfer of ammonium nitrate.
488b. Inspection and auditing of records.
488c. Administrative provisions.
488d. Theft reporting requirement.
488e. Prohibitions and penalty.

488f. Protection from civil liability.
488g. Preemption of other laws.
488h. Deadlines for regulations.
488i. Authorization of appropriations.

SUBCHAPTER IX—NATIONAL HOMELAND SECURITY COUNCIL

491. National Homeland Security Council.
492. Function.
493. Membership.
494. Other functions and activities.
495. Staff composition.
496. Relation to the National Security Council.

SUBCHAPTER X—CONSTRUCTION

511. Information security responsibilities of certain agencies.
512. Construction.
513. Federal air marshal program.

SUBCHAPTER XI—DEPARTMENT OF JUSTICE DIVISIONS

PART A—EXECUTIVE OFFICE FOR IMMIGRATION REVIEW

521. Legal status of EOIR.
522. Statutory construction.

PART B—TRANSFER OF THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS TO THE DEPARTMENT OF JUSTICE

531. Bureau of Alcohol, Tobacco, Firearms, and Explosives.
532. Explosives Training and Research Facility.
533. Transferred.

SUBCHAPTER XII—TRANSITION

PART A—REORGANIZATION PLAN

541. Definitions.
542. Reorganization plan.
543. Review of congressional committee structures.

PART B—TRANSITIONAL PROVISIONS

551. Transitional authorities.
552. Savings provisions.
552a. Savings provision of certain transfers made under the Homeland Security Act of 2002.
553. Terminations.
554. National identification system not authorized.
555. Continuity of Inspector General oversight.
556. Incidental transfers.
557. Reference.

SUBCHAPTER XII–A—TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

561. Definitions.

PART B—TRANSPORTATION SECURITY ADMINISTRATION ACQUISITION IMPROVEMENTS

563. 5-year technology investment plan.
563a. Acquisition justification and reports.
563b. Acquisition baseline establishment and reports.
563c. Inventory utilization.
563d. Small business contracting goals.
563e. Consistency with the Federal Acquisition Regulation and departmental policies and directives.

563f. Diversified security technology industry marketplace.

PART C—MAINTENANCE OF SECURITY-RELATED TECHNOLOGY

565. Maintenance validation and oversight.

SUBCHAPTER XIII—EMERGENCY COMMUNICATIONS

571. Emergency Communications Division.
572. National Emergency Communications Plan.
573. Assessments and reports.
574. Coordination of Department emergency communications grant programs.
575. Regional emergency communications coordination.
576. Emergency Communications Preparedness Center.
577. Urban and other high risk area communications capabilities.
578. Definition.
579. Interoperable Emergency Communications Grant Program.
580. Border interoperability demonstration project.

SUBCHAPTER XIV—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

590. Definitions.

PART A—COUNTERING WEAPONS OF MASS DESTRUCTION

591. Countering Weapons of Mass Destruction Office.

PART B—MISSION OF THE OFFICE

591g. Mission of the Office.
591h. Relationship to other Department components and Federal agencies.
592. Responsibilities.
592a. Technology research and development investment strategy for nuclear and radiological detection.
593. Hiring authority.
594. Testing authority.
595. Repealed.
596. Contracting and grant making authorities.
596a. Joint annual interagency review of global nuclear detection architecture.
596b. Securing the Cities program.

PART C—CHIEF MEDICAL OFFICER

597. Chief Medical Officer.
597a. Medical countermeasures.

SUBCHAPTER XV—HOMELAND SECURITY GRANTS

601. Definitions.

PART A—GRANTS TO STATES AND HIGH-RISK URBAN AREAS

603. Homeland security grant programs.
604. Urban Area Security Initiative.
605. State Homeland Security Grant Program.
606. Grants to directly eligible tribes.
607. Terrorism prevention.
608. Prioritization.
609. Use of funds.
609a. Nonprofit Security Grant Program.

PART B—GRANTS ADMINISTRATION

611. Administration and coordination.
612. Accountability.
613. Identification of reporting redundancies and development of performance metrics.

SUBCHAPTER XVI—CHEMICAL FACILITY ANTI-TERRORISM STANDARDS

621 to 629. Omitted.

SUBCHAPTER XVII—ANTI-TRAFFICKING TRAINING FOR DEPARTMENT OF HOMELAND SECURITY PERSONNEL

641. Definitions.
642. Training for Department personnel to identify human trafficking.
643. Certification and report to Congress.
644. Assistance to non-Federal entities.
645. Victim protection training for the Department of Homeland Security.
645a. Human trafficking assessment.

SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

650. Definitions.

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

651. Definition.
652. Cybersecurity and Infrastructure Security Agency.
652a. Sector Risk Management Agencies.
653. Cybersecurity Division.
654. Infrastructure Security Division.
655. Enhancement of Federal and non-Federal cybersecurity.
656. NET Guard.
657. Cyber Security Enhancement Act of 2002.
658. Cybersecurity recruitment and retention.
659. National cybersecurity and communications integration center.
660. Cybersecurity plans.
661. Cybersecurity strategy.
662. Clearances.
663. Federal intrusion detection and prevention system.
664. National asset database.
665. Duties and authorities relating to .gov internet domain.
665a. Intelligence and cybersecurity diversity fellowship program.
665b. Joint cyber planning office.
665c. Cybersecurity State Coordinator.
665d. Sector Risk Management Agencies.
665e. Cybersecurity Advisory Committee.
665f. Cybersecurity education and training programs.
665g. State and Local Cybersecurity Grant Program.
665h. National Cyber Exercise Program.
665i. CyberSentry program.
665j. Ransomware threat mitigation activities.
665k. Federal Clearinghouse on School Safety Evidence-based Practices.
665*l*. School and daycare protection.
665m. President's Cup Cybersecurity Competition.
665n. Industrial Control Systems Cybersecurity Training Initiative.

PART B—CRITICAL INFRASTRUCTURE INFORMATION

671. Definitions.
672. Designation of critical infrastructure protection program.
673. Protection of voluntarily shared critical infrastructure information.
674. No private right of action.

PART C—DECLARATION OF A SIGNIFICANT INCIDENT

677. Sense of Congress.
677a. Definitions.
677b. Declaration.
677c. Cyber Response and Recovery Fund.

677d. Notification and reporting.
677e. Rule of construction.
677f. Authorization of appropriations.
677g. Sunset.

PART D—CYBER INCIDENT REPORTING

681. Definitions.
681a. Cyber incident review.
681b. Required reporting of certain cyber incidents.
681c. Voluntary reporting of other cyber incidents.
681d. Noncompliance with required reporting.
681e. Information shared with or provided to the Federal Government.
681f. Cyber Incident Reporting Council.
681g. Federal sharing of incident reports.

§101. Definitions

In this chapter, the following definitions apply:

(1) Each of the terms "American homeland" and "homeland" means the United States.

(2) The term "appropriate congressional committee" means any committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.

(3) The term "assets" includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) The term "critical infrastructure" has the meaning given that term in section 5195c(e) of title 42.

(5) The term "Department" means the Department of Homeland Security.

(6) The term "emergency response providers" includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

(7) The term "EMP" means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including such a pulse caused by an act of terrorism.

(8) The term "executive agency" means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5.

(9) The term "functions" includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.

(10) The term "GMD" means a geomagnetic disturbance caused by a solar storm or another naturally occurring phenomenon.

(11) The term "intelligence component of the Department" means any element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence, as defined under section 3003(5) of title 50, except—

(A) the United States Secret Service; and

(B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy pursuant to section 3 [1] of title 14, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3003(4) of title 50.[2]

(12) The term "key resources" means publicly or privately controlled resources essential to the minimal operations of the economy and government.

(13) The term "local government" means—

(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(C) a rural community, unincorporated town or village, or other public entity.

(14) The term "major disaster" has the meaning given in section 5122(2) of title 42.

(15) The term "personnel" means officers and employees.

(16) The term "Secretary" means the Secretary of Homeland Security.

(17) The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(18) The term "terrorism" means any activity that—

(A) involves an act that—

(i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and

(ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and

(B) appears to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

(19)(A) The term "United States", when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this chapter shall be construed to modify the definition of "United States" for the purposes of the Immigration and Nationality Act [8 U.S.C. 1101 et seq.] or any other immigration or nationality law.

(20) The term "voluntary preparedness standards" means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as the American National Standards Institute's National Fire Protection Association Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600).

(Pub. L. 107–296, §2, Nov. 25, 2002, 116 Stat. 2140; Pub. L. 109–295, title VI, §612(d), Oct. 4, 2006, 120 Stat. 1410; Pub. L. 109–347, title VI, §613, Oct. 13, 2006, 120 Stat. 1943; Pub. L. 110–53, title V, §502(a), title IX, §901(d), Aug. 3, 2007, 121 Stat. 310, 371; Pub. L. 114–328, div. A, title XIX, §1913(a)(1), Dec. 23, 2016, 130 Stat. 2684.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out below and Tables.

Section 3 of title 14, referred to in par. (11)(B), was redesignated section 103 of title 14 by Pub. L. 115–282, title I, §103(b), Dec. 4, 2018, 132 Stat. 4195, and references to section 3 of title 14 deemed to refer to such redesignated section, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of

Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

The Immigration and Nationality Act, referred to in par. (19)(B), is act June 27, 1952, ch. 477, 66 Stat. 163, as amended, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

AMENDMENTS

2016—Pars. (7) to (20). Pub. L. 114–328 added par. (7), redesignated former pars. (7) and (8) as (8) and (9), respectively, added par. (10), and redesignated former pars. (9) to (18) as (11) to (20), respectively.

2007—Pars. (9) to (17). Pub. L. 110–53, §502(a), added par. (9) and redesignated former pars. (9) to (16) as (10) to (17), respectively.

Par. (18). Pub. L. 110–53, §901(d), added par. (18).

2006—Par. (6). Pub. L. 109–347 inserted "governmental and nongovernmental" after "local".

Pub. L. 109–295 inserted "fire," after "safety,".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Pub. L. 107–296, §4, Nov. 25, 2002, 116 Stat. 2142, provided that: "This Act [see Tables for classification] shall take effect 60 days after the date of enactment [Nov. 25, 2002]."

SHORT TITLE OF 2025 AMENDMENT

Pub. L. 119–60, div. H, title LXXXVI, §8601, Dec. 18, 2025, 139 Stat. 1938, provided that: "This title [enacting section 124n–1 of this title, amending section 124n of this title, sections 10152 and 10381 of title 34, Crime Control and Law Enforcement, and section 46307 of Title 49, Transportation, enacting provisions set out as notes under sections 124n and 124n–1 of this title and listed in a table relating to sentencing guidelines set out as a note under section 994 of Title 28, Judiciary and Judicial Procedure] may be cited as the 'SAFER SKIES Act'."

SHORT TITLE OF 2024 AMENDMENT

Pub. L. 118–186, §1, Dec. 23, 2024, 138 Stat. 2636, provided that: "This Act [amending section 182 of this title and enacting provisions set out as notes under section 182 of this title] may be cited as the 'Detection Equipment and Technology Evaluation to Counter the Threat of Fentanyl and Xylazine Act of 2024' or the 'DETECT Fentanyl and Xylazine Act of 2024'."

Pub. L. 118–165, §1, Dec. 23, 2024, 138 Stat. 2581, provided that: "This Act [amending section 609 of this title] may be cited as the 'First Responder Access to Innovative Technologies Act'."

Pub. L. 118–103, §1, Oct. 1, 2024, 138 Stat. 1584, provided that: "This Act [amending section 348 of this title and enacting provisions set out as a note under section 348 of this title] may be cited as the 'DHS Joint Task Forces Reauthorization Act of 2024'."

Pub. L. 118–96, §1, Oct. 1, 2024, 138 Stat. 1569, provided that: "This Act [enacting section 258 of this title, amending sections 252 and 253 of this title, and enacting provisions set out as notes under sections 252 and 258 of this title] may be cited as the 'IMPACTT Human Trafficking Act'."

Pub. L. 118–43, §1, Mar. 18, 2024, 138 Stat. 453, provided that: "This Act [enacting section 226 of this title] may be cited as the 'Eradicating Narcotic Drugs and Formulating Effective New Tools to Address National Yearly Losses of life Act' or the 'END FENTANYL Act'."

SHORT TITLE OF 2022 AMENDMENT

Pub. L. 117–322, §1, Dec. 27, 2022, 136 Stat. 4433, provided that: "This Act [enacting sections 242a and 242b of this title and provisions set out as notes under sections 242 and 242a of this title] may be cited as the 'Countering Human Trafficking Act of 2021'."

Pub. L. 117–263, div. G, title LXXI, §7105(a), Dec. 23, 2022, 136 Stat. 3622, provided that: "This section [enacting section 475 of this title] may be cited as the 'Transnational Criminal Investigative Unit Stipend Act'."

Pub. L. 117–263, div. G, title LXXI, §7111(a), Dec. 23, 2022, 136 Stat. 3625, provided that: "This section [amending section 348 of this title] may be cited as the 'DHS Joint Task Forces Reauthorization Act of 2022'."

Pub. L. 117–248, §1, Dec. 20, 2022, 136 Stat. 2348, provided that: "This Act [enacting section 323 of this title] may be cited as the 'Protecting Firefighters from Adverse Substances Act' or the 'PFAS Act'."

Pub. L. 117–150, §1, June 21, 2022, 136 Stat. 1295, provided that: "This Act [amending sections 651 and

659 of this title] may be cited as the 'State and Local Government Cybersecurity Act of 2021'."

Pub. L. 117–130, §1, June 6, 2022, 136 Stat. 1229, provided that: "This Act [amending sections 112 and 313 of this title] may be cited as the 'Homeland Security for Children Act'."

Pub. L. 117–103, div. Y, §101, Mar. 15, 2022, 136 Stat. 1038, provided that: "This division [enacting part D of subchapter XVIII of this chapter and section 665j of this title, amending section 659 of this title, and enacting provisions set out as notes under sections 652 and 665j of this title] may be cited as the 'Cyber Incident Reporting for Critical Infrastructure Act of 2022'."

SHORT TITLE OF 2021 AMENDMENT

Pub. L. 117–58, div. G, title VI, §70601, Nov. 15, 2021, 135 Stat. 1267, provided that: "This subtitle [subtitle A (§§70601, 70602) of title VI of div. G of Pub. L. 117–58, enacting part C of subchapter XVIII of this chapter] may be cited as the 'Cyber Response and Recovery Act'."

Pub. L. 117–58, div. G, title VI, §70611, Nov. 15, 2021, 135 Stat. 1272, provided that: "This subtitle [subtitle B (§§70611, 70612) of title VI of div. G of Pub. L. 117–58, enacting section 665g of this title] may be cited as the 'State and Local Cybersecurity Improvement Act'."

SHORT TITLE OF 2020 AMENDMENT

Pub. L. 116–260, div. U, title III, §301, Dec. 27, 2020, 134 Stat. 2291, provided that: "This title [enacting section 216 of this title] may be cited as the 'Synthetic Opioid Exposure Prevention and Training Act'."

Pub. L. 116–260, div. U, title VI, §601, Dec. 27, 2020, 134 Stat. 2294, provided that: "This title [enacting section 124m–1 of this title and provisions set out as a note under section 124m–1 of this title] may be cited as the 'Counter Threats Advisory Board Act of 2019'."

Pub. L. 116–260, div. U, title VII, §701(a), Dec. 27, 2020, 134 Stat. 2295, provided that: "This title [enacting section 195g of this title] may be cited as the 'DHS Countering Unmanned Aircraft Systems Coordinator Act'."

Pub. L. 116–260, div. U, title IX, §901, Dec. 27, 2020, 134 Stat. 2297, provided that: "This title [enacting section 665 of this title, amending sections 609 and 652 of this title, and enacting provisions set out as notes under section 665 of this title] may be cited as the 'DOTGOV Online Trust in Government Act of 2020' or the 'DOTGOV Act of 2020'."

Pub. L. 116–116, §1, Mar. 2, 2020, 134 Stat. 110, provided that: "This Act [amending section 124h of this title and enacting provisions set out as a note under section 121 of this title] may be cited as the 'DHS Field Engagement Accountability Act'."

Pub. L. 116–108, §1, Jan. 24, 2020, 133 Stat. 3294, provided that: "This Act [enacting section 609a of this title and amending section 603 of this title] may be cited as the 'Securing American Nonprofit Organizations Against Terrorism Act of 2019'."

SHORT TITLE OF 2019 AMENDMENT

Pub. L. 116–94, div. L, §101, Dec. 20, 2019, 133 Stat. 3089, provided that: "This division [amending section 659 of this title] may be cited as the 'DHS Cyber Hunt and Incident Response Teams Act of 2019'."

Pub. L. 116–2, §1, Jan. 18, 2019, 133 Stat. 5, provided that: "This Act [amending provisions set out as a note under section 621 of this title] may be cited as the 'Chemical Facility Anti-Terrorism Standards Program Extension Act'."

SHORT TITLE OF 2018 AMENDMENT

Pub. L. 115–387, §1, Dec. 21, 2018, 132 Stat. 5162, provided that: "This Act [enacting sections 350, 590, 591, 591g, 591h, 596b, and 597 of this title, amending sections 113, 195b, 195c, 315, 321q, 592, 593, 594, 596, and 596a of this title, repealing sections 321e, 591, and 595 of this title, and enacting provisions set out as notes under section 591 of this title] may be cited as the 'Countering Weapons of Mass Destruction Act of 2018'."

Pub. L. 115–331, §1, Dec. 19, 2018, 132 Stat. 4484, provided that: "This Act [enacting section 126 of this title] may be cited as the 'Department of Homeland Security Data Framework Act of 2018'."

Pub. L. 115–278, §1, Nov. 16, 2018, 132 Stat. 4168, provided that: "This Act [see Tables for classification] may be cited as the 'Cybersecurity and Infrastructure Security Agency Act of 2018'."

Pub. L. 115–254, div. H, §1601, Oct. 5, 2018, 132 Stat. 3522, provided that: "This division [enacting section 124 of this title and section 104 of Title 14, Coast Guard] may be cited as the 'Preventing Emerging Threats Act of 2018'."

Pub. L. 115–125, §1, Feb. 14, 2018, 132 Stat. 315, provided that: "This Act [enacting section 242 of this title and provisions set out as a note under section 242 of this title] may be cited as the 'Department of Homeland Security Blue Campaign Authorization Act'."

SHORT TITLE OF 2017 AMENDMENT

Pub. L. 115–79, §1, Nov. 2, 2017, 131 Stat. 1258, provided that: "This Act [enacting section 218 of this title, amending section 211 of this title, enacting provisions set out as notes under section 218 of this title and section 1185 of Title 8, Aliens and Nationality, and repealing provisions set out as a note under section 1185 of Title 8] may be cited as the 'Asia-Pacific Economic Cooperation Business Travel Cards Act of 2017'."

Pub. L. 115–43, §1, June 30, 2017, 131 Stat. 884, provided that: "This Act [enacting section 321q of this title] may be cited as the 'Securing our Agriculture and Food Act'."

Pub. L. 115–38, §1, June 6, 2017, 131 Stat. 855, provided that: "This Act [amending section 341 of this title] may be cited as the 'DHS Stop Asset and Vehicle Excess Act' or the 'DHS SAVE Act'."

SHORT TITLE OF 2016 AMENDMENT

Pub. L. 114–321, §1, Dec. 16, 2016, 130 Stat. 1623, provided that: "This Act [amending section 318 of this title] may be cited as the 'RESPONSE Act of 2016'."

Pub. L. 114–304, §1, Dec. 16, 2016, 130 Stat. 1519, provided that: "This Act [amending section 195c of this title and section 8606 of Title 22, Foreign Relations and Intercourse] may be cited as the 'United States-Israel Advanced Research Partnership Act of 2016'."

Pub. L. 114–285, §1, Dec. 16, 2016, 130 Stat. 1453, provided that: "This Act [amending section 464 of this title] may be cited as the 'Federal Law Enforcement Training Centers Reform and Improvement Act of 2015'."

Pub. L. 114–279, §1, Dec. 16, 2016, 130 Stat. 1413, provided that: "This Act [enacting part G of subchapter IV of this chapter, amending section 221 of this title and section 4451 of Title 19, Customs Duties, and repealing provisions set out as a note under section 211 of this title] may be cited as the 'Cross-Border Trade Enhancement Act of 2016'."

Pub. L. 114–143, §1, Apr. 11, 2016, 130 Stat. 327, provided that: "This Act [enacting section 321o of this title and provisions set out as a note under section 321o of this title] may be cited as the 'Integrated Public Alert and Warning System Modernization Act of 2015'."

SHORT TITLE OF 2015 AMENDMENT

Pub. L. 114–113, div. N, title II, §201, Dec. 18, 2015, 129 Stat. 2956, provided that: "This subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, amending sections 131, 148, and 149 of this title and enacting provisions set out as notes under section 131 of this title] may be cited as the 'National Cybersecurity Protection Advancement Act of 2015'."

Pub. L. 114–80, §1, Nov. 5, 2015, 129 Stat. 646, provided that: "This Act [enacting section 195d of this title] may be cited as the 'DHS Social Media Improvement Act of 2015'."

Pub. L. 114–22, title III, §301, May 29, 2015, 129 Stat. 251, provided that: "This title [enacting section 473 of this title and section 2421 of Title 18, Crimes and Criminal Procedure, amending section 187 of this title, repealing former section 2421 of Title 18, and enacting provisions set out as a note under section 473 of this title] may be cited as the 'Human Exploitation Rescue Operations Act of 2015' or the 'HERO Act of 2015'."

SHORT TITLE OF 2014 AMENDMENT

Pub. L. 113–284, §1, Dec. 18, 2014, 128 Stat. 3089, provided that: "This Act [amending sections 468 and 612 of this title, enacting provisions set out as a note under section 612 of this title, and amending provisions set out as a note under section 70101 of Title 46, Shipping] may be cited as the 'DHS OIG Mandates Revision Act of 2014'."

Pub. L. 113–282, §1, Dec. 18, 2014, 128 Stat. 3066, provided that: "This Act [enacting sections 148 to 150 of this title and provisions set out as notes under sections 148 and 149 of this title and formerly set out as a note under section 3543 of Title 44, Public Printing and Documents] may be cited as the 'National Cybersecurity Protection Act of 2014'."

Pub. L. 113–254, §1, Dec. 18, 2014, 128 Stat. 2898, provided that: "This Act [enacting subchapter XVI of this chapter and enacting and repealing provisions set out as notes under section 121 of this title] may be cited as the 'Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014'."

Pub. L. 113–246, §1, Dec. 18, 2014, 128 Stat. 2880, provided that: "This Act [enacting section 146 of this title and provisions set out as a note under section 146 of this title] may be cited as the 'Cybersecurity Workforce Assessment Act'."

Pub. L. 113–245, §1, Dec. 18, 2014, 128 Stat. 2871, provided that: "This Act [enacting subchapter XII–A of this chapter and provisions set out as notes under section 561 of this title] may be cited as the 'Transportation Security Acquisition Reform Act'."

SHORT TITLE OF 2013 AMENDMENT

Pub. L. 112–265, §1, Jan. 14, 2013, 126 Stat. 2435, provided that: "This Act [amending section 455 of this title and section 530C of Title 28, Judiciary and Judicial Procedure] may be cited as the 'Investigative Assistance for Violent Crimes Act of 2012'."

SHORT TITLE OF 2012 AMENDMENT

Pub. L. 112–205, §1, Dec. 7, 2012, 126 Stat. 1487, provided that: "This Act [enacting section 240 of this title and provisions set out as a note under section 240 of this title] may be cited as the 'Jaime Zapata Border Enforcement Security Task Force Act'."

SHORT TITLE OF 2011 AMENDMENT

Pub. L. 111–376, §1, Jan. 4, 2011, 124 Stat. 4104, provided that: "This Act [enacting section 221 of this title and provisions set out as a note under section 221 of this title] may be cited as the 'Anti-Border Corruption Act of 2010'."

SHORT TITLE OF 2010 AMENDMENT

Pub. L. 111–271, §1, Oct. 12, 2010, 124 Stat. 2852, provided that: "This Act [enacting section 613 of this title] may be cited as the 'Redundancy Elimination and Enhanced Performance for Preparedness Grants Act'."

Pub. L. 111–258, §1, Oct. 7, 2010, 124 Stat. 2648, provided that: "This Act [enacting section 124m of this title and section 435d of Title 50, War and National Defense, amending sections 121 and 124k of this title and section 403–1 of Title 50, and enacting provisions set out as notes under section 124m of this title and sections 435 and 435d of Title 50] may be cited as the 'Reducing Over-Classification Act'."

Pub. L. 111–245, §1, Sept. 30, 2010, 124 Stat. 2620, provided that: "This Act [enacting section 321n of this title, amending sections 453 and 464 of this title, and repealing section 464a of this title] may be cited as the 'First Responder Anti-Terrorism Training Resources Act'."

Pub. L. 111–140, §1, Feb. 16, 2010, 124 Stat. 31, provided that: "This Act [amending sections 592 and 596a of this title and enacting provisions set out as a note under section 592 of this title] may be cited as the 'Nuclear Forensics and Attribution Act'."

SHORT TITLE OF 2008 AMENDMENT

Pub. L. 110–412, §1, Oct. 14, 2008, 122 Stat. 4336, provided that: "This Act [amending section 609 of this title] may be cited as the 'Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008' or the 'PRICE of Homeland Security Act'."

SHORT TITLE OF 2007 AMENDMENT

Pub. L. 110–53, §1(a), Aug. 3, 2007, 121 Stat. 266, provided that: "This Act [see Tables for classification] may be cited as the 'Implementing Recommendations of the 9/11 Commission Act of 2007'."

SHORT TITLE OF 2006 AMENDMENT

Pub. L. 109–295, title VI, §671(a), Oct. 4, 2006, 120 Stat. 1433, provided that: "This section [enacting subchapter XIII of this chapter] may be cited as the '21st Century Emergency Communications Act of 2006'."

SHORT TITLE OF 2004 AMENDMENT

Pub. L. 108–458, title VII, §7001, Dec. 17, 2004, 118 Stat. 3775, provided that: "This title [see Tables for classification] may be cited as the '9/11 Commission Implementation Act of 2004'."

Pub. L. 108–458, title VIII, §8301, Dec. 17, 2004, 118 Stat. 3867, provided that: "This subtitle [subtitle C (§§8301–8306) of title VIII of Pub. L. 108–458, amending sections 111, 142, and 345 of this title and section 8I of the Inspector General Act of 1978, Pub. L. 95–452, set out in the Appendix to Title 5, Government Organization and Employees, and enacting provisions set out as a note under section 112 of this title] may be cited as the 'Homeland Security Civil Rights and Civil Liberties Protection Act of 2004'."

Pub. L. 108–330, §1, Oct. 16, 2004, 118 Stat. 1275, provided that: "This Act [amending sections 113, 342, and 454 of this title and sections 901 and 3516 of Title 31, Money and Finance, and enacting provisions set out as notes under section 342 of this title and sections 901 and 3516 of Title 31] may be cited as 'Department of Homeland Security Financial Accountability Act'."

SHORT TITLE OF 2003 AMENDMENT

Pub. L. 108–7, div. L, Feb. 20, 2003, 117 Stat. 532, provided in part that: "This division [enacting sections 103 and 552a of this title and section 8I of the Inspector General Act of 1978, Pub. L. 95–452, set out in the Appendix to Title 5, Government Organization and Employees, amending sections 113, 162, 164, 188, 395, 453, and 551 of this title, section 8D of the Inspector General Act of 1978, sections 1103 and 1356 of Title 8, Aliens and Nationality, and section 300aa–33 of Title 42, The Public Health and Welfare, redesignating

section 8I of the Inspector General Act of 1978 as section 8J, repealing section 371 of this title and former section 8J of the Inspector General Act of 1978, enacting provisions set out as notes under section 521 of this title, section 1356 of Title 8, and section 300aa–33 of Title 42, and repealing provisions set out as a note under section 300aa–33 of Title 42] may be cited as the 'Homeland Security Act Amendments of 2003'."

SHORT TITLE

Pub. L. 107–296, §1(a), Nov. 25, 2002, 116 Stat. 2135, provided that: "This Act [see Tables for classification] may be cited as the 'Homeland Security Act of 2002'."

Pub. L. 107–296, title XXII, §2221, formerly title II, §211, Nov. 25, 2002, 116 Stat. 2150; renumbered §2221, Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, provided that: "This subtitle [subtitle B (§§2221–2225) of title XXII of Pub. L. 107–296, enacting part B of subchapter XVIII of this chapter] may be cited as the 'Critical Infrastructure Information Act of 2002'."

Pub. L. 107–296, title VIII, §861, Nov. 25, 2002, 116 Stat. 2238, provided that: "This subtitle [subtitle G (§§861–865) of title VIII of Pub. L. 107–296, enacting part G of subchapter VIII of this chapter] may be cited as the 'Support Anti-terrorism by Fostering Effective Technologies Act of 2002' or the 'SAFETY Act'."

For short title of part I of subchapter VIII of this chapter as the "Homeland Security Information Sharing Act", see section 481(a) of this title.

Pub. L. 107–296, title X, §1001(a), Nov. 25, 2002, 116 Stat. 2259, provided that: "This title [enacting subchapter X of this chapter and sections 3531 to 3537 and 3538 of Title 44, Public Printing and Documents, amending section 2224 of Title 10, Armed Forces, sections 278g–3 and 278g–4 of Title 15, Commerce and Trade, section 11331 of Title 40, Public Buildings, Property, and Works, and sections 3504 to 3506 of Title 44, and repealing section 11332 of Title 40 and provisions set out as notes under section 3531 of Title 44] may be cited as the 'Federal Information Security Management Act of 2002'."

[For another Federal Information Security Management Act of 2002, see section 301(a) of Pub. L. 107–347, title III, Dec. 17, 2002, 116 Stat. 2946, set out as a note under section 101 of Title 44, Public Printing and Documents.]

PROHIBITION ON REGULATORY AUTHORITY

Pub. L. 114–328, div. A, title XIX, §1913(e), Dec. 23, 2016, 130 Stat. 2687, provided that: "Nothing in this section [enacting sections 195f and 321p of this title, amending this section, sections 121 and 311 of this title, and section 712 of Title 14, Coast Guard, and enacting provisions set out as a note under section 121 of this title], including the amendments made by this section, shall be construed to grant any regulatory authority."

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Pub. L. 107–306, title VI, Nov. 27, 2002, 116 Stat. 2408, as amended by Pub. L. 108–207, §1, Mar. 16, 2004, 118 Stat. 556; Pub. L. 117–286, §4(a)(11), Dec. 27, 2022, 136 Stat. 4306, provided that:

"SEC. 601. ESTABLISHMENT OF COMMISSION.

"There is established in the legislative branch the National Commission on Terrorist Attacks Upon the United States (in this title referred to as the 'Commission').

"SEC. 602. PURPOSES.

"The purposes of the Commission are to—

"(1) examine and report upon the facts and causes relating to the terrorist attacks of September 11, 2001, occurring at the World Trade Center in New York, New York, in Somerset County, Pennsylvania, and at the Pentagon in Virginia;

"(2) ascertain, evaluate, and report on the evidence developed by all relevant governmental agencies regarding the facts and circumstances surrounding the attacks;

"(3) build upon the investigations of other entities, and avoid unnecessary duplication, by reviewing the findings, conclusions, and recommendations of—

"(A) the Joint Inquiry of the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives regarding the terrorist attacks of September 11, 2001, (hereinafter in this title referred to as the 'Joint Inquiry'); and

"(B) other executive branch, congressional, or independent commission investigations into the terrorist attacks of September 11, 2001, other terrorist attacks, and terrorism generally;

"(4) make a full and complete accounting of the circumstances surrounding the attacks, and the extent of the United States' preparedness for, and immediate response to, the attacks; and

"(5) investigate and report to the President and Congress on its findings, conclusions, and recommendations for corrective measures that can be taken to prevent acts of terrorism.

"SEC. 603. COMPOSITION OF COMMISSION.

"(a) MEMBERS.—The Commission shall be composed of 10 members, of whom—

"(1) 1 member shall be appointed by the President, who shall serve as chairman of the Commission;

"(2) 1 member shall be appointed by the leader of the Senate (majority or minority leader, as the case may be) of the Democratic Party, in consultation with the leader of the House of Representatives (majority or minority leader, as the case may be) of the Democratic Party, who shall serve as vice chairman of the Commission;

"(3) 2 members shall be appointed by the senior member of the Senate leadership of the Democratic Party;

"(4) 2 members shall be appointed by the senior member of the leadership of the House of Representatives of the Republican Party;

"(5) 2 members shall be appointed by the senior member of the Senate leadership of the Republican Party; and

"(6) 2 members shall be appointed by the senior member of the leadership of the House of Representatives of the Democratic Party.

"(b) QUALIFICATIONS; INITIAL MEETING.—

"(1) POLITICAL PARTY AFFILIATION.—Not more than 5 members of the Commission shall be from the same political party.

"(2) NONGOVERNMENTAL APPOINTEES.—An individual appointed to the Commission may not be an officer or employee of the Federal Government or any State or local government.

"(3) OTHER QUALIFICATIONS.—It is the sense of Congress that individuals appointed to the Commission should be prominent United States citizens, with national recognition and significant depth of experience in such professions as governmental service, law enforcement, the armed services, law, public administration, intelligence gathering, commerce (including aviation matters), and foreign affairs.

"(4) DEADLINE FOR APPOINTMENT.—All members of the Commission shall be appointed on or before December 15, 2002.

"(5) INITIAL MEETING.—The Commission shall meet and begin the operations of the Commission as soon as practicable.

"(c) QUORUM; VACANCIES.—After its initial meeting, the Commission shall meet upon the call of the chairman or a majority of its members. Six members of the Commission shall constitute a quorum. Any vacancy in the Commission shall not affect its powers, but shall be filled in the same manner in which the original appointment was made.

"SEC. 604. FUNCTIONS OF COMMISSION.

"(a) IN GENERAL.—The functions of the Commission are to—

"(1) conduct an investigation that—

"(A) investigates relevant facts and circumstances relating to the terrorist attacks of September 11, 2001, including any relevant legislation, Executive order, regulation, plan, policy, practice, or procedure; and

"(B) may include relevant facts and circumstances relating to—

"(i) intelligence agencies;

"(ii) law enforcement agencies;

"(iii) diplomacy;

"(iv) immigration, nonimmigrant visas, and border control;

"(v) the flow of assets to terrorist organizations;

"(vi) commercial aviation;

"(vii) the role of congressional oversight and resource allocation; and

"(viii) other areas of the public and private sectors determined relevant by the Commission for its inquiry;

"(2) identify, review, and evaluate the lessons learned from the terrorist attacks of September 11, 2001, regarding the structure, coordination, management policies, and procedures of the Federal Government, and, if appropriate, State and local governments and nongovernmental entities, relative to detecting, preventing, and responding to such terrorist attacks; and

"(3) submit to the President and Congress such reports as are required by this title containing such findings, conclusions, and recommendations as the Commission shall determine, including proposing organization, coordination, planning, management arrangements, procedures, rules, and regulations.

"(b) RELATIONSHIP TO INTELLIGENCE COMMITTEES' INQUIRY.—When investigating facts and circumstances relating to the intelligence community, the Commission shall—

"(1) first review the information compiled by, and the findings, conclusions, and recommendations of, the Joint Inquiry; and

"(2) after that review pursue any appropriate area of inquiry if the Commission determines that—

"(A) the Joint Inquiry had not investigated that area;

"(B) the Joint Inquiry's investigation of that area had not been complete; or

"(C) new information not reviewed by the Joint Inquiry had become available with respect to that area.

"SEC. 605. POWERS OF COMMISSION.

"(a) IN GENERAL.—

"(1) HEARINGS AND EVIDENCE.—The Commission or, on the authority of the Commission, any subcommittee or member thereof, may, for the purpose of carrying out this title—

"(A) hold such hearings and sit and act at such times and places, take such testimony, receive such evidence, administer such oaths; and

"(B) subject to paragraph (2)(A), require, by subpoena or otherwise, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, and documents, as the Commission or such designated subcommittee or designated member may determine advisable.

"(2) SUBPOENAS.—

"(A) ISSUANCE.—

"(i) IN GENERAL.—A subpoena may be issued under this subsection only—

"(I) by the agreement of the chairman and the vice chairman; or

"(II) by the affirmative vote of 6 members of the Commission.

"(ii) SIGNATURE.—Subject to clause (i), subpoenas issued under this subsection may be issued under the signature of the chairman or any member designated by a majority of the Commission, and may be served by any person designated by the chairman or by a member designated by a majority of the Commission.

"(B) ENFORCEMENT.—

"(i) IN GENERAL.—In the case of contumacy or failure to obey a subpoena issued under subsection (a), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found, or where the subpoena is returnable, may issue an order requiring such person to appear at any designated place to testify or to produce documentary or other evidence. Any failure to obey the order of the court may be punished by the court as a contempt of that court.

"(ii) ADDITIONAL ENFORCEMENT.—In the case of any failure of any witness to comply with any subpoena or to testify when summoned under authority of this section, the Commission may, by majority vote, certify a statement of fact constituting such failure to the appropriate United States attorney, who may bring the matter before the grand jury for its action, under the same statutory authority and procedures as if the United States attorney had received a certification under sections 102 through 104 of the Revised Statutes of the United States (2 U.S.C. 192 through 194).

"(b) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriation Acts, enter into contracts to enable the Commission to discharge its duties under this title.

"(c) INFORMATION FROM FEDERAL AGENCIES.—

"(1) IN GENERAL.—The Commission is authorized to secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government, information, suggestions, estimates, and statistics for the purposes of this title. Each department, bureau, agency, board, commission, office, independent establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Commission, upon request made by the chairman, the chairman of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission.

"(2) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information shall only be received, handled, stored, and disseminated by members of the Commission and its staff consistent with all applicable statutes, regulations, and Executive orders.

"(d) ASSISTANCE FROM FEDERAL AGENCIES.—

"(1) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall provide to the Commission on a reimbursable basis administrative support and other services for the performance of the Commission's functions.

"(2) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance prescribed in paragraph (1), departments and agencies of the United States may provide to the Commission such services, funds, facilities, staff, and other support services as they may determine advisable and as may be authorized

by law.

"(e) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

"(f) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as departments and agencies of the United States.

"SEC. 606. NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5, UNITED STATES CODE.

"(a) IN GENERAL.—Chapter 10 of title 5, United States Code, shall not apply to the Commission.

"(b) PUBLIC MEETINGS AND RELEASE OF PUBLIC VERSIONS OF REPORTS.—The Commission shall—

"(1) hold public hearings and meetings to the extent appropriate; and

"(2) release public versions of the reports required under section 610(a) and (b).

"(c) PUBLIC HEARINGS.—Any public hearings of the Commission shall be conducted in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or Executive order.

"SEC. 607. STAFF OF COMMISSION.

"(a) IN GENERAL.—

"(1) APPOINTMENT AND COMPENSATION.—The chairman, in consultation with vice chairman, in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of a staff director and such other personnel as may be necessary to enable the Commission to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

"(2) PERSONNEL AS FEDERAL EMPLOYEES.—

"(A) IN GENERAL.—The executive director and any personnel of the Commission who are employees shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, and 90 of that title.

"(B) MEMBERS OF COMMISSION.—Subparagraph (A) shall not be construed to apply to members of the Commission.

"(b) DETAILEES.—Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

"(c) CONSULTANT SERVICES.—The Commission is authorized to procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code.

"SEC. 608. COMPENSATION AND TRAVEL EXPENSES.

"(a) COMPENSATION.—Each member of the Commission may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Commission.

"(b) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703(b) [5703] of title 5, United States Code.

"SEC. 609. SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.

"The appropriate Federal agencies or departments shall cooperate with the Commission in expeditiously providing to the Commission members and staff appropriate security clearances to the extent possible pursuant to existing procedures and requirements, except that no person shall be provided with access to classified information under this title without the appropriate security clearances.

"SEC. 610. REPORTS OF COMMISSION; TERMINATION.

"(a) INTERIM REPORTS.—The Commission may submit to the President and Congress interim reports containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

"(b) FINAL REPORT.—Not later than 20 months after the date of the enactment of this Act [Nov. 27,

2002], the Commission shall submit to the President and Congress a final report containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

"(c) TERMINATION.—

"(1) IN GENERAL.—The Commission, and all the authorities of this title, shall terminate 30 days after the date on which the final report is submitted under subsection (b).

"(2) ADMINISTRATIVE ACTIVITIES BEFORE TERMINATION.—The Commission may use the 30-day period referred to in paragraph (1) for the purpose of concluding its activities, including providing testimony to committees of Congress concerning its reports and disseminating the final report.

"SEC. 611. FUNDING.

"(a) TRANSFER FROM THE NATIONAL FOREIGN INTELLIGENCE PROGRAM.—Of the amounts authorized to be appropriated by this Act [see Tables for classification] and made available in public law 107–248 [see Tables for classification] (Department of Defense Appropriations Act, 2003) for the National Foreign Intelligence Program, not to exceed $3,000,000 shall be available for transfer to the Commission for purposes of the activities of the Commission under this title.

"(b) ADDITIONAL FUNDING.—In addition to the amounts made available to the Commission under subsection (a) and under chapter 2 of title II of the Emergency Wartime Supplemental Appropriations Act, 2003 (Public Law 108–11; 117 Stat. 591), of the amounts appropriated for the programs and activities of the Federal Government for fiscal year 2004 that remain available for obligation, not more than $1,000,000 shall be available for transfer to the Commission for purposes of the activities of the Commission under this title.

"(c) DURATION OF AVAILABILITY.—Amounts made available to the Commission under this section shall remain available until the termination of the Commission."

[1] See References in Text note below.

[2] So in original. A closing parenthesis probably should precede the period.

§102. Construction; severability

Any provision of this chapter held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this chapter and shall not affect the remainder thereof, or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

(Pub. L. 107–296, §3, Nov. 25, 2002, 116 Stat. 2141.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§103. Use of appropriated funds

Notwithstanding any other provision of this chapter, any report, notification, or consultation addressing directly or indirectly the use of appropriated funds and stipulated by this chapter to be submitted to, or held with, the Congress or any Congressional committee shall also be submitted to, or held with, the Committees on Appropriations of the Senate and the House of Representatives under the same conditions and with the same restrictions as stipulated by this chapter.

(Pub. L. 107–296, title XVII, §1714, as added Pub. L. 108–7, div. L, §103(5), Feb. 20, 2003, 117

Stat. 529.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

PRIOR PROVISIONS

A prior section 1714 of Pub. L. 107–296 amended section 300aa–33 of Title 42, The Public Health and Welfare, prior to repeal by Pub. L. 108–7, div. L, §102(a), Feb. 20, 2003, 117 Stat. 528.

STATUTORY NOTES AND RELATED SUBSIDIARIES

NOTIFICATIONS FOR REPROGRAMMING OR TRANSFER OF FUNDS

Pub. L. 109–90, title V, §503(e), Oct. 18, 2005, 119 Stat. 2082, provided that: "Hereafter, notwithstanding any other provision of law, notifications pursuant to this section or any other authority for reprogramming or transfer of funds shall be made solely to the Committees on Appropriations of the Senate and the House of Representatives."

§103a. Department of Homeland Security Nonrecurring Expenses Fund

(a) Establishment

There is hereby established in the Treasury of the United States a fund to be known as the "Department of Homeland Security Nonrecurring Expenses Fund" (the Fund).

(b) Transfer of unobligated balances of expired discretionary funds

Unobligated balances of expired discretionary funds appropriated for this or any succeeding fiscal year from the General Fund of the Treasury to the Department of Homeland Security by this or any other Act may be transferred (not later than the end of the fifth fiscal year after the last fiscal year for which such funds are available for the purposes for which appropriated) into the Fund.

(c) Availability of funds

Amounts deposited in the Fund shall be available until expended, and in addition to such other funds as may be available for such purposes, for information technology system modernization and facilities infrastructure improvements necessary for the operation of the Department, subject to approval by the Office of Management and Budget.

(d) Limitation on apportionment or allotment of funds

Amounts in the Fund may not be apportioned or allotted for any fiscal year until after the date on which the Act making full-year appropriations for the Department of Homeland Security for the applicable fiscal year is enacted into law, subject to subsection (e).

(e) Notification of planned use of funds

The Committees on Appropriations of the House of Representatives and the Senate shall be notified at least 15 days in advance of the planned use of funds.

(Pub. L. 117–103, div. F, title V, §538, Mar. 15, 2022, 136 Stat. 343; Pub. L. 118–47, div. C, title V, §539(a), Mar. 23, 2024, 138 Stat. 623.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2022, and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2024—Subsecs. (d), (e). Pub. L. 118–47 added subsecs. (d) and (e) and struck out former subsec. (d). Prior to amendment, text of subsec. (d) read as follows: "Amounts in the Fund may be obligated only after the Committees on Appropriations of the House of Representatives and the Senate are notified at least 15 days in advance of the planned use of funds."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2024 AMENDMENT

Pub. L. 118–47, div. C, title V, §539(b), Mar. 23, 2024, 138 Stat. 624, provided that: "The amendments made by this section [amending this section] shall apply to amounts transferred under such section 538 [of Pub. L. 117–103, 6 U.S.C. 103a] on or after the date of enactment of this Act [Mar. 23, 2024]."

§104. National biodefense strategy

(a) Strategy and implementation plan required

The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture shall jointly develop a national biodefense strategy and associated implementation plan, which shall include a review and assessment of biodefense policies, practices, programs and initiatives. Such Secretaries shall review and, as appropriate, revise the strategy biennially.

(b) Elements

The strategy and associated implementation plan required under subsection (a) shall include each of the following:

(1) An inventory and assessment of all existing strategies, plans, policies, laws, and interagency agreements related to biodefense, including prevention, deterrence, preparedness, detection, response, attribution, recovery, and mitigation.

(2) A description of the biological threats, including biological warfare, bioterrorism, naturally occurring infectious diseases, and accidental exposures.

(3) A description of the current programs, efforts, or activities of the United States Government with respect to preventing the acquisition, proliferation, and use of a biological weapon, preventing an accidental or naturally occurring biological outbreak, and mitigating the effects of a biological epidemic.

(4) A description of the roles and responsibilities of the Executive Agencies, including internal and external coordination procedures, in identifying and sharing information related to, warning of, and protection against, acts of terrorism using biological agents and weapons and accidental or naturally occurring biological outbreaks.

(5) An articulation of related or required interagency capabilities and whole-of-Government activities required to support the national biodefense strategy.

(6) Recommendations for strengthening and improving the current biodefense capabilities, authorities, and command structures of the United States Government.

(7) Recommendations for improving and formalizing interagency coordination and support mechanisms with respect to providing a robust national biodefense.

(8) Any other matters the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture determine necessary.

(c) Submittal to Congress

Not later than 275 days after December 23, 2016, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture

shall submit to the appropriate congressional committees the strategy and associated implementation plan required by subsection (a). The strategy and implementation plan shall be submitted in unclassified form, but may include a classified annex.

(d) Briefings

Not later than March 1, 2017, and annually thereafter until March 1, 2025, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Homeland Security, and the Secretary of Agriculture shall provide to the Committee on Armed Services of the House of Representatives, the Committee on Energy and Commerce of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Agriculture of the House of Representatives a joint briefing on the strategy developed under subsection (a) and the status of the implementation of such strategy.

(e) GAO Review

Not later than 180 days after the date of the submittal of the strategy and implementation plan under subsection (c), the Comptroller General of the United States shall conduct a review of the strategy and implementation plan to analyze gaps and resources mapped against the requirements of the National Biodefense Strategy and existing United States biodefense policy documents.

(f) Appropriate congressional committees defined

In this section, the term "appropriate congressional committees" means the following:

(1) The congressional defense committees.

(2) The Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

(3) The Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(4) The Committee on Agriculture of the House of Representatives and the Committee on Agriculture, Nutrition, and Forestry of the Senate.

(Pub. L. 114–328, div. A, title X, §1086, Dec. 23, 2016, 130 Stat. 2423; Pub. L. 116–92, div. A, title XVII, §1704, Dec. 20, 2019, 133 Stat. 1797.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2017, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2019—Subsec. (d). Pub. L. 116–92 substituted "March 1, 2025" for "March 1, 2019".

STATUTORY NOTES AND RELATED SUBSIDIARIES

ENHANCEMENT OF INTERNATIONAL BIODEFENSE CAPACITY

Pub. L. 119–60, div. A, title XII, §1207, Dec. 18, 2025, 139 Stat. 1082, provided that:

"(a) CLARIFICATION OF ROLES AND RESPONSIBILITIES.—The Secretary of Defense shall direct the Assistant Secretary of Defense for Nuclear Deterrence, Chemical and Biological Defense Programs, in consultation with the Director of the Defense Threat Reduction Agency, to seek to enter into memoranda of understanding with other departments and agencies of the Federal Government to clarify the roles and responsibilities of those departments and agencies for building biodefense capabilities internationally in execution of national security and other policies of the Federal Government, with the Secretary focused on working with defense counterparts in countries that are allies or partners of the United States.

"(b) ELEMENTS OF MEMORANDA OF UNDERSTANDING.—The memoranda of understanding entered into under subsection (a) shall address how each relevant department or agency selects partner countries and the feasibility of coordinating efforts with each such country."

"CONGRESSIONAL DEFENSE COMMITTEES" DEFINED

Congressional defense committees means the Committees on Armed Services and Appropriations of the Senate and the House of Representatives, see section 3 of Pub. L. 114–328, 130 Stat. 2025. See note under section 101 of Title 10, Armed Forces.

§105. Biodefense analysis and budget submission

(a) Annual analysis

For each fiscal year, beginning in fiscal year 2023, the Director of the Office of Management and Budget, in consultation with the Secretary of Health and Human Services shall—

(1) conduct a detailed and comprehensive analysis of Federal biodefense programs; and

(2) develop an integrated biodefense budget submission.

(b) Definition of biodefense

In accordance with the National Biodefense Strategy, the Director shall develop and disseminate to all Federal departments and agencies a unified definition of the term "biodefense" to identify which programs and activities are included in the annual budget submission required under subsection (a).

(c) Requirements for analysis

The analysis required under subsection (a) shall include—

(1) the display of all funds requested for biodefense activities, both mandatory and discretionary, by agency and categorized by biodefense enterprise element, such as threat awareness, prevention, deterrence, preparedness, surveillance and detection, response, attribution (including bioforensic capabilities), recovery, and mitigation; and

(2) detailed explanations of how each program and activity included aligns with biodefense goals and objectives as part of the National Biodefense Strategy required under section 104 of this title.

(d) Submittal to Congress

The Director, in consultation with the Secretary of Health and Human Services, shall submit to Congress the analysis required under subsection (a) for a fiscal year concurrently with the President's annual budget request for that fiscal year.

(Pub. L. 116–283, div. A, title III, §363, Jan. 1, 2021, 134 Stat. 3547.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§106. Update of national biodefense implementation plan

(a) In general

The Secretaries of Health and Human Services, Defense, Agriculture, Homeland Security, and all other Departments and agencies with responsibilities for biodefense, such as the Department of State, in consultation with the Assistant to the President for National Security Affairs and the Director of the Office of Management and Budget, as appropriate, shall jointly, after reviewing the biodefense threat assessment described in subsection (d) and any relevant input from external stakeholders, as appropriate, update the National Biodefense Implementation Plan developed under section 104 of this title to clearly document established processes, roles, and responsibilities related to the National Biodefense Strategy.

(b) Specific updates

The updated National Biodefense Implementation Plan shall—

(1) describe the roles and responsibilities of the Federal departments and agencies, including internal and external coordination procedures, in identifying and sharing information between and among Federal departments and agencies, as described in section 104(b)(4) of this title and consistent with the statutory roles and authorities of such departments and agencies;

(2) describe roles, responsibilities, and processes for decisionmaking, including decisions regarding use of resources for effective risk management across the enterprise;

(3) describe resource plans for each department and agency with responsibility for biodefense to support implementation of the strategy within the jurisdiction of such department or agency, including for the Biodefense Coordination Team, as appropriate;

(4) describe guidance and methods for analyzing the data collected from agencies to include non-Federal resources and capabilities to the extent practicable; and

(5) describe and update, as appropriate, short-, medium-, and long-term goals for executing the National Biodefense Strategy and metrics for meeting each objective of the Strategy.

(c) Submittal to Congress

The Secretary of Health and Human Services, the Secretary of Defense, the Secretary of Agriculture, and the Secretary of Homeland Security shall, not later than 6 months after the date of the completion of the assessment in subsection (d)(1)(A), submit the updated Implementation Plan to the appropriate congressional committees.

(d) Updated biodefense threat assessment

(1) In general

The Secretaries of Health and Human Services, Defense, Agriculture, and Homeland Security, shall jointly, and in consultation with the Director of National Intelligence, and other agency heads as appropriate—

(A) conduct an assessment of current and potential biological threats against the United States, both naturally occurring and man-made, either accidental or deliberate, including the potential for catastrophic biological threats, such as a pandemic;

(B) not later than 1 year after January 1, 2021, submit the findings of the assessment conducted under subparagraph (A) to the Federal officials described in subsection (d)(1)and [1] the appropriate congressional committees described in subsection (e);

(C) not later than 30 days after the date on which the assessment is submitted under subparagraph (B), conduct a briefing for the appropriate congressional committees on the findings of the assessment;

(D) update the assessment under subparagraph (A) biennially, as appropriate, and provide the findings of such updated assessments to the Federal officials described in subsection (d)(1) and the appropriate congressional committees; and

(E) conduct briefings for the appropriate congressional committees as needed any time an assessment under this paragraph is updated.

(2) Classification and format

Assessments under paragraph (1) shall be submitted in an unclassified format and include a classified annex, as appropriate.

(e) Appropriate congressional committees defined

In this section, the term "appropriate congressional committees" means the following:

(1) The Committees on Armed Services of the House of Representatives and the Senate.

(2) The Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

(3) The Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(4) The Committee on Agriculture of the House of Representatives and the Committee on Agriculture, Nutrition, and Forestry of the Senate.

(5) The Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

(6) The Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate.

(f) Rule of construction

Nothing in this section shall be construed to alter, limit, or duplicate the roles, responsibilities, authorities, or current activities, as established in statute or otherwise through existing practice or policy, of each Federal department or agency with responsibilities for biodefense or otherwise relevant to implementation of the National Biodefense Strategy.

(Pub. L. 116–283, div. A, title III, §364, Jan. 1, 2021, 134 Stat. 3548.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *So in original.*

SUBCHAPTER I—DEPARTMENT OF HOMELAND SECURITY

§111. Executive department; mission

(a) Establishment

There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5.

(b) Mission

(1) In general

The primary mission of the Department is to—

(A) prevent terrorist attacks within the United States;

(B) reduce the vulnerability of the United States to terrorism;

(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;

(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;

(E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;

(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland;

(G) ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland; and

(H) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

(2) Responsibility for investigating and prosecuting terrorism

Except as specifically provided by law with respect to entities transferred to the Department under this chapter, primary responsibility for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies

with jurisdiction over the acts in question.

(Pub. L. 107–296, title I, §101, Nov. 25, 2002, 116 Stat. 2142; Pub. L. 108–458, title VIII, §8302, Dec. 17, 2004, 118 Stat. 3867.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (b)(2), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2004—Subsec. (b)(1)(G), (H). Pub. L. 108–458 added subpar. (G) and redesignated former subpar. (G) as (H).

STATUTORY NOTES AND RELATED SUBSIDIARIES

TRANSFER OF CERTAIN OPM AUTHORITY TO DEPARTMENT OF HOMELAND SECURITY

Pub. L. 109–295, title V, §513, Oct. 4, 2006, 120 Stat. 1378, provided that: "Notwithstanding any other provision of law, the authority of the Office of Personnel Management to conduct personnel security and suitability background investigations, update investigations, and periodic reinvestigations of applicants for, or appointees in, positions in the Office of the Secretary and Executive Management, the Office of the Under Secretary for Management, Analysis and Operations, Immigration and Customs Enforcement, the Directorate for Preparedness, and the Directorate of Science and Technology of the Department of Homeland Security is transferred to the Department of Homeland Security: *Provided*, That on request of the Department of Homeland Security, the Office of Personnel Management shall cooperate with and assist the Department in any investigation or reinvestigation under this section: *Provided further*, That this section shall cease to be effective at such time as the President has selected a single agency to conduct security clearance investigations pursuant to section 3001(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 50 U.S.C. 435b [now 50 U.S.C. 3341]) and the entity selected pursuant to section 3001(b) of such Act has reported to Congress that the agency selected pursuant to such section 3001(c) is capable of conducting all necessary investigations in a timely manner or has authorized the entities within the Department of Homeland Security covered by this section to conduct their own investigations pursuant to section 3001 of such Act."

[For transfer of all functions, personnel, assets, components, authorities, grant programs, and liabilities of the Directorate for Preparedness, as constituted on June 1, 2006, including the functions of the Under Secretary for Preparedness relating thereto, to the Federal Emergency Management Agency, with certain exceptions, see section 315(a)(2), (b) of this title.]

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 109–90, title V, §516, Oct. 18, 2005, 119 Stat. 2084.

Pub. L. 108–334, title V, §518, Oct. 18, 2004, 118 Stat. 1318.

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13286. AMENDMENT OF EXECUTIVE ORDERS, AND OTHER ACTIONS, IN CONNECTION WITH THE TRANSFER OF CERTAIN FUNCTIONS TO THE SECRETARY OF HOMELAND SECURITY

Ex. Ord. No. 13286, Feb. 28, 2003, 68 F.R. 10619, as amended by Ex. Ord. No. 13442, §1, Aug. 13, 2007, 72 F.R. 45877; Ex. Ord. No. 13753, §1, Dec. 9, 2016, 81 F.R. 90667; Ex. Ord. No. 14135, §3(b), Jan. 3, 2025, 90 F.R. 2579, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Homeland Security Act of 2002 (Public Law 107–296) [see Tables for classification] and section 301 of title 3, United States Code, and in order to reflect the transfer of certain functions to, and other

responsibilities vested in, the Secretary of Homeland Security, the transfer of certain agencies and agency components to the Department of Homeland Security, and the delegation of appropriate responsibilities to the Secretary of Homeland Security, it is hereby ordered as follows:

SECTION 1. [Amended Ex. Ord. No. 13276, set out as a note under section 1182 of Title 8, Aliens and Nationality.]

SEC. 2. [Amended Ex. Ord. No. 13274, set out as a note under section 301 of Title 49, Transportation.]

SEC. 3. [Amended Ex. Ord. No. 13271, formerly set out as a note under section 509 of Title 28, Judiciary and Judicial Procedure.]

SEC. 4. [Amended and revoked Ex. Ord. No. 13260, set out as a note under section 3021 of Title 50, War and National Defense.]

SEC. 5. [Amended Ex. Ord. No. 13257, set out as a note under section 7103 of Title 22, Foreign Relations and Intercourse.]

SEC. 6. [Amended Ex. Ord. No. 13254, set out as a note under section 12501 of Title 42, The Public Health and Welfare.]

SEC. 7. [Amended Ex. Ord. No. 13231, set out as a note under section 121 of this title.]

SEC. 8. [Amended Ex. Ord. No. 13228, set out as a note under section 3021 of Title 50, War and National Defense.]

SEC. 9. [Amended Ex. Ord. No. 13223, set out as a note under section 12302 of Title 10, Armed Forces.]

SEC. 10. [Amended Ex. Ord. No. 13212, set out as a note under section 13201 of Title 42, The Public Health and Welfare.]

SEC. 11. [Amended Ex. Ord. No. 13165, set out as a note under section 1701 of Title 21, Food and Drugs.]

SEC. 12. [Amended Ex. Ord. No. 13154.]

SEC. 13. [Amended Ex. Ord. No. 13133.]

SEC. 14. [Amended Ex. Ord. No. 13120, set out as a note under section 12304 of Title 10, Armed Forces.]

SEC. 15. [Amended Ex. Ord. No. 13112, set out as a note under section 4321 of Title 42, The Public Health and Welfare.]

SEC. 16. [Amended Ex. Ord. No. 13100, set out as a note under section 341 of Title 21, Food and Drugs.]

SEC. 17. [Amended Ex. Ord. No. 13076, set out as a note under section 12304 of Title 10, Armed Forces.]

SEC. 18. [Amended Ex. Ord. No. 13011, set out as a note under section 11101 of Title 40, Public Buildings, Property, and Works.]

SEC. 19. [Amended Ex. Ord. No. 12989, set out as a note under section 1324a of Title 8, Aliens and Nationality.]

SEC. 20. [Amended Ex. Ord. No. 12985, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 21. [Amended Ex. Ord. No. 12982, set out as a note under section 12304 of Title 10, Armed Forces.]

SEC. 22. [Amended Ex. Ord. No. 12978, listed in a table under section 1701 of Title 50, War and National Defense.]

SEC. 23. [Amended Ex. Ord. No. 12977, set out as a note under section 121 of Title 40, Public Buildings, Property, and Works.]

SEC. 24. [Amended Ex. Ord. No. 12919, formerly set out as a note under section 2153 of the former Appendix to Title 50, War and National Defense.]

SEC. 25. [Amended Ex. Ord. No. 12906, set out as a note under section 1457 of Title 43, Public Lands.]

SEC. 26. [Amended Ex. Ord. No. 12870, set out as a note under section 4727 of Title 15, Commerce and Trade.]

SEC. 27. [Amended Ex. Ord. No. 12835, set out as a note under section 1023 of Title 15, Commerce and Trade.]

SEC. 28. [Amended Ex. Ord. No. 12830, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 29. [Amended Ex. Ord. No. 12824, set out as a note under section 2736 of Title 14, Coast Guard.]

SEC. 30. [Amended Ex. Ord. No. 12807, set out as a note under section 1182 of Title 8, Aliens and Nationality.]

SEC. 31. [Amended Ex. Ord. No. 12793, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 32. [Amended Ex. Ord. No. 12789, set out as a note under section 1364 of Title 8, Aliens and Nationality.]

SEC. 33. [Amended Ex. Ord. No. 12788, set out as a note under section 2391 of Title 10, Armed Forces.]

SEC. 34. [Amended Ex. Ord. No. 12777, set out as a note under section 1321 of Title 33, Navigation and Navigable Waters.]

SEC. 35. [Amended Ex. Ord. No. 12743, formerly set out as a note under section 12302 of Title 10, Armed Forces.]

SEC. 36. [Amended Ex. Ord. No. 12742, set out as a note under section 82 of Title 50, War and National Defense.]

SEC. 37. [Amended Ex. Ord. No. 12733, set out as a note under section 12304 of Title 10, Armed Forces.]

SEC. 38. [Amended Ex. Ord. No. 12728, set out as a note under section 12305 of Title 10, Armed Forces.]

SEC. 39. [Amended Ex. Ord. No. 12727, set out as a note under section 12304 of Title 10, Armed Forces.]

SEC. 40. [Amended Ex. Ord. No. 12699, set out as a note under section 7704 of Title 42, The Public Health and Welfare.]

SEC. 41. [Amended Ex. Ord. No. 12657, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

SEC. 42. [(a) to (i) amended Ex. Ord. No. 12656, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

Without prejudice to subsections (a) through (i) of this section, all responsibilities assigned to specific Federal officials pursuant to Executive Order 12656 that are substantially the same as any responsibility assigned to, or function transferred to, the Secretary of Homeland Security pursuant to the Homeland Security Act of 2002 (regardless of whether such responsibility or function is expressly required to be carried out through another official of the Department of Homeland Security or not pursuant to such Act), or intended or required to be carried out by an agency or an agency component transferred to the Department of Homeland Security pursuant to such Act, are hereby reassigned to the Secretary of Homeland Security.

SEC. 43. [Amended Ex. Ord. No. 12580, set out as a note under section 9615 of Title 42, The Public Health and Welfare.]

SEC. 44. [Amended Ex. Ord. No. 12555, set out as a note under section 2602 of Title 19, Customs Duties.]

SEC. 45. [Amended Ex. Ord. No. 12501, set out as a note under section 4101 of Title 15, Commerce and Trade.]

SEC. 46. [Amended Ex. Ord. No. 12472, formerly set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

SEC. 47. [Amended Ex. Ord. No. 12382, set out as a note under section 901 of Title 47, Telecommunications.]

SEC. 48. [Amended Ex. Ord. No. 12341, set out as a note under section 1522 of Title 8, Aliens and Nationality.]

SEC. 49. [Amended Ex. Ord. No. 12208, set out as a note under section 1157 of Title 8, Aliens and Nationality.]

SEC. 50. [Amended Ex. Ord. No. 12188, set out as a note under section 2171 of Title 19, Customs Duties.]

SEC. 51. [Amended Ex. Ord. No. 12160, set out as a note under section 3501 of Title 42, The Public Health and Welfare.]

SEC. 52. [Amended Ex. Ord. No. 12148, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

SEC. 53. [Amended Ex. Ord. No. 12146, set out as a note under section 509 of Title 28, Judiciary and Judicial Procedures.]

SEC. 54. [Amended Ex. Ord. No. 12002, set out as a note under former section 4603 of Title 50, War and National Defense.]

SEC. 55. [Amended Ex. Ord. No. 11965, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 56. [Amended Ex. Ord. No. 11926, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 57. [Amended Ex. Ord. No. 11858, set out as a note under section 4565 of Title 50, War and National Defense.]

SEC. 58. [Amended Ex. Ord. No. 11800, formerly set out as a note under section 301a of Title 37, Pay and Allowances of the Uniformed Services.]

SEC. 59. [Amended Ex. Ord. No. 11645, set out as a note under section 2943 of Title 14, Coast Guard.]

SEC. 60. [Amended Ex. Ord. No. 11623, set out as a note under section 3809 of Title 50, War and National Defense.]

SEC. 61. [Amended Ex. Ord. No. 11448, set out as a note preceding section 1121 of Title 10, Armed Forces.]

SEC. 62. [Amended Ex. Ord. No. 11446, set out as a note under section 7342 of Title 5, Government Organization and Employees.]

SEC. 63. [Amended Ex. Ord. No. 11438, set out as a note under section 1124 of Title 10, Armed Forces.]

SEC. 64. [Amended Ex. Ord. No. 11366, set out as a note under section 12303 of Title 10, Armed Forces.]

SEC. 65. [Amended Ex. Ord. No. 11239, set out as a note under former section 1051 of Title 33, Navigation and Navigable Waters.]

SEC. 66. [Amended Ex. Ord. No. 11231.]

SEC. 67. [Amended Ex. Ord. No. 11190, set out as a note under section 10149 of Title 10, Armed Forces.]

SEC. 68. [Amended Ex. Ord. No. 11139.]

SEC. 69. [Amended Ex. Ord. No. 11079, set out as a note under section 2603 of Title 10, Armed Forces.]

SEC. 70. [Amended Ex. Ord. No. 11046, set out as a note under section 7276 of Title 10, Armed Forces.]

SEC. 71. [Amended Ex. Ord. No. 11016, set out as a note under section 1129 of Title 10, Armed Forces.]

SEC. 72. [Amended Ex. Ord. No. 10977.]

SEC. 73. [Amended Ex. Ord. No. 10789, set out as a note under section 1431 of Title 50, War and National Defense.]

SEC. 74. [Amended Ex. Ord. No. 10694.]

SEC. 75. [Amended Ex. Ord. No. 10637, set out as a note under section 301 of Title 3, The President.]

SEC. 76. [Amended Ex. Ord. No. 10631, set out as a note under section 802 of Title 10, Armed Forces.]

SEC. 77. [Amended Ex. Ord. No. 10554, set out as a note under section 772 of Title 10, Armed Forces.]

SEC. 78. [Amended Ex. Ord. No. 10499.]

SEC. 79. [Amended Ex. Ord. No. 10448.]

SEC. 80. [Amended Ex. Ord. No. 10271, set out as a note under section 3819 of Title 50, War and National Defense.]

SEC. 81. [Amended Ex. Ord. No. 10179.]

SEC. 82. [Amended Ex. Ord. No. 10163.]

SEC. 83. [Amended Ex. Ord. No. 10113, set out as a note under section 418 of Title 37, Pay and Allowances of the Uniformed Services.]

SEC. 84. [Amended Ex. Ord. No. 4601.]

SEC. 85. *Designation as a Defense Agency of the United States.*

I hereby designate the Department of Homeland Security as a defense agency of the United States for the purposes of chapter 17 of title 35 of the United States Code.

SEC. 86. *Exception from the Provisions of the Government Employees Training Act.*

Those elements of the Department of Homeland Security that are supervised by the Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection through the Department's Assistant Secretary for Information Analysis are, pursuant to section 4102(b)(1) of title 5, United States Code, and in the public interest, excepted from the following provisions of the Government Employees Training Act as codified in title 5: sections 4103(a)(1), 4108, 4115, 4117, and 4118, and that part of 4109(a) that provides "under the regulations prescribed under section 4118(a)(8) of this title and".

SEC. 87. *Functions of Certain Officials in the Coast Guard.*

The Commandant and the Assistant Commandant for Intelligence of the Coast Guard each shall be considered a "Senior Official of the Intelligence Community" for purposes of Executive Order 12333 of December 4, 1981 [50 U.S.C. 3001 note], and all other relevant authorities.

SEC. 88. *Savings Provision.*

Except as otherwise specifically provided above or in Executive Order 13284 of January 23, 2003 ("Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security") [6 U.S.C. 121 note], references in any prior Executive Order relating to an agency or an agency component that is transferred to the Department of Homeland Security ("the Department"), or relating to a function that is transferred to the Secretary of Homeland Security, shall be deemed to refer, as appropriate, to the Department or its officers, employees, agents, organizational units, or functions.

SEC. 89. Nothing in this order shall be construed to impair or otherwise affect the authority of the Secretary of Defense with respect to the Department of Defense, including the chain of command for the armed forces of the United States under section 162(b) of title 10, United States Code, and the authority of the Secretary of Defense with respect to the Department of Defense under section 113(b) of that title.

SEC. 90. Nothing in this order shall be construed to limit or restrict the authorities of the Central Intelligence Agency and the Director of Central Intelligence pursuant to the National Security Act of 1947 [act July 26, 1947, ch. 343; see Tables for classification] and the CIA Act of 1949 [probably means the Central Intelligence Agency Act of 1949, act June 20, 1949, ch. 227; see Tables for classification].

SEC. 91. This order shall become effective on March 1, 2003.

SEC. 92. This order does not create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any

other person.

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a) and (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.]

EXECUTIVE ORDER NO. 13362

Ex. Ord. No. 13362, Nov. 29, 2004, 69 F.R. 70173, which designated additional officers for the Department of Homeland Security order of succession, was revoked by Ex. Ord. No. 13442, §2, Aug. 13, 2007, 72 F.R. 45878.

§112. Secretary; functions

(a) Secretary

(1) In general

There is a Secretary of Homeland Security, appointed by the President, by and with the advice and consent of the Senate.

(2) Head of Department

The Secretary is the head of the Department and shall have direction, authority, and control over it.

(3) Functions vested in Secretary

All functions of all officers, employees, and organizational units of the Department are vested in the Secretary.

(b) Functions

The Secretary—

(1) except as otherwise provided by this chapter, may delegate any of the Secretary's functions to any officer, employee, or organizational unit of the Department;

(2) shall have the authority to make contracts, grants, and cooperative agreements, and to enter into agreements with other executive agencies, as may be necessary and proper to carry out the Secretary's responsibilities under this chapter or otherwise provided by law; and

(3) shall take reasonable steps to ensure that information systems and databases of the Department are compatible with each other and with appropriate databases of other Departments.

(c) Coordination with non-Federal entities

With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination [1] (established under section 361 of this title) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by—

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

(d) Meetings of National Security Council

The Secretary may, subject to the direction of the President, attend and participate in meetings of the National Security Council.

(e) Issuance of regulations

The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, except as specifically provided in this chapter, in laws granting regulatory authorities that are transferred by this chapter, and in laws enacted after November 25, 2002.

(f) Special Assistant to the Secretary

The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) creating and fostering strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland;

(2) advising the Secretary on the impact of the Department's policies, regulations, processes, and actions on the private sector;

(3) interfacing with other relevant Federal agencies with homeland security missions to assess the impact of these agencies' actions on the private sector;

(4) creating and managing private sector advisory councils composed of representatives of industries and associations designated by the Secretary to—

(A) advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges;

(B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations; and

(C) advise the Secretary on private sector preparedness issues, including effective methods for—

(i) promoting voluntary preparedness standards to the private sector; and

(ii) assisting the private sector in adopting voluntary preparedness standards;

(5) working with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions;

(6) promoting existing public-private partnerships and developing new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges;

(7) assisting in the development and promotion of private sector best practices to secure critical infrastructure;

(8) providing information to the private sector regarding voluntary preparedness standards and the business justification for preparedness and promoting to the private sector the adoption of voluntary preparedness standards;

(9) coordinating industry efforts, with respect to functions of the Department of Homeland Security, to identify private sector resources and capabilities that could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack;

(10) coordinating with the Commissioner of U.S. Customs and Border Protection and the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries; and

(11) consulting with the Office of State and Local Government Coordination and Preparedness on all matters of concern to the private sector, including the tourism industry.

(g) Standards policy

All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A–119.

(h) Planning requirements

The Secretary shall ensure the head of each office and component of the Department takes into account the needs of children, including children within under-served communities, in mission

planning and mission execution. In furtherance of this subsection, the Secretary shall require each such head to seek, to the extent practicable, advice and feedback from organizations representing the needs of children. The Federal Advisory Committee Act (5 U.S.C. App.) [2] shall not apply whenever such advice or feedback is sought in accordance with this subsection.

(Pub. L. 107–296, title I, §102, Nov. 25, 2002, 116 Stat. 2142; Pub. L. 108–458, title VII, §7402, Dec. 17, 2004, 118 Stat. 3850; Pub. L. 110–53, title IX, §902, Aug. 3, 2007, 121 Stat. 371; Pub. L. 114–125, title VIII, §802(g)(1)(A)(i), Feb. 24, 2016, 130 Stat. 210; Pub. L. 117–130, §2, June 6, 2022, 136 Stat. 1229.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsecs. (b)(1), (2), and (e), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

Section 12(d) of the National Technology Transfer Advancement Act of 1995, referred to in subsec. (g), probably means section 12(d) of the National Technology Transfer and Advancement Act of 1995, which is section 12(d) of Pub. L. 104–113, and which is set out as a note under section 272 of Title 15, Commerce and Trade.

The Federal Advisory Committee Act, referred to in subsec. (h), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

AMENDMENTS

2022—Subsec. (h). Pub. L. 117–130 added subsec. (h).

2016—Subsec. (f)(10). Pub. L. 114–125 substituted "the Commissioner of U.S. Customs and Border Protection" for "the Directorate of Border and Transportation Security".

2007—Subsec. (f)(4)(C). Pub. L. 110–53, §902(b), added subpar. (C).

Subsec. (f)(8) to (11). Pub. L. 110–53, §902(a), added par. (8) and redesignated former pars. (8) to (10) as (9) to (11), respectively.

2004—Subsec. (f)(8) to (10). Pub. L. 108–458 added pars. (8) to (10).

STATUTORY NOTES AND RELATED SUBSIDIARIES

DAILY PUBLIC REPORT OF COVERED CONTRACT AWARDS

Pub. L. 117–263, div. G, title LXXI, §7113, Dec. 23, 2022, 136 Stat. 3631, provided that:

"(a) DAILY CONTRACT REPORTING REQUIREMENTS.—

"(1) REPORT.—

"(A) IN GENERAL.—The Secretary shall post, maintain, and update in accordance with paragraph (2), on a publicly available website of the Department, a daily report of all covered contract awards.

"(B) CONTENTS.—Each report under this paragraph shall include, for each covered contract award, information relating to the following:

"(i) The contract number, modification number, or delivery order number.

"(ii) The contract type.

"(iii) The amount obligated for the award.

"(iv) The total contract value for the award, including all options.

"(v) The description of the purpose for the award.

"(vi) The number of proposals or bids received.

"(vii) The name and address of the vendor, and whether the vendor is a small business.

"(viii) The period and primary place of performance for the award.

"(ix) Whether the award is multiyear.

"(x) The contracting office.

"(2) UPDATE.—The Secretary shall make updates referred to in paragraph (1) not later than five business days after the date on which a covered contract is authorized or modified.

"(3) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date that is 180 days after the date of the enactment of this Act [Dec. 23, 2022].

"(b) UNDEFINITIZED CONTRACT ACTION OR DEFINITIZED AMOUNT.—If a covered contract award reported under subsection (a) includes an undefinitized contract action, the Secretary shall—

"(1) report the estimated total contract value for the award and the amount obligated upon award; and

"(2) once there is a definitized amount for the award, update the total contract value and amount obligated.

"(c) EXEMPTION.—Each report required under subsection (a) shall not include covered contract awards for which synopsis was exempted under section 5.202(a)(1) of the Federal Acquisition Regulation, or any successor thereto.

"(d) DEFINITIONS.—In this section:

"(1) COVERED CONTRACT AWARD.—The term 'covered contract award'—

"(A) means a contract action of the Department with a total contract value of not less than $4,000,000, including unexercised options; and

"(B) includes—

"(i) contract awards governed by the Federal Acquisition Regulation;

"(ii) modifications to a contract award that increase the total value, expand the scope of work, or extend the period of performance;

"(iii) orders placed on a multiple-award or multiple-agency contract that includes delivery or quantity terms that are indefinite;

"(iv) other transaction authority agreements; and

"(v) contract awards made with other than full and open competition.

"(2) DEFINITIZED AMOUNT.—The term 'definitized amount' means the final amount of a covered contract award after agreement between the Department and the contractor at issue.

"(3) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

"(4) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(5) SMALL BUSINESS.—The term 'small business' means an entity that qualifies as a small business concern, as defined under section 3 of the Small Business Act (15 U.S.C. 632).

"(6) TOTAL CONTRACT VALUE.—The term 'total contract value' means the total amount of funds expected to be provided to the contractor at issue under the terms of the contract through the full period of performance.

"(7) UNDEFINITIZED CONTRACT ACTION.—The term 'undefinitized contract action' means any contract action for which the contract terms, specifications, or price is not established prior to the start of the performance of the covered contract award.

"(e) SUNSET.—This section shall cease to have force or effect on the date that is five years after the date of the enactment of this Act [Dec. 23, 2022]."

REQUIRED COORDINATION

Pub. L. 108–458, title VII, §7405, Dec. 17, 2004, 118 Stat. 3851, provided that: "The Secretary of Homeland Security shall ensure that there is effective and ongoing coordination of Federal efforts to prevent, prepare for, and respond to acts of terrorism and other major disasters and emergencies among the divisions of the Department of Homeland Security, including the Directorate of Emergency Preparedness and Response and the Office for State and Local Government Coordination and Preparedness."

PROTECTIONS FOR HUMAN RESEARCH SUBJECTS OF THE DEPARTMENT OF HOMELAND SECURITY

Pub. L. 108–458, title VIII, §8306, Dec. 17, 2004, 118 Stat. 3869, provided that: "The Secretary of Homeland Security shall ensure that the Department of Homeland Security complies with the protections for human research subjects, as described in part 46 of title 45, Code of Federal Regulations, or in equivalent regulations as promulgated by such Secretary, with respect to research that is conducted or supported by the Department."

[1] So in original. Probably should be "Office for State and Local Government Coordination".

[2] See References in Text note below.

§113. Other officers

(a) Deputy Secretary; Under Secretaries

(1) In general

Except as provided under paragraph (2), there are the following officers, appointed by the President, by and with the advice and consent of the Senate:

(A) A Deputy Secretary of Homeland Security, who shall be the Secretary's first assistant for purposes of subchapter III of chapter 33 of title 5.

(B) An Under Secretary for Science and Technology.

(C) A Commissioner of U.S. Customs and Border Protection.

(D) An Administrator of the Federal Emergency Management Agency.

(E) A Director of the Bureau of Citizenship and Immigration Services.

(F) An Under Secretary for Management, who shall be first assistant to the Deputy Secretary of Homeland Security for purposes of subchapter III of chapter 33 of title 5.

(G) A Director of U.S. Immigration and Customs Enforcement.

(H) A Director of the Cybersecurity and Infrastructure Security Agency.

(I) Not more than 12 Assistant Secretaries.

(J) A General Counsel, who shall be the chief legal officer of the Department.

(K) An Under Secretary for Strategy, Policy, and Plans.

(2) Assistant Secretaries

If any of the Assistant Secretaries referred to under paragraph (1)(I) is designated to be the Assistant Secretary for Health Affairs, the Assistant Secretary for Legislative Affairs, or the Assistant Secretary for Public Affairs, that Assistant Secretary shall be appointed by the President without the advice and consent of the Senate.

(b) Inspector General

There shall be in the Department an Office of Inspector General and an Inspector General at the head of such office, as provided in chapter 4 of title 5.

(c) Commandant of the Coast Guard

To assist the Secretary in the performance of the Secretary's functions, there is a Commandant of the Coast Guard, who shall be appointed as provided in section 44 [1] of title 14 and who shall report directly to the Secretary. In addition to such duties as may be provided in this chapter and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 [1] of title 14.

(d) Other officers

To assist the Secretary in the performance of the Secretary's functions, there are the following officers, appointed by the President:

(1) A Director of the Secret Service.

(2) A Chief Information Officer.

(3) An Officer for Civil Rights and Civil Liberties.

(4) An Assistant Secretary for the Countering Weapons of Mass Destruction Office.

(5) Any Director of a Joint Task Force under section 348 of this title.

(e) Chief Financial Officer

There shall be in the Department a Chief Financial Officer, as provided in chapter 9 of title 31.

(f) Performance of specific functions

Subject to the provisions of this chapter, every officer of the Department shall perform the functions specified by law for the official's office or prescribed by the Secretary.

(g) Vacancies

(1) Absence, disability, or vacancy of Secretary or Deputy Secretary

Notwithstanding chapter 33 of title 5, the Under Secretary for Management shall serve as the Acting Secretary if by reason of absence, disability, or vacancy in office, neither the Secretary nor Deputy Secretary is available to exercise the duties of the Office of the Secretary.

(2) Further order of succession

Notwithstanding chapter 33 of title 5, the Secretary may designate such other officers of the Department in further order of succession to serve as Acting Secretary.

(3) Notification of vacancies

The Secretary shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of any vacancies that require notification under sections 3345 through 3349d of title 5 (commonly known as the "Federal Vacancies Reform Act of 1998").

(Pub. L. 107–296, title I, §103, Nov. 25, 2002, 116 Stat. 2144; Pub. L. 108–7, div. L, §104(a), Feb. 20, 2003, 117 Stat. 529; Pub. L. 108–330, §3(d)(1)(A), Oct. 16, 2004, 118 Stat. 1276; Pub. L. 108–458, title VII, §7407(b), Dec. 17, 2004, 118 Stat. 3853; Pub. L. 109–295, title VI, §612(b), Oct. 4, 2006, 120 Stat. 1410; Pub. L. 109–347, title V, §501(b)(1), Oct. 13, 2006, 120 Stat. 1935; Pub. L. 110–53, title V, §531(b)(2), Aug. 3, 2007, 121 Stat. 334; Pub. L. 110–388, §1, Oct. 10, 2008, 122 Stat. 4144; Pub. L. 112–166, §2(f)(5), Aug. 10, 2012, 126 Stat. 1285; Pub. L. 114–125, title VIII, §802(g)(1)(A)(ii), Feb. 24, 2016, 130 Stat. 211; Pub. L. 114–328, div. A, title XIX, §§1901(a), 1903(a), Dec. 23, 2016, 130 Stat. 2665, 2672; Pub. L. 115–278, §2(g)(1), Nov. 16, 2018, 132 Stat. 4176; Pub. L. 115–387, §2(f)(1), Dec. 21, 2018, 132 Stat. 5168; Pub. L. 117–286, §4(b)(21), Dec. 27, 2022, 136 Stat. 4345.)

EDITORIAL NOTES

REFERENCES IN TEXT

Sections 2 and 44 of title 14, referred to in subsec. (c), redesignated sections 102 and 302, respectively, of title 14 by Pub. L. 115–282, title I, §§103(b), 104(b), Dec. 4, 2018, 132 Stat. 4195, 4196, and references to sections 2 and 44 of title 14 deemed to refer to such redesignated sections, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

This chapter, referred to in subsecs. (c) and (f), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The Federal Vacancies Reform Act of 1998, referred to in subsec. (g)(3), is section 151(a) of title I of div. C of Pub. L. 105–277, Oct. 21, 1998, 112 Stat. 2681–611, which enacted sections 3345 to 3349d of Title 5, Government Organization and Employees, repealed former sections 3345 to 3349 of Title 5, and enacted provisions set out as a note under section 3345 of Title 5. For complete classification of this Act to the Code, see Short Title of 1998 Amendment note set out under section 3301 of Title 5 and Tables.

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–286 substituted "chapter 4 of title 5." for "the Inspector General Act of 1978 (5 U.S.C. App.)."

2018—Subsec. (a)(1)(H). Pub. L. 115–278 amended subpar. (H) generally. Prior to amendment, subpar. (H) read as follows: "An Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department."

Subsec. (d)(4). Pub. L. 115–387 substituted "An Assistant Secretary for the Countering Weapons of Mass Destruction Office" for "A Director for Domestic Nuclear Detection".

2016—Subsec. (a)(1)(C). Pub. L. 114–125, §802(g)(1)(A)(ii)(I), substituted "A Commissioner of U.S. Customs and Border Protection." for "An Under Secretary for Border and Transportation Security."

Subsec. (a)(1)(F). Pub. L. 114–328, §1903(a)(1)(A), inserted ", who shall be first assistant to the Deputy Secretary of Homeland Security for purposes of subchapter III of chapter 33 of title 5" before period at end.

Subsec. (a)(1)(G). Pub. L. 114–125, §802(g)(1)(A)(ii)(II), substituted "A Director of U.S. Immigration and

Customs Enforcement." for "A Director of the Office of Counternarcotics Enforcement."

Subsec. (a)(1)(K). Pub. L. 114–328, §1903(a)(1)(B), added subpar. (K).

Subsec. (d)(5). Pub. L. 114–328, §1901(a), added par. (5).

Subsec. (g). Pub. L. 114–328, §1903(a)(2), added subsec. (g).

2012—Subsec. (a). Pub. L. 112–166 redesignated introductory provisions as introductory provisions of par. (1), inserted par. (1) heading, substituted "Except as provided under paragraph (2), there" for "There", redesignated pars. (1) to (10) as subpars. (A) to (J), respectively, of par. (1), and added par. (2).

2008—Subsec. (d)(3) to (5). Pub. L. 110–388 redesignated pars. (4) and (5) as (3) and (4), respectively, and struck out former par. (3) which read as follows: "A Chief Human Capital Officer."

2007—Subsec. (a)(8) to (10). Pub. L. 110–53 added par. (8) and redesignated former pars. (8) and (9) as (9) and (10), respectively.

2006—Subsec. (a)(2) to (4). Pub. L. 109–295, §612(b)(2), (3), redesignated pars. (3) to (5) as (2) to (4), respectively, and struck out former par. (2) which read as follows: "An Under Secretary for Information Analysis and Infrastructure Protection."

Subsec. (a)(5). Pub. L. 109–295, §612(b)(3), redesignated par. (6) as (5). Former par. (5) redesignated (4).

Pub. L. 109–295, §612(b)(1), added par. (5) and struck out former par. (5) which read as follows: "An Under Secretary for Emergency Preparedness and Response."

Subsec. (a)(6) to (10). Pub. L. 109–295, §612(b)(3), redesignated pars. (7) to (10) as (6) to (9), respectively. Former par. (6) redesignated (5).

Subsec. (d)(5). Pub. L. 109–347 added par. (5).

2004—Subsec. (a)(8) to (10). Pub. L. 108–458 added par. (8) and redesignated former pars. (8) and (9) as (9) and (10), respectively.

Subsec. (d)(4), (5). Pub. L. 108–330, §3(d)(1)(A)(i), redesignated par. (5) as (4) and struck out former par. (4) which read as follows: "A Chief Financial Officer."

Subsecs. (e), (f). Pub. L. 108–330, §3(d)(1)(A)(ii), (iii), added subsec. (e) and redesignated former subsec. (e) as (f).

2003—Subsec. (b). Pub. L. 108–7 reenacted heading without change and amended text generally. Prior to amendment, text read as follows: "There is an Inspector General, who shall be appointed as provided in section 3(a) of the Inspector General Act of 1978."

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

EFFECTIVE DATE OF 2012 AMENDMENT

Pub. L. 112–166, §6(a), Aug. 10, 2012, 126 Stat. 1295, provided that: "The amendments made by section 2 [see Tables for classification] shall take effect 60 days after the date of enactment of this Act [Aug. 10, 2012] and apply to appointments made on and after that effective date, including any nomination pending in the Senate on that date."

UNDER SECRETARY RESPONSIBLE FOR OVERSEEING CRITICAL INFRASTRUCTURE PROTECTION, CYBERSECURITY AND RELATED PROGRAMS AUTHORIZED TO SERVE AS DIRECTOR OF CYBERSECURITY AND INFRASTRUCTURE SECURITY

For authorization of individual serving as Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity and related programs on the day before Nov. 16, 2018, to continue to serve as Director of Cybersecurity and Infrastructure Security on and after such date, see section 2(b)(1) of Pub. L. 115–278, Nov. 16, 2018, 132 Stat. 4175, set out as a note under section 652 of this title.

[1] *See References in Text note below.*

§114. Sensitive Security Information

Using funds made available in this Act, the Secretary of Homeland Security shall provide that each office within the Department that handles documents marked as Sensitive Security Information (SSI) shall have at least one employee in that office with authority to coordinate and make determinations on behalf of the agency that such documents meet the criteria for marking as SSI: *Provided*, That not later than December 31, 2005, the Secretary shall submit to the Committees on Appropriations of the Senate and the House of Representatives: (1) Department-wide policies for designating, coordinating and marking documents as SSI; (2) Department-wide auditing and accountability procedures for documents designated and marked as SSI; (3) the total number of SSI Coordinators within the Department; and (4) the total number of staff authorized to designate SSI documents within the Department: *Provided further*, That not later than January 31, 2006, the Secretary shall provide to the Committees on Appropriations of the Senate and the House of Representatives the title of all DHS documents that are designated as SSI in their entirety during the period October 1, 2005, through December 31, 2005: *Provided further*, That not later than January 31 of each succeeding year, starting on January 31, 2007, the Secretary shall provide annually a similar report to the Committees on Appropriations of the Senate and the House of Representatives on the titles of all DHS documents that are designated as SSI in their entirety during the period of January 1 through December 31 for the preceding year: *Provided further*, That the Secretary shall promulgate guidance that includes common but extensive examples of SSI that further define the individual categories of information cited under 49 CFR 1520(b)(1) through (16) and eliminates judgment by covered persons in the application of the SSI marking: *Provided further*, That such guidance shall serve as the primary basis and authority for the marking of DHS information as SSI by covered persons.

(Pub. L. 109–90, title V, §537, Oct. 18, 2005, 119 Stat. 2088.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in text, is Pub. L. 109–90, Oct. 18, 2005, 119 Stat. 2064, known as the Department of Homeland Security Appropriations Act, 2006. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2006, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

APPLICABILITY OF THIRD PROVISO

Pub. L. 114–113, div. F, title V, §510(b), Dec. 18, 2015, 129 Stat. 2514, provided that: "The third proviso of section 537 of the Department of Homeland Security Appropriations Act, 2006 (6 U.S.C. 114), shall hereafter not apply with respect to funds made available in this or any other Act."

TSA SENSITIVE SECURITY INFORMATION

Pub. L. 117–81, div. F, title LXIV, §6423(a), Dec. 27, 2021, 135 Stat. 2419, provided that:

"(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 27, 2021], the Administrator of the Transportation Security Administration (TSA) shall—

"(A) ensure clear and consistent designation of 'Sensitive Security Information', including reasonable security justifications for such designation;

"(B) develop and implement a schedule to regularly review and update, as necessary, TSA Sensitive Security Information identification guidelines;

"(C) develop a tracking mechanism for all Sensitive Security Information redaction and designation challenges;

"(D) document justifications for changes in position regarding Sensitive Security Information redactions and designations, and make such changes accessible to TSA personnel for use with relevant stakeholders, including air carriers, airport operators, surface transportation operators, and State and local law enforcement, as necessary; and

"(E) ensure that TSA personnel are adequately trained on appropriate designation policies.

"(2) STAKEHOLDER OUTREACH.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall conduct outreach to relevant stakeholders described in paragraph (1)(D) that regularly are granted access to Sensitive Security Information to raise awareness of the TSA's policies and guidelines governing the designation and use of Sensitive Security Information."

§115. Trade and customs revenue functions of the Department

(a) Trade and customs revenue functions

(1) Designation of appropriate official

The Secretary shall designate an appropriate senior official in the office of the Secretary who shall—

(A) ensure that the trade and customs revenue functions of the Department are coordinated within the Department and with other Federal departments and agencies, and that the impact on legitimate trade is taken into account in any action impacting the functions; and

(B) monitor and report to Congress on the Department's mandate to ensure that the trade and customs revenue functions of the Department are not diminished, including how spending, operations, and personnel related to these functions have kept pace with the level of trade entering the United States.

(2) Director of Trade Policy

There shall be a Director of Trade Policy (in this subsection referred to as the "Director"), who shall be subject to the direction and control of the official designated pursuant to paragraph (1). The Director shall—

(A) advise the official designated pursuant to paragraph (1) regarding all aspects of Department policies relating to the trade and customs revenue functions of the Department;

(B) coordinate the development of Department-wide policies regarding trade and customs revenue functions and trade facilitation; and

(C) coordinate the trade and customs revenue-related policies of the Department with the policies of other Federal departments and agencies.

(b) Study; report

(1) In general

The Comptroller General of the United States shall conduct a study evaluating the extent to which the Department of Homeland Security is meeting its obligations under section 212(b) of this title with respect to the maintenance of customs revenue functions.

(2) Analysis

The study shall include an analysis of—

(A) the extent to which the customs revenue functions carried out by the former United States Customs Service have been consolidated with other functions of the Department (including the assignment of noncustoms revenue functions to personnel responsible for customs revenue collection), discontinued, or diminished following the transfer of the United States Customs Service to the Department;

(B) the extent to which staffing levels or resources attributable to customs revenue functions have decreased since the transfer of the United States Customs Service to the Department; and

(C) the extent to which the management structure created by the Department ensures effective trade facilitation and customs revenue collection.

(3) Report

Not later than 180 days after October 13, 2006, the Comptroller General shall submit to the appropriate congressional committees a report on the results of the study conducted under subsection (a).

(4) Maintenance of functions

Not later than September 30, 2007, the Secretary shall ensure that the requirements of section 212(b) of this title are fully satisfied and shall report to the Committee on Finance of the Senate and the Committee on Ways and Means of the House of Representatives regarding implementation of this paragraph.

(5) Definition

In this section, the term "customs revenue functions" means the functions described in section 212(b)(2) of this title.

(c) Consultation on trade and customs revenue functions

(1) Business community consultations

The Secretary shall consult with representatives of the business community involved in international trade, including seeking the advice and recommendations of the Commercial Operations Advisory Committee, not later than 30 days after proposing, and not later than 30 days before finalizing, any Department policies, initiatives, or actions that will have a significant impact on international trade and customs revenue functions.

(2) Congressional consultation and notification

(A) In general

Subject to subparagraph (B), the Secretary shall notify the appropriate congressional committees not later than 60 days before proposing, and not later than 60 days before finalizing, any Department policies, initiatives, or actions that will have a major impact on trade and customs revenue functions. Such notifications shall include a description of the proposed policies, initiatives, or actions and any comments or recommendations provided by the Commercial Operations Advisory Committee and other relevant groups regarding the proposed policies, initiatives, or actions.

(B) Exception

If the Secretary determines that it is important to the national security interest of the United States to finalize any Department policies, initiatives, or actions prior to the consultation described in subparagraph (A), the Secretary shall—

(i) notify and provide any recommendations of the Commercial Operations Advisory Committee received to the appropriate congressional committees not later than 45 days after the date on which the policies, initiatives, or actions are finalized; and

(ii) to the extent appropriate, modify the policies, initiatives, or actions based upon the consultations with the appropriate congressional committees.

(d) Notification of reorganization of customs revenue functions

(1) In general

Not less than 45 days prior to any change in the organization of any of the customs revenue functions of the Department, the Secretary shall notify the Committee on Appropriations, the Committee on Finance, and the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Appropriations, the Committee on Homeland Security, and the Committee on Ways and Means of the House of Representatives of the specific assets, functions, or personnel to be transferred as part of such reorganization, and the reason for such transfer. The notification shall also include—

(A) an explanation of how trade enforcement functions will be impacted by the reorganization;

(B) an explanation of how the reorganization meets the requirements of section 212(b) of this title that the Department not diminish the customs revenue and trade facilitation functions formerly performed by the United States Customs Service; and

(C) any comments or recommendations provided by the Commercial Operations Advisory Committee regarding such reorganization.

(2) Analysis

Any congressional committee referred to in paragraph (1) may request that the Commercial Operations Advisory Committee provide a report to the committee analyzing the impact of the reorganization and providing any recommendations for modifying the reorganization.

(3) Report

Not later than 1 year after any reorganization referred to in paragraph (1) takes place, the Secretary, in consultation with the Commercial Operations Advisory Committee, shall submit a report to the Committee on Finance of the Senate and the Committee on Ways and Means of the House of Representatives. Such report shall include an assessment of the impact of, and any suggested modifications to, such reorganization.

(Pub. L. 109–347, title IV, §401, Oct. 13, 2006, 120 Stat. 1921; Pub. L. 114–125, title IX, §902, Feb. 24, 2016, 130 Stat. 223.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2016—Subsec. (c)(1). Pub. L. 114–125, §902(1), substituted "not later than 30 days after proposing, and not later than 30 days before finalizing, any Department policies, initiatives, or actions that will have" for "on Department policies and actions that have".

Subsec. (c)(2)(A). Pub. L. 114–125, §902(2), substituted "not later than 60 days before proposing, and not later than 60 days before finalizing," for "not later than 30 days prior to the finalization of".

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of terms used in this section, see section 901 of this title.

SUBCHAPTER II—INFORMATION ANALYSIS

EDITORIAL NOTES

CODIFICATION

Pub. L. 115–278, §2(g)(2)(A), Nov. 16, 2018, 132 Stat. 4176, struck out "AND INFRASTRUCTURE PROTECTION" after "INFORMATION ANALYSIS" in subchapter heading.

PART A—INFORMATION AND ANALYSIS; ACCESS TO INFORMATION

EDITORIAL NOTES

CODIFICATION

Pub. L. 115–278, §2(g)(2)(B), Nov. 16, 2018, 132 Stat. 4177, struck out "and Infrastructure Protection" after "Information and Analysis" in part heading.

Pub. L. 110–53, title V, §531(b)(3), Aug. 3, 2007, 121 Stat. 334, substituted "Information and" for "Directorate for Information" in part heading.

§121. Information and Analysis

(a) Intelligence and analysis

There shall be in the Department an Office of Intelligence and Analysis.

(b) Under Secretary for Intelligence and Analysis

(1) Office of Intelligence and Analysis

The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) Chief Intelligence Officer

The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

(c) Discharge of responsibilities

The Secretary shall ensure that the responsibilities of the Department relating to information analysis, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis.

(d) Responsibilities of Secretary relating to intelligence and analysis

The responsibilities of the Secretary relating to intelligence and analysis shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 [50 U.S.C. 3056], in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State,[1] and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.

(4) To ensure, pursuant to section 122 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing

environment established under section 485 of this title, including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

(6) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(7) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(8) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(9) To ensure that—

(A) any material received pursuant to this chapter is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this chapter is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 [50 U.S.C. 3001 et seq.] and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(10) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(11) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(12) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(13) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(14) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

(15) To provide intelligence and information analysis and support to other elements of the Department.

(16) To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.

(17) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence.

(18) To establish a structure and process to support the missions and goals of the intelligence components of the Department.

(19) To ensure that, whenever possible, the Department—

(A) produces and disseminates unclassified reports and analytic products based on open-source information; and

(B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.

(20) To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.

(21) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—

(A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and

(B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.

(22) To perform such other duties relating to such responsibilities as the Secretary may provide.

(23)(A) Not later than six months after December 23, 2016, to conduct an intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure, and submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate—

(i) a recommended strategy to protect and prepare the critical infrastructure of the homeland against threats of EMP and GMD; and

(ii) not less frequently than every two years thereafter for the next six years, updates of the recommended strategy.

(B) The recommended strategy under subparagraph (A) shall—

(i) be based on findings of the research and development conducted under section 195f of this title;

(ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Presidential Policy Directive-21) for critical infrastructure;

(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructure;

(iv) be informed, to the extent practicable, by the findings of the intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure conducted under subparagraph (A); and

(v) be submitted in unclassified form, but may include a classified annex.

(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism, cyber attacks, and other threats if, as incorporated, the recommended strategy complies with subparagraph (B).

(e) Staff

(1) In general

The Secretary shall provide the Office of Intelligence and Analysis with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section.

(2) Private sector analysts

Analysts under this subsection may include analysts from the private sector.

(3) Security clearances

Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) Detail of personnel

(1) In general

In order to assist the Office of Intelligence and Analysis in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) Covered agencies

The agencies referred to in this paragraph are as follows:

(A) The Department of State.
(B) The Central Intelligence Agency.
(C) The Federal Bureau of Investigation.
(D) The National Security Agency.
(E) The National Geospatial-Intelligence Agency.
(F) The Defense Intelligence Agency.
(G) Any other agency of the Federal Government that the President considers appropriate.

(3) Cooperative agreements

The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) Basis

The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) Functions transferred

In accordance with subchapter XII, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

(Pub. L. 107–296, title II, §201, Nov. 25, 2002, 116 Stat. 2145; Pub. L. 110–53, title V, §§501(a)(2)(A), (b), 531(a), title X, §1002(a), Aug. 3, 2007, 121 Stat. 309, 332, 374; Pub. L. 110–417, [div. A], title IX, §931(b)(5), Oct. 14, 2008, 122 Stat. 4575; Pub. L. 111–84, div. A, title X, §1073(c)(9), Oct. 28, 2009, 123 Stat. 2475; Pub. L. 111–258, §5(b)(1), Oct. 7, 2010, 124 Stat. 2650;

Pub. L. 114–328, div. A, title XIX, §1913(a)(2), Dec. 23, 2016, 130 Stat. 2685; Pub. L. 115–278, §2(g)(2)(C), Nov. 16, 2018, 132 Stat. 4177.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (d)(9), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The National Security Act of 1947, referred to in subsec. (d)(9)(B), is act July 26, 1947, ch. 343, 61 Stat. 495, which was formerly classified principally to chapter 15 (§401 et seq.) of Title 50, War and National Defense, prior to editorial reclassification in Title 50, and is now classified principally to chapter 44 (§3001 et seq.) of Title 50. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section is comprised of section 201 of Pub. L. 107–296. Subsec. (h) of section 201 of Pub. L. 107–296 amended section 3003 of Title 50, War and National Defense.

AMENDMENTS

2018—Pub. L. 115–278, §2(g)(2)(C)(i), struck out "and Infrastructure Protection" after "Information and Analysis" in section catchline.

Subsec. (a). Pub. L. 115–278, §2(g)(2)(C)(ii), struck out "and infrastructure protection" after "Intelligence and analysis" in heading and "and an Office of Infrastructure Protection" after "Office of Intelligence and Analysis" in text.

Subsec. (b). Pub. L. 115–278, §2(g)(2)(C)(iii)(I), struck out "and Assistant Secretary for Infrastructure Protection" after "Under Secretary for Intelligence and Analysis" in heading.

Subsec. (b)(3). Pub. L. 115–278, §2(g)(2)(C)(iii)(II), struck out par. (3). Text read as follows: "The Office of Infrastructure Protection shall be headed by an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President."

Subsec. (c). Pub. L. 115–278, §2(g)(2)(C)(iv), struck out "and infrastructure protection" after "information analysis" and "or the Assistant Secretary for Infrastructure Protection, as appropriate" after "the Under Secretary for Intelligence and Analysis".

Subsec. (d). Pub. L. 115–278, §2(g)(2)(C)(v)(I), (II), struck out "and infrastructure protection" after "intelligence and analysis" in heading and introductory provisions.

Subsec. (d)(5) to (22). Pub. L. 115–278, §2(g)(2)(C)(v)(III), (IV), redesignated pars. (7) to (24) as (5) to (22), respectively, and struck out former pars. (5) and (6). Prior to amendment, pars. (5) and (6) read as follows:

"(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

"(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

Subsec. (d)(23). Pub. L. 115–278, §2(g)(2)(C)(v)(V), redesignated par. (26) as (23). Former par. (23) redesignated (21).

Subsec. (d)(23)(B)(i). Pub. L. 115–278, §2(g)(2)(C)(v)(VI), made technical amendment to reference in original act which appears in text as reference to section 195f of this title.

Subsec. (d)(24). Pub. L. 115–278, §2(g)(2)(C)(v)(IV), redesignated par. (24) as (22).

Subsec. (d)(25). Pub. L. 115–278, §2(g)(2)(C)(v)(III), struck out par. (25) which read as follows: "To prepare and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security in the House of Representatives, and to other appropriate congressional committees having jurisdiction over the critical infrastructure or key resources, for each sector identified in the National Infrastructure Protection Plan, a report on the comprehensive assessments carried out by the Secretary of the critical infrastructure and key resources of the United States, evaluating threat, vulnerability, and consequence, as required under this subsection. Each such report—

"(A) shall contain, if applicable, actions or countermeasures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in the assessments;

"(B) shall be required for fiscal year 2007 and each subsequent fiscal year and shall be submitted not later than 35 days after the last day of the fiscal year covered by the report; and

"(C) may be classified."

Subsec. (d)(26). Pub. L. 115–278, §2(g)(2)(C)(v)(V), redesignated par. (26) as (23).

Subsecs. (e)(1), (f)(1). Pub. L. 115–278, §2(g)(2)(C)(vi), (vii), struck out "and the Office of Infrastructure Protection" after "the Office of Intelligence and Analysis".

2016—Subsec. (d)(26). Pub. L. 114–328 added par. (26).

2010—Subsec. (d)(3). Pub. L. 111–258 amended par. (3) generally. Prior to amendment, par. (3) read as follows: "To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities."

2009—Subsec. (f)(2)(E). Pub. L. 111–84 made technical amendment to directory language of Pub. L. 110–417. See 2008 amendment note below.

2008—Subsec. (f)(2)(E). Pub. L. 110–417, §931(b)(5), as amended by Pub. L. 111–84, substituted "National Geospatial-Intelligence Agency" for "National Imagery and Mapping Agency".

2007—Pub. L. 110–53, §531(a)(1), substituted "Information and" for "Directorate for Information" in section catchline.

Subsecs. (a) to (c). Pub. L. 110–53, §531(a)(2), added subsecs. (a) to (c) and struck out former subsecs. (a) to (c) which related to, in subsec. (a), establishment and responsibilities of Directorate for Information Analysis and Infrastructure Protection, in subsec. (b), positions of Assistant Secretary for Information Analysis and Assistant Secretary for Infrastructure Protection, and, in subsec. (c), Secretary's duty to ensure that responsibilities regarding information analysis and infrastructure protection would be carried out through the Under Secretary for Information Analysis and Infrastructure Protection.

Subsec. (d). Pub. L. 110–53, §531(a)(3), substituted "Secretary relating to intelligence and analysis and infrastructure protection" for "Under Secretary" in heading and "The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection" for "Subject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection" in introductory provisions.

Subsec. (d)(1). Pub. L. 110–53, §501(b)(1), inserted ", in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o)," after "to integrate such information" in introductory provisions.

Subsec. (d)(7). Pub. L. 110–53, §501(b)(2), added par. (7) and struck out former par. (7) which read as follows: "To review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities."

Pub. L. 110–53, §501(a)(2)(A), redesignated par. (8) as (7) and struck out former par. (7) which read as follows: "To administer the Homeland Security Advisory System, including—

"(A) exercising primary responsibility for public advisories related to threats to homeland security; and

"(B) in coordination with other agencies of the Federal Government, providing specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public."

Subsec. (d)(8). Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (9) as (8). Former par. (8) redesignated (7).

Subsec. (d)(9). Pub. L. 110–53, §531(a)(3)(C), substituted "Director of National Intelligence" for "Director of Central Intelligence".

Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (10) as (9). Former par. (9) redesignated (8).

Subsec. (d)(10). Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (11) as (10). Former par. (10) redesignated (9).

Subsec. (d)(11). Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (12) as (11). Former par. (11) redesignated (10).

Subsec. (d)(11)(B). Pub. L. 110–53, §531(a)(3)(D), substituted "Director of National Intelligence" for "Director of Central Intelligence".

Subsec. (d)(12) to (17). Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated pars. (13) to (18) as (12) to (17),

respectively. Former par. (12) redesignated (11).

Subsec. (d)(18). Pub. L. 110–53, §531(a)(3)(E), (F), added par. (18) and redesignated former par. (18) as (24).

Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (19) as (18). Former par. (18) redesignated (17).

Subsec. (d)(19). Pub. L. 110–53, §531(a)(3)(F), added par. (19).

Pub. L. 110–53, §501(a)(2)(A)(ii), redesignated par. (19) as (18).

Subsec. (d)(20) to (23). Pub. L. 110–53, §531(a)(3)(F), added pars. (20) to (23).

Subsec. (d)(24). Pub. L. 110–53, §531(a)(3)(E), redesignated par. (18) as (24).

Subsec. (d)(25). Pub. L. 110–53, §1002(a), added par. (25).

Subsec. (e)(1). Pub. L. 110–53, §531(a)(4), substituted "provide the Office of Intelligence and Analysis and the Office of Infrastructure Protection" for "provide the Directorate" and "assist such offices in discharging" for "assist the Directorate in discharging".

Subsec. (f)(1). Pub. L. 110–53, §531(a)(5), substituted "Office of Intelligence and Analysis and the Office of Infrastructure Protection" for "Directorate".

Subsec. (g). Pub. L. 110–53, §531(a)(6), substituted "Office of Intelligence and Analysis and the Office of Infrastructure Protection" for "Under Secretary for Information Analysis and Infrastructure Protection" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2009 AMENDMENT

Pub. L. 111–84, div. A, title X, §1073(c), Oct. 28, 2009, 123 Stat. 2474, provided that the amendment by section 1073(c)(9) is effective as of Oct. 14, 2008, and as if included in Pub. L. 110–417 as enacted.

REGULATIONS

Pub. L. 109–295, title V, §550, Oct. 4, 2006, 120 Stat. 1388, as amended by Pub. L. 110–161, div. E, title V, §534, Dec. 26, 2007, 121 Stat. 2075; Pub. L. 111–83, title V, §550, Oct. 28, 2009, 123 Stat. 2177; Pub. L. 112–10, div. B, title VI, §1650, Apr. 15, 2011, 125 Stat. 146; Pub. L. 112–74, div. D, title V, §540, Dec. 23, 2011, 125 Stat. 976; Pub. L. 113–6, div. D, title V, §537, Mar. 26, 2013, 127 Stat. 373; Pub. L. 113–76, div. F, title V, §536, Jan. 17, 2014, 128 Stat. 275, required interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for chemical facilities, prior to repeal by Pub. L. 113–254, §4(b), Dec. 18, 2014, 128 Stat. 2919. See section 627 of this title.

[Pub. L. 113–254, §4(b), Dec. 18, 2014, 128 Stat. 2919, provided that the repeal of section 550 of Pub. L. 109–295, formerly set out above, is effective as of the effective date of Pub. L. 113–254, which is the date that is 30 days after Dec. 18, 2014. See section 4(a) of Pub. L. 113–254, set out as an Effective and Termination Dates note under former section 621 of this title.]

PROHIBITION ON AVAILABILITY OF FUNDS FOR CERTAIN ACTIVITIES AND ASSESSMENT OF THE OVERT HUMAN INTELLIGENCE AND OPEN SOURCE INTELLIGENCE COLLECTION PROGRAMS OF THE OFFICE OF INTELLIGENCE AND ANALYSIS OF THE DEPARTMENT OF HOMELAND SECURITY

Pub. L. 118–31, div. G, title III, §7324, Dec. 22, 2023, 137 Stat. 1039, provided that:

"(a) DEFINITIONS.—In this section:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means the following:

"(A) The congressional intelligence committees [Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives].

"(B) The Committee on Homeland Security and Governmental Affairs of the Senate.

"(C) The Committee on Homeland Security of the House of Representatives.

"(2) COVERED ACTIVITY.—The term 'covered activity' means—

"(A) with respect to the Overt Human Intelligence Collection Program, an interview for intelligence collection purposes with any individual, including a United States person, who has been criminally charged, arraigned, or taken into the custody of a Federal, State, or local law enforcement agency, but whose guilt with respect to such criminal matters has not yet been adjudicated, unless the Office of Intelligence and Analysis has obtained the consent of the interviewee following consultation with counsel;

"(B) with respect to either the Overt Human Intelligence Collection Program or the Open Source

Intelligence Collection Program, any collection targeting journalists in the performance of their journalistic functions; and

"(C) with respect to the Overt Human Intelligence Collection Program, an interview for intelligence collection purposes with a United States person where the Office of Intelligence and Analysis lacks a reasonable belief based on facts and circumstances that the United States person may possess significant foreign intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

"(3) OVERT HUMAN INTELLIGENCE COLLECTION PROGRAM.—The term 'Overt Human Intelligence Collection Program' means the program established by the Under Secretary of Homeland Security for Intelligence and Analysis pursuant to Policy Instruction 907 of the Office of Intelligence and Analysis, issued on June 29, 2016, or any successor program.

"(4) OPEN SOURCE INTELLIGENCE COLLECTION PROGRAM.—The term 'Open Source Collection Intelligence Program' means the program established by the Under Secretary of Homeland Security for Intelligence and Analysis for the purpose of collecting intelligence and information for potential production and reporting in the form of Open Source Information Reports as reflected in Policy Instruction 900 of the Office of Intelligence and Analysis, issued on January 13, 2015, or any successor program.

"(5) UNITED STATES PERSON.—The term 'United States person' means—

"(A) a United States citizen;

"(B) an alien known by the Office of Intelligence and Analysis to be a permanent resident alien;

"(C) an unincorporated association substantially composed of United States citizens or permanent resident aliens; or

"(D) a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

"(6) UNITED STATES PERSON INFORMATION (USPI).—The term 'United States person information'—

"(A) means information that is reasonably likely to identify 1 or more specific United States persons; and

"(B) may be either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific United States persons.

"(b) PROHIBITION ON AVAILABILITY OF FUNDS FOR COVERED ACTIVITIES OF OVERT HUMAN INTELLIGENCE COLLECTION PROGRAM AND OPEN SOURCE INTELLIGENCE COLLECTION PROGRAM.—None of the funds authorized to be appropriated by this division [see Tables for classification] may be made available to the Office of Intelligence and Analysis of the Department of Homeland Security to conduct a covered activity.

"(c) LIMITATION ON PERSONNEL.—None of the funds authorized to be appropriated by this division may be used by the Office of Intelligence and Analysis of the Department of Homeland Security to increase, above the staffing level in effect on the day before the date of the enactment of this Act [Dec. 22, 2023], the number of personnel assigned to the Open Source Intelligence Division who work exclusively or predominantly on domestic terrorism issues.

"(d) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY ASSESSMENT OF OVERT HUMAN INTELLIGENCE COLLECTION PROGRAM AND OPEN SOURCE INTELLIGENCE COLLECTION PROGRAM.—

"(1) REQUIREMENT.—The Inspector General of the Intelligence Community shall conduct an assessment of the Overt Human Intelligence Collection Program and the Open Source Intelligence Collection Program.

"(2) ELEMENTS.—The assessment under paragraph (1) shall include findings and, as the Inspector General considers appropriate, recommendations on the following:

"(A) Whether the Overt Human Intelligence Collection Program and the Open Source Intelligence Collection Program are legally authorized, and if so, an identification of the legal authorities.

"(B) Whether, and to what extent, such programs have provided valuable insights on national intelligence priorities and intelligence priorities of the Department of Homeland Security, citing specific examples of such insights at the appropriate classification level.

"(C) Whether there is sufficient training provided to, and sufficient oversight provided of, personnel of the Office of Intelligence and Analysis of the Department of Homeland Security who conduct intelligence collection under such programs.

"(D) Whether the responsibilities and requirements for such programs set forth in the relevant policy instructions, intelligence oversight guidelines, and other governing documents or standard

operating procedures of the Office of Intelligence and Analysis, particularly as they relate to the obligation to safeguard the privacy, civil liberties, and civil rights of United States persons, are adequate, appropriate, and consistently adhered to by such personnel.

"(E) Whether such programs raise or have raised legal, ethical, or operational concerns, including concerns relating to the actual or potential violation of any applicable policies or procedures for protecting the constitutional or statutory rights of United States persons.

"(F) Whether other Federal agencies, such as the Federal Bureau of Investigation, conduct similar programs and, if so, a comparison of any similarities and differences between the respective programs.

"(G) With respect to non-analytic intelligence reports produced by the Office of Intelligence and Analysis derived in whole or in part from such programs, whether such reports appropriately minimize United States person information and use press reporting in an appropriate manner.

"(H) With respect to the Open Source Intelligence Collection Program, whether such program is effective at identifying threats directed against the United States, including true threats, incitement to violence, and malign cyber activity.

"(I) Whether there have been any identified instances in which State, local, territorial, or Tribal government agencies have used, or sought to use, the Office of Intelligence and Analysis as an instrument to introduce political or politicized information into the national intelligence collection and reporting stream.

"(J) Any other matter the Inspector General of the Intelligence Community determines appropriate.

"(3) BRIEFING.—Not later than 120 days after the date of the enactment of this Act [Dec. 22, 2023], the Inspector General of the Intelligence Community shall provide to the appropriate congressional committees a briefing on the preliminary findings and recommendations of the Inspector General with respect to the assessment under paragraph (1).

"(4) REPORT.—

"(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the appropriate congressional committees a report containing the findings and recommendations of the Inspector General with respect to the assessment under paragraph (1).

"(B) FORM.—The report submitted pursuant to subparagraph (A) shall be submitted under that subparagraph in unclassified form, but may include a classified annex.

"(5) QUARTERLY BRIEFINGS.—The Under Secretary of Homeland Security for Intelligence and Analysis shall, not less than once per quarter, provide to the appropriate congressional committees a briefing on the intelligence collection activities of the Office of Intelligence and Analysis. These briefings shall include—

"(A) a description of any new activities, initiatives, or efforts undertaken pursuant to the Overt Human Intelligence Collection Program or the Open Source Intelligence Collection Program;

"(B) a description of any new policies, procedures, or guidance concerning the Overt Human Intelligence Collection Program or the Open Source Intelligence Collection Program;

"(C) a description of any compliance-related inquiries, investigations, reviews, checks, or audits initiated concerning the Overt Human Intelligence Collection Program or the Open Source Intelligence Collection Program, as well as an update on the outcome or status of any preexisting inquiries, investigations, reviews, checks, or audits concerning these programs;

"(D) a comparison of the volume of intelligence and information collected on United States persons by the Office and used in finished intelligence products produced by the Office with the volume of intelligence or information on United States persons that is—

"(i) collected by State, local, and Tribal territory governments, the private sector, and other components of the Department of Homeland Security;

"(ii) provided directly or indirectly to the Office; and

"(iii) used in finished intelligence products produced by the Office; and

"(E) information on the reports and products issued by the Overt Human Intelligence Collection Program and the Open Source Intelligence Collection Program for the quarter covered by the briefing, which shall reflect—

"(i) the number of reports and products issued by each program;

"(ii) the number of reports and products issued by type or format of the report or product;

"(iii) the number of reports and products based on information provided by representatives of Federal, foreign or international, State, local, Tribal, territorial, or private sector entities, respectively, and, for each of these subcategories, the number of reports or products based on information provided

by known or presumed United States persons;

"(iv) the number of reports and products based on information provided by individuals in administrative custody and, within that number, the number of reports or products based on information provided by known or presumed United States persons;

"(v) the number of reports and products based on information provided by confidential informants and, within that number, the number of reports or products based on information provided by known or presumed United States persons;

"(vi) the number of reports and products supporting different national or departmental missions and, for each of these subcategories, the number of reports or products based on information provided by known or presumed United States persons; and

"(vii) the number of reports and products identifying United States persons.

"(e) RULES OF CONSTRUCTION.—

"(1) EFFECT ON OTHER INTELLIGENCE OVERSIGHT.—Nothing in this section shall be construed as limiting or superseding the authority of any official within the Department of Homeland Security to conduct legal, privacy, civil rights, or civil liberties oversight of the intelligence activities of the Office of Intelligence and Analysis.

"(2) SHARING AND RECEIVING INTELLIGENCE INFORMATION.—Nothing in this section shall be construed to prohibit, or to limit the authority of, personnel of the Office of Intelligence and Analysis from sharing intelligence information with, or receiving information from—

"(A) foreign, State, local, Tribal, or territorial governments (or any agency or subdivision thereof);

"(B) the private sector; or

"(C) other elements of the Federal government, including the components of the Department of Homeland Security."

DHS COMPONENT USAGE OF THE HOMELAND SECURITY INFORMATION NETWORK

Pub. L. 116–116, §4, Mar. 2, 2020, 134 Stat. 111, provided that:

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Mar. 2, 2020], the Chief Information Officer, in consultation with the Under Secretary for Intelligence and Analysis, and in accordance with the functions and responsibilities assigned to the Under Secretary under title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), shall—

"(1) develop policies and metrics to ensure effective use by components of the Department of the unclassified Homeland Security Information Network (referred to in this section as 'HSIN'), or any successor system; and

"(2) develop policies for posting unclassified products on HSIN, or any successor system.

"(b) TECHNICAL ENHANCEMENTS.—The Chief Information Officer, in consultation with the Chief Intelligence Officer, shall assess and implement, as appropriate, technical enhancements to HSIN to improve usability, including search functionality, data analysis, and collaboration capabilities."

DEADLINE FOR INITIAL RECOMMENDED STRATEGY

Pub. L. 114–328, div. A, title XIX, §1913(c), Dec. 23, 2016, 130 Stat. 2687, provided that: "Not later than one year after the date of the enactment of this section [Dec. 23, 2016], the Secretary of Homeland Security shall submit the recommended strategy required under paragraph (26) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)), as added by this section."

ENHANCED GRID SECURITY

Pub. L. 114–94, div. F, §61003(c), Dec. 4, 2015, 129 Stat. 1778, provided that:

"(1) DEFINITIONS.—In this subsection:

"(A) CRITICAL ELECTRIC INFRASTRUCTURE; CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The terms 'critical electric infrastructure' and 'critical electric infrastructure information' have the meanings given those terms in section 215A of the Federal Power Act [16 U.S.C. 824o–1].

"(B) SECTOR-SPECIFIC AGENCY.—The term 'Sector-Specific Agency' has the meaning given that term in the Presidential Policy Directive entitled 'Critical Infrastructure Security and Resilience', numbered 21, and dated February 12, 2013.

"(2) SECTOR-SPECIFIC AGENCY FOR CYBERSECURITY FOR THE ENERGY SECTOR.—

"(A) IN GENERAL.—The Department of Energy shall be the lead Sector-Specific Agency for cybersecurity for the energy sector.

"(B) DUTIES.—As head of the designated Sector-Specific Agency for cybersecurity, the duties of the

Secretary of Energy shall include—

"(i) coordinating with the Department of Homeland Security and other relevant Federal departments and agencies;

"(ii) collaborating with—

"(I) critical electric infrastructure owners and operators; and

"(II) as appropriate—

"(aa) independent regulatory agencies; and

"(bb) State, local, tribal, and territorial entities;

"(cc) serving as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;

"(dd) carrying out incident management responsibilities consistent with applicable law (including regulations) and other appropriate policies or directives;

"(ee) providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate; and

"(ff) supporting the reporting requirements of the Department of Homeland Security under applicable law by providing, on an annual basis, sector-specific critical electric infrastructure information."

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

CYBERSECURITY COLLABORATION BETWEEN THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF HOMELAND SECURITY

Pub. L. 112–81, div. A, title X, §1090, Dec. 31, 2011, 125 Stat. 1603, provided that:

"(a) INTERDEPARTMENTAL COLLABORATION.—

"(1) IN GENERAL.—The Secretary of Defense and the Secretary of Homeland Security shall provide personnel, equipment, and facilities in order to increase interdepartmental collaboration with respect to—

"(A) strategic planning for the cybersecurity of the United States;

"(B) mutual support for cybersecurity capabilities development; and

"(C) synchronization of current operational cybersecurity mission activities.

"(2) EFFICIENCIES.—The collaboration provided for under paragraph (1) shall be designed—

"(A) to improve the efficiency and effectiveness of requirements formulation and requests for products, services, and technical assistance for, and coordination and performance assessment of, cybersecurity missions executed across a variety of Department of Defense and Department of Homeland Security elements; and

"(B) to leverage the expertise of each individual Department and to avoid duplicating, replicating, or aggregating unnecessarily the diverse line organizations across technology developments, operations, and customer support that collectively execute the cybersecurity mission of each Department.

"(b) RESPONSIBILITIES.—

"(1) DEPARTMENT OF HOMELAND SECURITY.—The Secretary of Homeland Security shall identify and assign, in coordination with the Department of Defense, a Director of Cybersecurity Coordination within the Department of Homeland Security to undertake collaborative activities with the Department of Defense.

"(2) DEPARTMENT OF DEFENSE.—The Secretary of Defense shall identify and assign, in coordination with the Department of Homeland Security, one or more officials within the Department of Defense to coordinate, oversee, and execute collaborative activities and the provision of cybersecurity support to the Department of Homeland Security."

CYBERSECURITY OVERSIGHT

Pub. L. 111–259, title III, §336, Oct. 7, 2010, 124 Stat. 2689, which related to cybersecurity oversight and provided for notification of cybersecurity programs, program and information sharing reports, provisions for the detailing of personnel, and provisions for further planning to recruit, retain, and train a highly-qualified workforce to secure the networks of the intelligence community, terminated on Dec. 31, 2013.

TREATMENT OF INCUMBENT UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS

Pub. L. 110–53, title V, §531(c), Aug. 3, 2007, 121 Stat. 335, provided that: "The individual administratively performing the duties of the Under Secretary for Intelligence and Analysis as of the date of the enactment of this Act [Aug. 3, 2007] may continue to perform such duties after the date on which the

President nominates an individual to serve as the Under Secretary pursuant to section 201 of the Homeland Security Act of 2002 [6 U.S.C. 121], as amended by this section, and until the individual so appointed assumes the duties of the position."

REPORTS TO BE SUBMITTED TO CERTAIN COMMITTEES

Pub. L. 110–53, title XXIV, §2403, Aug. 3, 2007, 121 Stat. 547, provided that: "The Committee on Commerce, Science, and Transportation of the Senate shall receive the reports required by the following provisions of law in the same manner and to the same extent that the reports are to be received by the Committee on Homeland Security and Governmental Affairs of the Senate:

"(1) Section 1016(j)(1) [now 1016(i)(1)] of the Intelligence Reform and Terrorist [Terrorism] Prevention Act of 2004 (6 U.S.C. 485(j)(1) [now 6 U.S.C. 485(i)(1)]).

"(2) Section 511(d) of this Act [121 Stat. 323].

"(3) [Former] [s]ubsection (a)(3)(D) of section 2022 of the Homeland Security Act of 2002 [former 6 U.S.C. 612(a)(3)(D)], as added by section 101 of this Act.

"(4) Section 7215(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 123(d)).

"(5) Section 7209(b)(1)(C) of the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458] (8 U.S.C. 1185 note).

"(6) Section 804(c) of this Act [42 U.S.C. 2000ee–3(c)].

"(7) Section 901(b) of this Act [121 Stat. 370].

"(8) Section 1002(a) of this Act [amending this section].

"(9) Title III of this Act [enacting sections 579 and 580 of this title and amending sections 194 and 572 of this title]."

SECURITY MANAGEMENT SYSTEMS DEMONSTRATION PROJECT

Pub. L. 110–53, title XXIV, §2404, Aug. 3, 2007, 121 Stat. 548, provided that:

"(a) DEMONSTRATION PROJECT REQUIRED.—Not later than 120 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall—

"(1) establish a demonstration project to conduct demonstrations of security management systems that—

"(A) shall use a management system standards approach; and

"(B) may be integrated into quality, safety, environmental and other internationally adopted management systems; and

"(2) enter into one or more agreements with a private sector entity to conduct such demonstrations of security management systems.

"(b) SECURITY MANAGEMENT SYSTEM DEFINED.—In this section, the term 'security management system' means a set of guidelines that address the security assessment needs of critical infrastructure and key resources that are consistent with a set of generally accepted management standards ratified and adopted by a standards making body."

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13231. CRITICAL INFRASTRUCTURE PROTECTION IN THE INFORMATION AGE

Ex. Ord. No. 13231, Oct. 16, 2001, 66 F.R. 53063, as amended by Ex. Ord. No. 13284, §2, Jan. 23, 2003, 68 F.R. 4075; Ex. Ord. No. 13286, §7, Feb. 28, 2003, 68 F.R. 10620; Ex. Ord. No. 13385, §5, Sept. 29, 2005, 70 F.R. 57990; Ex. Ord. No. 13652, §6, Sept. 30, 2013, 78 F.R. 61818; Ex. Ord. No. 14048, §6, Sept. 30, 2021, 86 F.R. 55467, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

SECTION 1. *Policy*. The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause

the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

SEC. 2. *Continuing Authorities*. This order does not alter the existing authorities or roles of United States Government departments and agencies. Authorities set forth in 44 U.S.C. chapter 35, and other applicable law, provide senior officials with responsibility for the security of Federal Government information systems.

(a) Executive Branch Information Systems Security. The Director of the Office of Management and Budget (OMB) has the responsibility to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, except those noted in section 2(b) of this order. The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices within the purview of this section in an executive branch department or agency.

(b) National Security Information Systems. The Secretary of Defense and the Director of Central Intelligence (DCI) shall have responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.

(i) Policies, principles, standards, and guidelines developed under this subsection may require more stringent protection than those developed in accordance with section 2(a) of this order.

(ii) The Assistant to the President for National Security Affairs shall advise the President and the appropriate department or agency when there is a critical deficiency in the security practices of a department or agency within the purview of this section.

(iii) National Security Systems. The National Security Telecommunications and Information Systems Security Committee, as established by and consistent with NSD–42 and chaired by the Department of Defense, shall be designated as the "Committee on National Security Systems."

(c) Additional Responsibilities. The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

SEC. 3. *The National Infrastructure Advisory Council*. The National Infrastructure Advisory Council (NIAC), established on October 16, 2001, shall provide the President, through the Secretary of Homeland Security, with advice on the security and resilience of the critical infrastructure sectors and their functional systems, physical assets, and cyber networks.

(a) *Membership*. The NIAC shall be composed of not more than 30 members appointed by the President, taking appropriate account of the benefits of having members:

(i) from the private sector, including individuals with experience in banking and finance, transportation, energy, water, communications, health care services, food and agriculture, government facilities, emergency services organizations, institutions of higher education, environmental and climate resilience, and State, local, and tribal governments;

(ii) with senior executive leadership responsibilities for the availability and reliability, including security and resilience, of critical infrastructure sectors;

(iii) with expertise relevant to the functions of the NIAC; and

(iv) with experience equivalent to that of a chief executive of an organization.

Unless otherwise determined by the President, no full-time officer or employee of the executive branch shall be appointed to serve as a member of the NIAC. The President shall designate from among the members of the NIAC a Chair and a Vice Chair, who shall perform the functions of the Chair if the Chair is absent or disabled, or in the instance of a vacancy in the Chair, each for a term of up to two years.. [sic]

(b) *Functions of the NIAC*. The NIAC shall meet periodically to:

(i) enhance the partnership of the public and private sectors in securing and enhancing the security and resilience of critical infrastructure and their supporting functional systems, physical assets, and cyber networks, and provide reports on this issue to the President, through the Secretary of Homeland Security, as appropriate;

(ii) propose and develop ways to encourage private industry to perform periodic risk assessments and implement risk-reduction programs;

(iii) monitor the development and operations of critical infrastructure sector coordinating councils and their information-sharing mechanisms and provide recommendations to the President, through the Secretary of Homeland Security, on how these organizations can best foster improved cooperation among the sectors, the Department of Homeland Security, and other Federal Government entities;

(iv) report to the President through the Secretary of Homeland Security, who shall ensure appropriate coordination with the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs under the terms of this order; and

(v) advise sector-specific agencies with critical infrastructure responsibilities to include issues pertaining to sector and government coordinating councils and their information sharing mechanisms.

In implementing this order, the NIAC shall not advise or otherwise act on matters pertaining to National Security and Emergency Preparedness (NS/EP) Communications and, with respect to any matters to which the NIAC is authorized by this order to provide advice or otherwise act on that may depend on or affect NS/EP Communications, shall coordinate with the National Security and Telecommunications Advisory Committee established by Executive Order 12382 of September 13, 1982, as amended.

(c) Administration of the NIAC.

(i) The NIAC may hold hearings, conduct inquiries, and establish subcommittees, as appropriate.

(ii) Upon request of the Chair, and to the extent permitted by law, the heads of the executive departments and agencies shall provide the NIAC with information and advice relating to its functions.

(iii) Senior Federal Government officials may participate in the meetings of the NIAC, as appropriate.

(iv) Members shall serve without compensation for their work on the NIAC. However, members may be reimbursed for travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service (5 U.S.C. 5701–5707).

(v) To the extent permitted by law and subject to the availability of appropriations, the Department of Homeland Security shall provide the NIAC with administrative services, staff, and other support services, and such funds as may be necessary for the performance of the NIAC's functions.

SEC. 4. *Judicial Review*. This order does not create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

EXTENSION OF TERM OF NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Term of National Infrastructure Advisory Council extended until Sept. 30, 2025, by Ex. Ord. No. 14109, Sept. 29, 2023, 88 F.R. 68447, set out as a note under section 1013 of Title 5, Government Organization and Employees.

Previous extensions of term of National Infrastructure Advisory Council were contained in the following prior Executive Orders:

Ex. Ord. No. 14048, Sept. 30, 2021, 86 F.R. 55465, extended term until Sept. 30, 2023.
Ex. Ord. No. 13889, Sept. 27, 2019, 84 F.R. 52743, extended term until Sept. 30, 2021.
Ex. Ord. No. 13811, Sept. 29, 2017, 82 F.R. 46363, extended term until Sept. 30, 2019.
Ex. Ord. No. 13708, Sept. 30, 2015, 80 F.R. 60271, extended term until Sept. 30, 2017.
Ex. Ord. No. 13652, Sept. 30, 2013, 78 F.R. 61817, extended term until Sept. 30, 2015.
Ex. Ord. No. 13585, Sept. 30, 2011, 76 F.R. 62281, extended term until Sept. 30, 2013.
Ex. Ord. No. 13511, Sept. 29, 2009, 74 F.R. 50909, extended term until Sept. 30, 2011.
Ex. Ord. No. 13446, Sept. 28, 2007, 72 F.R. 56175, extended term until Sept. 30, 2009.
Ex. Ord. No. 13385, Sept. 29, 2005, 70 F.R. 57989, extended term until Sept. 30, 2007.
Ex. Ord. No. 13316, Sept. 17, 2003, 68 F.R. 55255, extended term until Sept. 30, 2005.

EX. ORD. NO. 13284. AMENDMENT OF EXECUTIVE ORDERS, AND OTHER ACTIONS, IN CONNECTION WITH THE ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY

Ex. Ord. No. 13284, Jan. 23, 2003, 68 F.R. 4075, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Homeland Security Act of 2002 (Public Law 107–296) [see Tables for classification], and the National Security Act of 1947, as amended (50 U.S.C. 401 *et seq*.) [now 50 U.S.C. 3001 et seq.], and in order to reflect responsibilities vested in the Secretary of Homeland Security and take other actions in connection with the establishment of the Department of Homeland Security, it is hereby ordered as follows:

SECTION 1. [Amended Ex. Ord. No. 13234.]

SEC. 2. [Amended Ex. Ord. No. 13231, set out above.]

SEC. 3. Executive Order 13228 of October 8, 2001 ("Establishing the Office of Homeland Security and the Homeland Security Council") [50 U.S.C. 3021 note], is amended by inserting "the Secretary of Homeland Security," after "the Secretary of Transportation," in section 5(b). Further, during the period from January 24, 2003, until March 1, 2003, the Secretary of Homeland Security shall have the responsibility for coordinating the domestic response efforts otherwise assigned to the Assistant to the President for Homeland Security pursuant to section 3(g) of Executive Order 13228.

SEC. 4. [Amended Ex. Ord. No. 13224, listed in a table under section 1701 of Title 50, War and National Defense.]

SEC. 5. [Amended Ex. Ord. No. 13151, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

SEC. 6. [Amended Ex. Ord. No. 13122, set out as a note under section 3121 of Title 42, The Public Health and Welfare.]

SEC. 7. [Amended Ex. Ord. No. 13048, set out as a note under section 501 of Title 31, Money and Finance.]

SEC. 8. [Amended Ex. Ord. No. 12992, set out as a note under section 1708 of Title 21, Food and Drugs.]

SEC. 9. [Amended Ex. Ord. No. 12881, set out as a note under section 6601 of Title 42, The Public Health and Welfare.]

SEC. 10. [Amended Ex. Ord. No. 12859, set out as a note preceding section 101 of Title 3, The President.]

SEC. 11. [Amended Ex. Ord. No. 12590, set out as a note under former section 1201 of Title 21, Food and Drugs.]

SEC. 12. [Amended Ex. Ord. No. 12260, set out as a note under section 2511 of Title 19, Customs Duties.]

SEC. 13. [Amended Ex. Ord. No. 11958, set out as a note under section 2751 of Title 22, Foreign Relations and Intercourse.]

SEC. 14. [Amended Ex. Ord. No. 11423, set out as a note under section 301 of Title 3, The President.]

SEC. 15. [Amended Ex. Ord. No. 10865, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 16. [Amended Ex. Ord. No. 13011, set out as a note under section 11101 of Title 40, Public Buildings, Property, and Works.]

SEC. 17. Those elements of the Department of Homeland Security that are supervised by the Department's Under Secretary for Information Analysis and Infrastructure Protection through the Department's Assistant Secretary for Information Analysis, with the exception of those functions that involve no analysis of foreign intelligence information, are designated as elements of the Intelligence Community under section 201(h) of the Homeland Security Act of 2002 [Pub. L. 107–296, amending 50 U.S.C. 3003] and section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a[(4)]) [now 50 U.S.C. 3003(4)].

SEC. 18. [Amended Ex. Ord. No. 12333, set out as a note under section 3001 of title 50, War and National Defense.]

SEC. 19. *Functions of Certain Officials in the Department of Homeland Security.*

The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a "Senior Official of the Intelligence Community" for purposes of Executive Order 12333 [50 U.S.C. 3001 note], and all other relevant authorities, and shall:

(a) recognize and give effect to all current clearances for access to classified information held by those who become employees of the Department of Homeland Security by operation of law pursuant to the Homeland Security Act of 2002 or by Presidential appointment;

(b) recognize and give effect to all current clearances for access to classified information held by those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities;

(c) make all clearance and access determinations pursuant to Executive Order 12968 of August 2, 1995 [50 U.S.C. 3161 note], or any successor Executive Order, as to employees of, and applicants for employment in, the Department of Homeland Security who do not then hold a current clearance for access to classified information; and

(d) ensure all clearance and access determinations for those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities are made in accordance with Executive Order 12829 of January 6, 1993 [50 U.S.C. 3161 note].

SEC. 20. Pursuant to the provisions of section 1.4 of [former] Executive Order 12958 of April 17, 1995 ("Classified National Security Information"), I hereby authorize the Secretary of Homeland Security to

classify information originally as "Top Secret." Any delegation of this authority shall be in accordance with section 1.4 of that order or any successor Executive Orders.

SEC. 21. This order shall become effective on January 24, 2003.

SEC. 22. This order does not create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH.

EX. ORD. NO. 13636. IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Ex. Ord. No. 13636, Feb. 12, 2013, 78 F.R. 11739, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

SEC. 2. *Critical Infrastructure*. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

SEC. 3. *Policy Coordination*. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

SEC. 4. *Cybersecurity Information Sharing*. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with [former] 6 U.S.C. 143 [now 6 U.S.C. 655] and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and

types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

SEC. 5. *Privacy and Civil Liberties Protections*. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with [former] 6 U.S.C. 133 [now 6 U.S.C. 673] by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

SEC. 6. *Consultative Process*. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

SEC. 7. *Baseline Framework to Reduce Cyber Risk to Critical Infrastructure*. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order.

The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

SEC. 8. *Voluntary Critical Infrastructure Cybersecurity Program*. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

SEC. 9. *Identification of Critical Infrastructure at Greatest Risk*. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

SEC. 10. *Adoption of Framework*. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory

requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

SEC. 11. *Definitions*. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

SEC. 12. *General Provisions*. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to the National Security Staff deemed to be a reference to the National Security Council Staff, see Ex. Ord. No. 13657, set out as a note under section 3021 of Title 50, War and National Defense.]

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

EXECUTIVE ORDER NO. 13650

Ex. Ord. No. 13650, Aug. 1, 2013, 78 F.R. 48029, was transferred to a note set out under former section 621 of this title.

EX. ORD. NO. 13691. PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

Ex. Ord. No. 13691, Feb. 13, 2015, 80 F.R. 9349, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive–21 (PPD–21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–l [sic] (PPD–l [PPD–1]) of February 13, 2009 (Organization of the National Security Council System), or any successor.

SEC. 2. *Information Sharing and Analysis Organizations*. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

SEC. 3. *ISAO Standards Organization*. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

SEC. 4. *Critical Infrastructure Protection Program*. (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

SEC. 5. *Privacy and Civil Liberties Protections*. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency's activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

SEC. 6. *National Industrial Security Program*. [Amended Ex. Ord. No. 12829, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 7. *Definitions*. (a) "Critical infrastructure information" has the meaning given the term in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) "Critical infrastructure protection program" has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.

(c) "Cybersecurity risk" has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) "Incident" has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) "Information Sharing and Analysis Organization" has the meaning given the term in section 212(5) of the Critical Infrastrucure Information Act of 2002.

(g) "Sector-Specific Agency" has the meaning given the term in PPD–21, or any successor.

SEC. 8. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an

agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

[1] *So in original. The comma probably should not appear.*

§121a. Homeland Security Intelligence Program

There is established within the Department of Homeland Security a Homeland Security Intelligence Program. The Homeland Security Intelligence Program constitutes the intelligence activities of the Office of Intelligence and Analysis of the Department that serve predominantly departmental missions.

(Pub. L. 112–277, title V, §501, Jan. 14, 2013, 126 Stat. 2476.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2013, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§122. Access to information

(a) In general

(1) Threat and vulnerability information

Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

(2) Other information

The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide.

(b) Manner of access

Except as otherwise directed by the President, with respect to information to which the Secretary has access pursuant to this section—

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements

involving broad categories of material, access to electronic databases, or both; and

(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to paragraph (1), all agencies of the Federal Government shall promptly provide to the Secretary—

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed;

(C) all other information relating to significant and credible threats of terrorism against the United States, whether or not such information has been analyzed; and

(D) such other information or material as the President may direct.

(c) Treatment under certain laws

The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of National Intelligence, under any provision of the following:

(1) The USA PATRIOT Act of 2001 (Public Law 107–56).

(2) Section 2517(6) of title 18.

(3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) Access to intelligence and other information

(1) Access by elements of Federal Government

Nothing in this subchapter shall preclude any element of the intelligence community (as that term is defined in section 3003(4) of title 50,[1] or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any intelligence or other information relating to terrorism.

(2) Sharing of information

The Secretary, in consultation with the Director of National Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

(Pub. L. 107–296, title II, §202, Nov. 25, 2002, 116 Stat. 2149; Pub. L. 115–278, §2(g)(2)(D), Nov. 16, 2018, 132 Stat. 4177.)

EDITORIAL NOTES

REFERENCES IN TEXT

The USA PATRIOT Act of 2001, referred to in subsec. (c)(1), is Pub. L. 107–56, Oct. 26, 2001, 115 Stat. 272, known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 or the USA PATRIOT Act. For complete classification of this Act to the Code, see Short Title of 2001 Amendment note set out under section 1 of Title 18, Crimes and Criminal Procedure, and Tables.

The Federal Rules of Criminal Procedure, referred to in subsec. (c)(3), are set out in the Appendix to Title 18, Crimes and Criminal Procedure.

This subchapter, referred to in subsec. (d)(1), was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 3003 of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review,

Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c), (d)(2). Pub. L. 115–278 substituted "Director of National Intelligence" for "Director of Central Intelligence".

[1] *So in original. There probably should be a closing parenthesis after "50".*

§123. Terrorist travel program

(a) Requirement to establish

Not later than 90 days after August 3, 2007, the Secretary of Homeland Security, in consultation with the Director of the National Counterterrorism Center and consistent with the strategy developed under section 7201,[1] shall establish a program to oversee the implementation of the Secretary's responsibilities with respect to terrorist travel.

(b) Head of the program

The Secretary of Homeland Security shall designate an official of the Department of Homeland Security to be responsible for carrying out the program. Such official shall be—

(1) the Assistant Secretary for Policy of the Department of Homeland Security; or

(2) an official appointed by the Secretary who reports directly to the Secretary.

(c) Duties

The official designated under subsection (b) shall assist the Secretary of Homeland Security in improving the Department's ability to prevent terrorists from entering the United States or remaining in the United States undetected by—

(1) developing relevant strategies and policies;

(2) reviewing the effectiveness of existing programs and recommending improvements, if necessary;

(3) making recommendations on budget requests and on the allocation of funding and personnel;

(4) ensuring effective coordination, with respect to policies, programs, planning, operations, and dissemination of intelligence and information related to terrorist travel—

(A) among appropriate subdivisions of the Department of Homeland Security, as determined by the Secretary and including—

(i) United States Customs and Border Protection;

(ii) United States Immigration and Customs Enforcement;

(iii) United States Citizenship and Immigration Services;

(iv) the Transportation Security Administration; and

(v) the United States Coast Guard; and

(B) between the Department of Homeland Security and other appropriate Federal agencies; and

(5) serving as the Secretary's primary point of contact with the National Counterterrorism Center for implementing initiatives related to terrorist travel and ensuring that the recommendations of the Center related to terrorist travel are carried out by the Department.

(d) Report

Not later than 180 days after August 3, 2007, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this section.

(Pub. L. 108–458, title VII, §7215, Dec. 17, 2004, 118 Stat. 3832; Pub. L. 110–53, title VII, §722, Aug. 3, 2007, 121 Stat. 348.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 7201, referred to in subsec. (a), is section 7201 of Pub. L. 108–458, title VII, Dec. 17, 2004, 118 Stat. 3808, which enacted section 1776 of Title 8, Aliens and Nationality, and provisions set out as notes under section 1776 of Title 8 and sections 3024 and 3056 of Title 50, War and National Defense.

CODIFICATION

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the 9/11 Commission Implementation Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2007—Pub. L. 110–53 reenacted section catchline without change and amended text generally, substituting provisions relating to establishment of a program to oversee the implementation of the Secretary's responsibilities with respect to terrorist travel not later than 90 days after Aug. 3, 2007, and relating to the head of the program, such official's duties, and report on implementation for provisions relating to establishment of a program to oversee the implementation of the Department's responsibilities with respect to terrorist travel.

STATUTORY NOTES AND RELATED SUBSIDIARIES

NATIONAL STRATEGY TO COMBAT TERRORIST TRAVEL

Pub. L. 114–328, div. A, title XIX, §1908, Dec. 23, 2016, 130 Stat. 2678, provided that:

"(a) SENSE OF CONGRESS.—It is the sense of Congress that it should be the policy of the United States to—

"(1) continue to regularly assess the evolving terrorist threat to the United States;

"(2) catalog existing Federal Government efforts to obstruct terrorist and foreign fighter travel into, out of, and within the United States, and overseas;

"(3) identify such efforts that may benefit from reform or consolidation, or require elimination;

"(4) identify potential security vulnerabilities in United States defenses against terrorist travel; and

"(5) prioritize resources to address any such security vulnerabilities in a risk-based manner.

"(b) NATIONAL STRATEGY AND UPDATES.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees a national strategy to combat terrorist travel. The strategy shall address efforts to intercept terrorists and foreign fighters and constrain the domestic and international travel of such persons. Consistent with the protection of classified information, the strategy shall be submitted in unclassified form, including, as appropriate, a classified annex.

"(2) UPDATED STRATEGIES.—Not later than 180 days after the date on which a new President is inaugurated, the President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an updated version of the strategy described in paragraph (1).

"(3) CONTENTS.—The strategy and updates required under this subsection shall—

"(A) include an accounting and description of all Federal Government programs, projects, and activities designed to constrain domestic and international travel by terrorists and foreign fighters;

"(B) identify specific security vulnerabilities within the United States and outside of the United States that may be exploited by terrorists and foreign fighters;

"(C) delineate goals for—

"(i) closing the security vulnerabilities identified under subparagraph (B); and

"(ii) enhancing the ability of the Federal Government to constrain domestic and international

travel by terrorists and foreign fighters; and

"(D) describe the actions that will be taken to achieve the goals delineated under subparagraph (C) and the means needed to carry out such actions, including—

"(i) steps to reform, improve, and streamline existing Federal Government efforts to align with the current threat environment;

"(ii) new programs, projects, or activities that are requested, under development, or undergoing implementation;

"(iii) new authorities or changes in existing authorities needed from Congress;

"(iv) specific budget adjustments being requested to enhance United States security in a risk-based manner; and

"(v) the Federal departments and agencies responsible for the specific actions described in this subparagraph.

"(4) SUNSET.—The requirement to submit updated national strategies under this subsection shall terminate on the date that is seven years after the date of the enactment of this Act [Dec. 23, 2016].

"(c) DEVELOPMENT OF IMPLEMENTATION PLANS.—For each national strategy required under subsection (b), the President shall direct the heads of relevant Federal agencies to develop implementation plans for each such agency.

"(d) IMPLEMENTATION PLANS.—

"(1) IN GENERAL.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an implementation plan developed under subsection (c) with each national strategy required under subsection (b). Consistent with the protection of classified information, each such implementation plan shall be submitted in unclassified form, but may include a classified annex.

"(2) ANNUAL UPDATES.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an annual updated implementation plan during the ten-year period beginning on the date of the enactment of this Act [Dec. 23, 2016].

"(e) DEFINITION.—In this section, the term 'appropriate congressional committees' means—

"(1) in the House of Representatives—

"(A) the Committee on Homeland Security;

"(B) the Committee on Armed Services;

"(C) the Permanent Select Committee on Intelligence;

"(D) the Committee on the Judiciary;

"(E) the Committee on Foreign Affairs;

"(F) the Committee on Appropriations; and

"(2) in the Senate—

"(A) the Committee on Homeland Security and Governmental Affairs;

"(B) the Committee on Armed Services;

"(C) the Select Committee on Intelligence;

"(D) the Committee on the Judiciary;

"(E) the Committee on Foreign Relations; and

"(F) the Committee on Appropriations.

"(f) SPECIAL RULE FOR CERTAIN RECEIPT.—The definition under subsection (e) shall be treated as including the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate for purposes of receipt of those portions of—

"(1) the national strategy (including updates thereto), and

"(2) the implementation plan (including updates thereto),

required under this section that relate to maritime travel into and out of the United States."

[1] *See References in Text note below.*

§124. Homeland Security Advisory System

(a) Requirement

The Secretary shall administer the Homeland Security Advisory System in accordance with this section to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal, State, local, and tribal government authorities and to the people of the United States, as appropriate. The Secretary shall exercise primary responsibility for providing such advisories or warnings.

(b) Required elements

In administering the Homeland Security Advisory System, the Secretary shall—

(1) establish criteria for the issuance and revocation of such advisories or warnings;

(2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of such advisories or warnings;

(3) provide, in each such advisory or warning, specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable to enable individuals, government entities, emergency response providers, and the private sector to act appropriately;

(4) whenever possible, limit the scope of each such advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and

(5) not, in issuing any advisory or warning, use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

(Pub. L. 107–296, title II, §203, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 306.)

§124a. Homeland security information sharing

(a) Information sharing

Consistent with section 485 of this title, the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50) except for any internal security protocols or personnel information of such intelligence components, or other administrative processes that are administered by any chief security officer of the Department.

(b) Information sharing and knowledge management officers

For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3003(5) of title 50).

(c) State, local, and private-sector sources of information

(1) Establishment of business processes

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall—

(A) establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

(2) Feedback

The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of information provided by any entity of State, local, or tribal government or the private sector that provides such information to the Department.

(d) Training and evaluation of employees

(1) Training

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall provide to employees of the Department opportunities for training and education to develop an understanding of—

(A) the definitions of homeland security information and national intelligence (as defined in section 3003(5) of title 50); and

(B) how information available to such employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

(2) Evaluations

The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, as described in this subchapter, and participating in the information sharing environment established under section 485 of this title; and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

(Pub. L. 107–296, title II, §204, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 307; amended Pub. L. 115–278, §2(g)(2)(E), Nov. 16, 2018, 132 Stat. 4177.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in subsec. (d)(2)(A), was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c)(1), (d)(1). Pub. L. 115–278 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Assistant Secretary for Infrastructure Protection" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERVICE

Pub. L. 110–53, title V, §502(b), Aug. 3, 2007, 121 Stat. 311, provided that:

"(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall receive from the United States Secret Service homeland security information, terrorism information, weapons of mass destruction information (as these terms are defined in Section [sic] 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)), or national intelligence, as defined in Section [sic] 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)) [now 50 U.S.C. 3003(5)], as well as suspect information

obtained in criminal investigations. The United States Secret Service shall cooperate with the Under Secretary for Intelligence and Analysis with respect to activities under sections 204 and 205 of the Homeland Security Act of 2002 [6 U.S.C. 124a, 124b].

"(2) SAVINGS CLAUSE.—Nothing in this Act [see Tables for classification] shall interfere with the operation of Section [sic] 3056(g) of Title 18, United States Code, or with the authority of the Secretary of Homeland Security or the Director of the United States Secret Service regarding the budget of the United States Secret Service."

§124b. Comprehensive information technology network architecture

(a) Establishment

The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 485 of this title, and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department.

(b) Comprehensive information technology network architecture defined

The term "comprehensive information technology network architecture" means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic management and information resources management goals of the Office of Intelligence and Analysis.

(Pub. L. 107–296, title II, §205, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 308.)

§124c. Coordination with information sharing environment

(a) Guidance

All activities to comply with sections 124, 124a, and 124b of this title shall be—

(1) consistent with any policies, guidelines, procedures, instructions, or standards established under section 485 of this title;

(2) implemented in coordination with, as appropriate, the program manager for the information sharing environment established under that section;

(3) consistent with any applicable guidance issued by the Director of National Intelligence; and

(4) consistent with any applicable guidance issued by the Secretary relating to the protection of law enforcement information or proprietary information.

(b) Consultation

In carrying out the duties and responsibilities under this part, the Under Secretary for Intelligence and Analysis shall take into account the views of the heads of the intelligence components of the Department.

(Pub. L. 107–296, title II, §206, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 309.)

§124d. Intelligence components

Subject to the direction and control of the Secretary, and consistent with any applicable guidance issued by the Director of National Intelligence, the responsibilities of the head of each intelligence component of the Department are as follows:

(1) To ensure that the collection, processing, analysis, and dissemination of information within

the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence (as defined in section 3003(5) of title 50), are carried out effectively and efficiently in support of the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(2) To otherwise support and implement the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.

(4) To coordinate with the Under Secretary for Intelligence and Analysis in developing policies and requirements for the recruitment and selection of intelligence officials of the intelligence component.

(5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.

(6) To ensure that employees of the intelligence component have knowledge of, and comply with, the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that such employees comply with all applicable laws and regulations.

(7) To perform such other activities relating to such responsibilities as the Secretary may provide.

(Pub. L. 107–296, title II, §207, as added Pub. L. 110–53, title V, §503(a), Aug. 3, 2007, 121 Stat. 311.)

§124e. Training for employees of intelligence components

The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs that are related to the functions of the Department relating to the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50).

(Pub. L. 107–296, title II, §208, as added Pub. L. 110–53, title V, §503(a), Aug. 3, 2007, 121 Stat. 312.)

§124f. Intelligence training development for State and local government officials

(a) Curriculum

The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall—

(1) develop a curriculum for training State, local, and tribal government officials, including law enforcement officers, intelligence analysts, and other emergency response providers, in the intelligence cycle and Federal laws, practices, and regulations regarding the development, handling, and review of intelligence and other information; and

(2) ensure that the curriculum includes executive level training for senior level State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers.

(b) Training

To the extent possible, the Federal Law Enforcement Training Center and other existing Federal entities with the capacity and expertise to train State, local, and tribal government officials based on the curriculum developed under subsection (a) shall be used to carry out the training programs

created under this section. If such entities do not have the capacity, resources, or capabilities to conduct such training, the Secretary may approve another entity to conduct such training.

(c) Consultation

In carrying out the duties described in subsection (a), the Under Secretary for Intelligence and Analysis shall consult with the Director of the Federal Law Enforcement Training Center, the Attorney General, the Director of National Intelligence, the Administrator of the Federal Emergency Management Agency, and other appropriate parties, such as private industry, institutions of higher education, nonprofit institutions, and other intelligence agencies of the Federal Government.

(Pub. L. 107–296, title II, §209, as added Pub. L. 110–53, title V, §503(a), Aug. 3, 2007, 121 Stat. 312.)

§124g. Information sharing incentives

(a) Awards

In making cash awards under chapter 45 of title 5, the President or the head of an agency, in consultation with the program manager designated under section 485 of this title, may consider the success of an employee in appropriately sharing information within the scope of the information sharing environment established under that section, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50 [1], in a manner consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of that environment for the implementation and management of that environment.

(b) Other incentives

The head of each department or agency described in section 485(h) of this title, in consultation with the program manager designated under section 485 of this title, shall adopt best practices regarding effective ways to educate and motivate officers and employees of the Federal Government to participate fully in the information sharing environment, including—

(1) promotions and other nonmonetary awards; and

(2) publicizing information sharing accomplishments by individual employees and, where appropriate, the tangible end benefits that resulted.

(Pub. L. 107–296, title II, §210, as added Pub. L. 110–53, title V, §503(a), Aug. 3, 2007, 121 Stat. 313; amended Pub. L. 117–263, div. F, title LXVIII, §6811(c)(2), Dec. 23, 2022, 136 Stat. 3601.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–263 substituted "section 485(h) of this title" for "section 485(i) of this title" in introductory provisions.

[1] *So in original. A closing parenthesis probably should precede the comma.*

§124h. Department of Homeland Security State, Local, and Regional Fusion Center Initiative

(a) Establishment

The Secretary, in consultation with the program manager of the information sharing environment established under section 485 of this title, the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, shall establish a

Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

(b) Department support and coordination

Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

(7) provide management assistance to State, local, and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

(11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

(12) carry out such other duties as the Secretary determines are appropriate.

(c) Personnel assignment

(1) In general

The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.

(2) Personnel sources

Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

(A) Office of Intelligence and Analysis.

(B) Cybersecurity and Infrastructure Security Agency.

(C) Transportation Security Administration.

(D) United States Customs and Border Protection.

(E) United States Immigration and Customs Enforcement.

(F) United States Coast Guard.

(G) Other components of the Department, as determined by the Secretary.

(3) Qualifying criteria

(A) In general

The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.

(B) Criteria

Any criteria developed under subparagraph (A) may include—

(i) whether the fusion center, through its mission and governance structure, focuses on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;

(ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;

(iii) whether the fusion center has—

(I) access to relevant law enforcement, emergency response, private sector, open source, and national security data; and

(II) the ability to share and analytically utilize that data for lawful purposes;

(iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and

(v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

(4) Prerequisite

(A) Intelligence analysis, privacy, and civil liberties training

Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and

(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);

(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 142 of this title and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42; and

(iii) such other training prescribed by the Under Secretary for Intelligence and Analysis.

(B) Prior work experience in area

In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—

(i) has been previously assigned in the geographic area; or

(ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.

(5) Expedited security clearance processing

The Under Secretary for Intelligence and Analysis—

(A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and

(B) may request that security clearance processing be expedited for each such officer or intelligence analyst and may use available funds for such purpose.

(6) Further qualifications

Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other qualifications the Under Secretary for Intelligence and Analysis may prescribe.

(d) Responsibilities

An officer or intelligence analyst assigned to a fusion center under this section shall—

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

(3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; and

(4) assist in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies.

(e) Border intelligence priority

(1) In general

The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

(2) Border intelligence products

When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to participating State, local, and regional fusion centers under this section shall have, as a primary responsibility, the creation of border intelligence products that—

(A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

(f) Database access

In order to fulfill the objectives described under subsection (d), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

(g) Consumer feedback

(1) In general

The Secretary shall create a voluntary mechanism for any State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other information products referred to in subsection (d) to provide feedback to the Department on the quality and utility of such intelligence products.

(2) Report

Not later than one year after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

(h) Rule of construction

(1) In general

The authorities granted under this section shall supplement the authorities granted under section 121(d) of this title and nothing in this section shall be construed to abrogate the authorities granted under section 121(d) of this title.

(2) Participation

Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

(i) Guidelines

The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that any such fusion center shall—

(1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;

(2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;

(3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment;

(4) leverage the databases, systems, and networks available from public and private sector entities, in accordance with all applicable laws, to maximize information sharing;

(5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;

(6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private sector representatives at the fusion center;

(7) ensure appropriate security measures are in place for the facility, data, and personnel;

(8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;

(9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and

(10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

(j) Fusion center information sharing strategy

Not later than 1 year after March 2, 2020, and not less frequently than once every 5 years thereafter, the Secretary shall develop or update a strategy for Department engagement with fusion centers. Such strategy shall be developed and updated in consultation with the heads of intelligence

components of the Department, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, officials of fusion centers, officers designated as Homeland Security Advisors, and the heads of other relevant agencies, as appropriate. Such strategy shall include the following:

(1) Specific goals and objectives for sharing information and engaging with fusion centers—

(A) through the direct deployment of personnel from intelligence components of the Department;

(B) through the use of Department unclassified and classified information sharing systems, including the Homeland Security Information Network and the Homeland Secure Data Network, or any successor systems; and

(C) through any additional means.

(2) The performance metrics to be used to measure success in achieving the goals and objectives referred to in paragraph (1).

(3) A 5-year plan for continued engagement with fusion centers.

(k) Definitions

In this section—

(1) the term "fusion center" means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity;

(2) the term "information sharing environment" means the information sharing environment established under section 485 of this title;

(3) the term "intelligence analyst" means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

(4) the term "intelligence-led policing" means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; and

(5) the term "terrorism information" has the meaning given that term in section 485 of this title.

(l) Authorization of appropriations

There is authorized to be appropriated $10,000,000 for each of fiscal years 2008 through 2012, to carry out this section, except for subsection (i), including for hiring officers and intelligence analysts to replace officers and intelligence analysts who are assigned to fusion centers under this section.

(Pub. L. 107–296, title II, §210A, as added Pub. L. 110–53, title V, §511(a), Aug. 3, 2007, 121 Stat. 317; amended Pub. L. 115–278, §2(g)(2)(F), Nov. 16, 2018, 132 Stat. 4177; Pub. L. 116–116, §2, Mar. 2, 2020, 134 Stat. 110.)

EDITORIAL NOTES

AMENDMENTS

2020—Subsecs. (j) to (l). Pub. L. 116–116 added subsec. (j) and redesignated former subsecs. (j) and (k) as (k) and (l), respectively.

2018—Subsec. (c)(2)(B). Pub. L. 115–278 substituted "Cybersecurity and Infrastructure Security Agency" for "Office of Infrastructure Protection".

STATUTORY NOTES AND RELATED SUBSIDIARIES

OFFICE OF INTELLIGENCE AND ANALYSIS FIELD PERSONNEL SUPPORT TO FUSION CENTERS

Pub. L. 116–116, §3, Mar. 2, 2020, 134 Stat. 111, provided that:

"(a) PERFORMANCE METRICS.—Not later than 180 days after the date of the enactment of this Act [Mar. 2, 2020], the Under Secretary for Intelligence and Analysis shall—

"(1) consider the effectiveness of existing processes to identify and prepare field personnel for deployment to support fusion centers and internal mechanisms to ensure oversight and accountability of such field personnel, including field personnel assigned to one center and field personnel assigned to multiple centers; and

"(2) publish and disseminate performance metrics, taking into account, as appropriate, regional and threat diversity, for—

"(A) field personnel from the Office of Intelligence and Analysis assigned to an individual fusion center;

"(B) field personnel from the Office of Intelligence and Analysis assigned to multiple fusion centers; and

"(C) Regional Directors of the Office of Intelligence and Analysis to ensure accountability for monitoring all field personnel under the supervision of such Regional Directors.

"(b) TRAINING.—In consultation with the Chief Information Officer, the Under Secretary for Intelligence and Analysis shall develop and implement a formalized training module for fusion center personnel regarding the classified Homeland Secure Data Network, or any successor system.

"(c) FUSION CENTER DEFINED.—In this section, the term 'fusion center' has the meaning given such term in section 210A(k) of the Homeland Security Act of 2002 [6 U.S.C. 124h(k)], as so redesignated by section 2 [amending this section]."

TRAINING FOR PREDEPLOYED OFFICERS AND ANALYSTS

Pub. L. 110–53, title V, §511(b), Aug. 3, 2007, 121 Stat. 323, provided that: "An officer or analyst assigned to a fusion center by the Secretary of Homeland Security before the date of the enactment of this Act [Aug. 3, 2007] shall undergo the training described in section 210A(c)(4)(A) of the Homeland Security Act of 2002 [6 U.S.C. 124h(c)(4)(A)], as added by subsection (a), by not later than 6 months after such date."

§124h–1. Threat information sharing

(a) Prioritization

The Secretary of Homeland Security shall prioritize the assignment of officers and intelligence analysts under section 124h of this title from the Transportation Security Administration and, as appropriate, from the Office of Intelligence and Analysis of the Department of Homeland Security, to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset in order to enhance the security of such assets, including by improving timely sharing, in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, of information regarding threats of terrorism and other threats, including targeted violence.

(b) Intelligence products

Officers and intelligence analysts assigned to locations with participating State, local, and regional fusion centers under this section shall participate in the generation and dissemination of transportation security intelligence products, with an emphasis on such products that relate to threats of terrorism and other threats, including targeted violence, to surface transportation assets that—

(1) assist State, local, and Tribal law enforcement agencies in deploying their resources, including personnel, most efficiently to help detect, prevent, investigate, apprehend, and respond to such threats;

(2) promote more consistent and timely sharing with and among jurisdictions of threat information; and

(3) enhance the Department of Homeland Security's situational awareness of such threats.

(c) Clearances

The Secretary of Homeland Security shall make available to appropriate owners and operators of surface transportation assets, and to any other person that the Secretary determines appropriate to foster greater sharing of classified information relating to threats of terrorism and other threats,

including targeted violence, to surface transportation assets, the process of application for security clearances under Executive Order No. 13549 (75 Fed. Reg. 162; [1] relating to a classified national security information program) or any successor Executive order.

(d) Report to Congress

Not later than one year after December 27, 2021, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes a detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out this section.

(e) GAO report

Not later than two years after December 27, 2021, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a review of the implementation of this section, including an assessment of the measures used to ensure privacy rights, civil rights, and civil liberties protections, and any recommendations to improve this implementation, together with any recommendations to improve information sharing with State, local, Tribal, territorial, and private sector entities to prevent, identify, and respond to threats of terrorism and other threats, including targeted violence, to surface transportation assets.

(f) Definitions

In this section:

(1) The term "surface transportation asset" includes facilities, equipment, or systems used to provide transportation services by—

(A) a public transportation agency (as such term is defined in section 1131(5) of this title);

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49);

(C) an owner or operator of—

(i) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as such term is defined in section 1151(4) of this title); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(2) The term "targeted violence" means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(3) The term "terrorism" means the terms—

(A) domestic terrorism (as such term is defined in section 2331(5) of title 18, United States Code); and

(B) international terrorism (as such term is defined in section 2331(1) of title 18).

(Pub. L. 117–81, div. F, title LXIV, §6418, Dec. 27, 2021, 135 Stat. 2415.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order No. 13549, referred to in subsec. (c), is Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, which is set out as a note under section 3161 of Title 50, War and National Defense.

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *So in original. Probably should be "51609;".*

§124i. Homeland Security Information Sharing Fellows Program

(a) Establishment

(1) In general

The Secretary, acting through the Under Secretary for Intelligence and Analysis, and in consultation with the Chief Human Capital Officer, shall establish a fellowship program in accordance with this section for the purpose of—

(A) detailing State, local, and tribal law enforcement officers and intelligence analysts to the Department in accordance with subchapter VI of chapter 33 of title 5 to participate in the work of the Office of Intelligence and Analysis in order to become familiar with—

(i) the relevant missions and capabilities of the Department and other Federal agencies; and

(ii) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

(B) promoting information sharing between the Department and State, local, and tribal law enforcement officers and intelligence analysts by assigning such officers and analysts to—

(i) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;

(ii) identify information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is of interest to State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers;

(iii) assist Department analysts in preparing and disseminating products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal law enforcement officers and intelligence analysts and designed to prepare for and thwart acts of terrorism; and

(iv) assist Department analysts in preparing products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal emergency response providers and assist in the dissemination of such products through appropriate Department channels.

(2) Program name

The program under this section shall be known as the "Homeland Security Information Sharing Fellows Program".

(b) Eligibility

(1) In general

In order to be eligible for selection as an Information Sharing Fellow under the program under this section, an individual shall—

(A) have homeland security-related responsibilities;

(B) be eligible for an appropriate security clearance;

(C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis;

(D) be an employee of an eligible entity; and

(E) have undergone appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer and the Officer for Civil Rights and Civil Liberties, in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42.

(2) Eligible entities

In this subsection, the term "eligible entity" means—

(A) a State, local, or regional fusion center;

(B) a State or local law enforcement or other government entity that serves a major metropolitan area, suburban area, or rural area, as determined by the Secretary;

(C) a State or local law enforcement or other government entity with port, border, or agricultural responsibilities, as determined by the Secretary;

(D) a tribal law enforcement or other authority; or

(E) such other entity as the Secretary determines is appropriate.

(c) Optional participation

No State, local, or tribal law enforcement or other government entity shall be required to participate in the Homeland Security Information Sharing Fellows Program.

(d) Procedures for nomination and selection

(1) In general

The Under Secretary for Intelligence and Analysis shall establish procedures to provide for the nomination and selection of individuals to participate in the Homeland Security Information Sharing Fellows Program.

(2) Limitations

The Under Secretary for Intelligence and Analysis shall—

(A) select law enforcement officers and intelligence analysts representing a broad cross-section of State, local, and tribal agencies; and

(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis.

(Pub. L. 107–296, title II, §210B, as added Pub. L. 110–53, title V, §512(a), Aug. 3, 2007, 121 Stat. 324.)

§124j. Rural Policing Institute

(a) In general

The Secretary shall establish a Rural Policing Institute, which shall be administered by the Federal Law Enforcement Training Center, to target training to law enforcement agencies and other emergency response providers located in rural areas. The Secretary, through the Rural Policing Institute, shall—

(1) evaluate the needs of law enforcement agencies and other emergency response providers in rural areas;

(2) develop expert training programs designed to address the needs of law enforcement agencies and other emergency response providers in rural areas as identified in the evaluation conducted under paragraph (1), including training programs about intelligence-led policing and protections for privacy, civil rights, and civil liberties;

(3) provide the training programs developed under paragraph (2) to law enforcement agencies and other emergency response providers in rural areas; and

(4) conduct outreach efforts to ensure that local and tribal governments in rural areas are aware of the training programs developed under paragraph (2) so they can avail themselves of such programs.

(b) Curricula

The training at the Rural Policing Institute established under subsection (a) shall—

(1) be configured in a manner so as not to duplicate or displace any law enforcement or emergency response program of the Federal Law Enforcement Training Center or a local or tribal government entity in existence on August 3, 2007; and

(2) to the maximum extent practicable, be delivered in a cost-effective manner at facilities of

the Department, on closed military installations with adequate training facilities, or at facilities operated by the participants.

(c) Definition

In this section, the term "rural" means an area that is not located in a metropolitan statistical area, as defined by the Office of Management and Budget.

(d) Authorization of appropriations

There are authorized to be appropriated to carry out this section (including for contracts, staff, and equipment)—

(1) $10,000,000 for fiscal year 2008; and

(2) $5,000,000 for each of fiscal years 2009 through 2013.

(Pub. L. 107–296, title II, §210C, as added Pub. L. 110–53, title V, §513(a), Aug. 3, 2007, 121 Stat. 327.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

RURAL AREA

Pub. L. 112–74, div. D, title V, §546, Dec. 23, 2011, 125 Stat. 977, provided that: "For fiscal year 2012 and thereafter, for purposes of section 210C of the Homeland Security Act of 2002 (6 U.S.C. 124j), a rural area shall also include any area that is located in a metropolitan statistical area and a county, borough, parish, or area under the jurisdiction of an Indian tribe with a population of not more than 50,000."

§124k. Interagency Threat Assessment and Coordination Group

(a) In general

To improve the sharing of information within the scope of the information sharing environment established under section 485 of this title with State, local, tribal, and private sector officials, the Director of National Intelligence, through the program manager for the information sharing environment, in coordination with the Secretary, shall coordinate and oversee the creation of an Interagency Threat Assessment and Coordination Group (referred to in this section as the "ITACG").

(b) Composition of ITACG

The ITACG shall consist of—

(1) an ITACG Advisory Council to set policy and develop processes for the integration, analysis, and dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(2) an ITACG Detail comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work in the National Counterterrorism Center with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, through appropriate channels identified by the ITACG Advisory Council.

(c) Responsibilities of Secretary

The Secretary, or the Secretary's designee, in coordination with the Director of the National Counterterrorism Center and the ITACG Advisory Council, shall—

(1) create policies and standards for the creation of information products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are suitable for dissemination to State, local, and tribal governments and the private sector;

(2) evaluate and develop processes for the timely dissemination of federally-coordinated

information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal governments and the private sector;

(3) establish criteria and a methodology for indicating to State, local, and tribal governments and the private sector the reliability of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, disseminated to them;

(4) educate the intelligence community about the requirements of the State, local, and tribal homeland security, law enforcement, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(5) establish and maintain the ITACG Detail, which shall assign an appropriate number of State, local, and tribal homeland security and law enforcement officers and intelligence analysts to work in the National Counterterrorism Center who shall—

(A) educate and advise National Counterterrorism Center intelligence analysts about the requirements of the State, local, and tribal homeland security and law enforcement officers, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(B) assist National Counterterrorism Center intelligence analysts in integrating, analyzing, and otherwise preparing versions of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information that are unclassified or classified at the lowest possible level and suitable for dissemination to State, local, and tribal homeland security and law enforcement agencies in order to help deter and prevent terrorist attacks;

(C) implement, in coordination with National Counterterrorism Center intelligence analysts, the policies, processes, procedures, standards, and guidelines developed by the ITACG Advisory Council;

(D) assist in the dissemination of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal jurisdictions only through appropriate channels identified by the ITACG Advisory Council;

(E) make recommendations, as appropriate, to the Secretary or the Secretary's designee, for the further dissemination of intelligence products that could likely inform or improve the security of a State, local, or tribal government, (including a State, local, or tribal law enforcement agency) or a private sector entity; and

(F) report directly to the senior intelligence official from the Department under paragraph (6);

(6) detail a senior intelligence official from the Department of Homeland Security to the National Counterterrorism Center, who shall—

(A) manage the day-to-day operations of the ITACG Detail;

(B) report directly to the Director of the National Counterterrorism Center or the Director's designee; and

(C) in coordination with the Director of the Federal Bureau of Investigation, and subject to the approval of the Director of the National Counterterrorism Center, select a deputy from the pool of available detailees from the Federal Bureau of Investigation in the National Counterterrorism Center;

(7) establish, within the ITACG Advisory Council, a mechanism to select law enforcement officers and intelligence analysts for placement in the National Counterterrorism Center consistent with paragraph (5), using criteria developed by the ITACG Advisory Council that shall encourage participation from a broadly representative group of State, local, and tribal homeland security and law enforcement agencies; and

(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies) and private sector entities.

(d) Membership

The Secretary, or the Secretary's designee, shall serve as the chair of the ITACG Advisory Council, which shall include—

(1) representatives of—

(A) the Department;

(B) the Federal Bureau of Investigation;

(C) the National Counterterrorism Center;

(D) the Department of Defense;

(E) the Department of Energy;

(F) the Department of State; and

(G) other Federal entities as appropriate;

(2) the program manager of the information sharing environment, designated under section 485(f) of this title, or the program manager's designee; and

(3) executive level law enforcement and intelligence officials from State, local, and tribal governments.

(e) Criteria

The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the program manager of the information sharing environment established under section 485 of this title, shall—

(1) establish procedures for selecting members of the ITACG Advisory Council and for the proper handling and safeguarding of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by those members; and

(2) ensure that at least 50 percent of the members of the ITACG Advisory Council are from State, local, and tribal governments.

(f) Operations

(1) In general

Beginning not later than 90 days after August 3, 2007, the ITACG Advisory Council shall meet regularly, but not less than quarterly, at the facilities of the National Counterterrorism Center of the Office of the Director of National Intelligence.

(2) Management

Pursuant to section 3056(f)(E) [1] of title 50, the Director of the National Counterterrorism Center, acting through the senior intelligence official from the Department of Homeland Security detailed pursuant to subsection (d)(6),[2] shall ensure that—

(A) the products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, prepared by the National Counterterrorism Center and the ITACG Detail for distribution to State, local, and tribal homeland security and law enforcement agencies reflect the requirements of such agencies and are produced consistently with the policies, processes, procedures, standards, and guidelines established by the ITACG Advisory Council;

(B) in consultation with the ITACG Advisory Council and consistent with sections 3024(e)(1)(B)(iii) and 3056(f)(E) [1] of title 50, all products described in subparagraph (A) are disseminated through existing channels of the Department and the Department of Justice and other appropriate channels to State, local, and tribal government officials and other entities;

(C) all detailees under subsection (d)(5) [2] have appropriate access to all relevant information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, available at the National Counterterrorism Center in order to accomplish the objectives under that paragraph;

(D) all detailees under subsection (d)(5) [2] have the appropriate security clearances and are trained in the procedures for handling, processing, storing, and disseminating classified products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(E) all detailees under subsection (d)(5) [2] complete appropriate privacy and civil liberties training.

(g) Inapplicability of chapter 10 of title 5

Chapter 10 of title 5 shall not apply to the ITACG or any subsidiary groups thereof.

(h) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary for each of fiscal years 2008 through 2012 to carry out this section, including to obtain security clearances for the State, local, and tribal participants in the ITACG.

(Pub. L. 107–296, title II, §210D, as added Pub. L. 110–53, title V, §521(a), Aug. 3, 2007, 121 Stat. 328; amended Pub. L. 111–258, §5(b)(2), (c), Oct. 7, 2010, 124 Stat. 2650, 2651; Pub. L. 116–92, div. E, title LXVII, §6726(b), Dec. 20, 2019, 133 Stat. 2236; Pub. L. 117–286, §4(a)(12), Dec. 27, 2022, 136 Stat. 4306; Pub. L. 119–60, div. F, title LXIV, §6402(c)(2)(I), Dec. 18, 2025, 139 Stat. 1616.)

EDITORIAL NOTES

REFERENCES IN TEXT

Subsection (d)(5) and (6), referred to in subsec. (f)(2), was redesignated subsec. (c)(5) and (6), respectively, by Pub. L. 116–92, div. E, title LXVII, §6726(b)(2), Dec. 20, 2019, 133 Stat. 2236.

AMENDMENTS

2025—Subsec. (f)(2)(B). Pub. L. 119–60 substituted "sections 3024(e)(1)(B)(iii)" for "sections 3024(f)(1)(B)(iii)".

2022—Subsec. (g). Pub. L. 117–286, which directed amendment of subsec. (h) by substituting "chapter 10 of title 5" for "the Federal Advisory Committee Act" in heading and "Chapter 10 of title 5" for "The Federal Advisory Committee Act (5 U.S.C. App.)" in text, was executed by making the substitutions in subsec. (g) to reflect the probable intent of Congress and the prior amendment by Pub. L. 116–92. See 2019 Amendment below.

2019—Subsec. (c). Pub. L. 116–92, §6726(b)(1), (2), redesignated subsec. (d) as (c) and struck out former subsec. (c) which related to responsibilities of program manager.

Subsec. (c)(9). Pub. L. 116–92, §6726(b)(3), struck out par. (9) which read as follows: "provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2)."

Subsecs. (d) to (i). Pub. L. 116–92, §6726(b)(2), redesignated subsecs. (e) to (i) as (d) to (h), respectively.

2010—Subsec. (c). Pub. L. 111–258, §5(c)(1), struck out ", in consultation with the Information Sharing Council," after "program manager" in introductory provisions.

Subsec. (c)(3). Pub. L. 111–258, §5(c)(2)–(4), added par. (3).

Subsec. (d)(5)(E), (F). Pub. L. 111–258, §5(b)(2)(A), added subpar. (E) and redesignated former subpar. (E) as (F).

Subsec. (d)(8), (9). Pub. L. 111–258, §5(b)(2)(B)–(D), added pars. (8) and (9).

[1] *So in original. Probably should be section "3056(f)(1)(E)".*

[2] *See References in Text note below.*

§124*l*. Transferred

EDITORIAL NOTES

CODIFICATION

Section, Pub. L. 107–296, title II, §210E, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372, which related to national asset database, was renumbered section 2214 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(G), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 664 of this title.

§124m. Classified Information Advisory Officer

(a) Requirement to establish

The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

(b) Responsibilities

The responsibilities of the Classified Information Advisory Officer shall be as follows:

(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies) and private sector entities—

(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

(C) on the means by which such personnel may apply for security clearances.

(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

(c) Initial designation

Not later than 90 days after October 7, 2010, the Secretary shall—

(1) designate the initial Classified Information Advisory Officer; and

(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a written notification of the designation.

(Pub. L. 107–296, title II, §210E, formerly §210F, as added Pub. L. 111–258, §4(a), Oct. 7, 2010, 124 Stat. 2649; renumbered §210E, Pub. L. 115–278, §2(g)(2)(J), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 210E of Pub. L. 107–296, title II, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372, was renumbered section 2214 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(G), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 664 of this title.

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 111–258, §2, Oct. 7, 2010, 124 Stat. 2648, provided that: "Congress finds the following:

"(1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the '9/11 Commission') concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.

"(2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

"(3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.

"(4) Over-classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

"(5) Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification markings and the policies of the National Archives and Records Administration."

§124m–1. Departmental coordination on counter threats

(a) Establishment

There is authorized in the Department, for a period of 2 years beginning after December 27, 2020, a Counter Threats Advisory Board (in this section referred to as the "Board") which shall—

(1) be composed of senior representatives of departmental operational components and headquarters elements; and

(2) coordinate departmental intelligence activities and policy and information related to the mission and functions of the Department that counter threats.

(b) Charter

There shall be a charter to govern the structure and mission of the Board, which shall—

(1) direct the Board to focus on the current threat environment and the importance of aligning departmental activities to counter threats under the guidance of the Secretary; and

(2) be reviewed and updated as appropriate.

(c) Members

(1) In general

The Board shall be composed of senior representatives of departmental operational components and headquarters elements.

(2) Chair

The Under Secretary for Intelligence and Analysis shall serve as the Chair of the Board.

(3) Members

The Secretary shall appoint additional members of the Board from among the following:

(A) The Transportation Security Administration.
(B) U.S. Customs and Border Protection.
(C) U.S. Immigration and Customs Enforcement.
(D) The Federal Emergency Management Agency.
(E) The Coast Guard.
(F) U.S. Citizenship and Immigration Services.
(G) The United States Secret Service.
(H) The Cybersecurity and Infrastructure Security Agency.
(I) The Office of Operations Coordination.
(J) The Office of the General Counsel.

(K) The Office of Intelligence and Analysis.
(L) The Office of Strategy, Policy, and Plans.
(M) The Science and Technology Directorate.
(N) The Office for State and Local Law Enforcement.
(O) The Privacy Office.
(P) The Office for Civil Rights and Civil Liberties.
(Q) Other departmental offices and programs as determined appropriate by the Secretary.

(d) Meetings

The Board shall—

(1) meet on a regular basis to discuss intelligence and coordinate ongoing threat mitigation efforts and departmental activities, including coordination with other Federal, State, local, tribal, territorial, and private sector partners; and

(2) make recommendations to the Secretary.

(e) Terrorism alerts

The Board shall advise the Secretary on the issuance of terrorism alerts under section 124 of this title.

(f) Prohibition on additional funds

No additional funds are authorized to carry out this section.

(Pub. L. 107–296, title II, §210F, as added Pub. L. 116–260, div. U, title VI, §602(a), Dec. 27, 2020, 134 Stat. 2294.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 210F of Pub. L. 107–296 was renumbered section 210E and is classified to section 124m of this title.

STATUTORY NOTES AND RELATED SUBSIDIARIES

NOTICE REGARDING MECHANISMS TO COORDINATE THREATS

Pub. L. 116–260, div. U, title VI, §602(d), Dec. 27, 2020, 134 Stat. 2295, provided that: "The Secretary of Homeland Security shall provide written notification to and brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on any changes to or introductions of new mechanisms to coordinate threats across the Department of Homeland Security."

§124n. Protection of certain facilities and assets from unmanned aircraft

(a) Authorities

(1) Authority of the Department of Homeland Security and Department of Justice

Notwithstanding section 46502 of title 49 or sections 32, 1030, 1367 and chapters 119 and 206 of title 18, the Secretary and the Attorney General may, for their respective Departments, take and may authorize personnel to take such actions as are described in subsection (b)(1) that are necessary to enforce the law, protect the public, or to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(2) Authority of State, local, Tribal, and territorial law enforcement and correctional agencies

Notwithstanding section 46502 of title 49 or sections 32, 1030, 1367 and chapters 119 and 206 of title 18, notwithstanding the laws of any particular State, local, Tribal, or territorial jurisdiction,

and after completing the training detailed in subsection (d)(2), any State, local, Tribal, or territorial law enforcement or correctional agency may, subject to subsection (d)(2), take, and authorize personnel with assigned duties that include the security or protection of people, facilities, or assets, to take such actions as are described in subsection (b)(1) that are necessary to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of people, facilities, and assets, a venue or set of venues used for large-scale public gatherings or events, critical infrastructure, or correctional facilities.

(b) Actions described

(1) In general

The actions authorized in subsection (a) are the following:

(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, electromagnetic means, and through the use of remote identification broadcast or other means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) Required coordination

The Secretary and the Attorney General shall develop for their respective Departments the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(3) Research, testing, training, and evaluation

The Secretary and the Attorney General shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b)(1).

(4) Coordination

The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration when any action authorized by this section might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

(c) Forfeiture

(1) Federal agencies

Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary or the Attorney General pursuant to subsection (a)(1) is subject to forfeiture to the United States.

(2) Other agencies

Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by a State, local, Tribal, or territorial law enforcement or correctional agency pursuant to subsection (a)(2) is subject to forfeiture under the laws of the agency's jurisdiction.

(d) Regulations and guidance

(1) In general

The Secretary, the Attorney General, and the Secretary of Transportation may prescribe

regulations and shall issue guidance in the respective areas of each Secretary, the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency to carry out this section.

(2) State, local, Tribal, and territorial law enforcement training and certification

(A) Training and certification required

(i) In general

Only State, local, Tribal, or territorial law enforcement and correctional officers who have been trained and certified by the Attorney General, or the Attorney General's designee, in coordination with the Secretary of Homeland Security through a national schoolhouse which will serve as the sole certifying authority for State, local, Tribal, territorial, and correctional officers in the use of the authority granted under subsection (a)(2), may exercise authorities in subsection (b)(1)(C), (D), and (F).

(ii) Training and certification procedures

The Attorney General, in coordination with the Secretary of Homeland Security, the Secretary of Defense, and the Secretary of Transportation, shall, not later than 180 days after December 18, 2025, develop training and certification procedures for the use of the authority described in subsection (a)(2) that State, local, Tribal, and territorial law enforcement and correctional officers shall be required to satisfy before taking any actions described in subsection (b)(1).

(iii) Technologies

Technologies used by State, local, Tribal, and territorial law enforcement or correctional agencies to take actions described in subsection (b)(1) shall be limited to systems or technologies that are included on a list of authorized technologies maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation, the Federal Communications Commission, and the National Telecommunications and Information Administration.

(B) Oversight

The Attorney General, in coordination with the Secretary of Homeland Security and the Administrator of the Federal Aviation Administration, shall oversee compliance with the requirements set forth in subsection (e) with respect to the use of the authority granted under subsection (a)(2) by each State, local, Tribal, and territorial law enforcement agency that has been certified pursuant to the training and certification requirements described in subparagraph (A).

(C) State, local, Tribal, and territorial law enforcement and correctional agencies mitigation notification requirement

(i) In general

Any State, local, Tribal, or territorial law enforcement or correctional agency exercising authority under subsection (a)(2) shall, within 48 hours of taking any mitigation action described in subsection (b)(1), submit a notification to the Attorney General and the Secretary of Homeland Security containing—

(I) the date, time, and geographic location of the mitigation action;

(II) a brief description of the credible threat or safety concern necessitating such action;

(III) the type of mitigation capability employed; and

(IV) any known operational effects, including the seizure, disabling, or destruction of an unmanned aircraft system or unmanned aircraft.

(ii) Report mechanism

The Attorney General and the Secretary of Homeland Security shall establish a streamlined and secure submission mechanism to support the notification requirement under clause (i).

(D) Reports

Not later than 1 year after December 18, 2025, and biannually thereafter, the Attorney General, in coordination with the Secretary of Homeland Security and the Secretary of Transportation, shall submit to the appropriate congressional committees an unclassified report with a classified annex on activities carried out by State, local, Tribal, and territorial law and correctional enforcement agencies exercising the authority granted under subsection (a)(2) and subject to the training and certification requirements described in subparagraph (A), including—

(i) a description of the training and certification procedures developed and implemented pursuant to subparagraph (A)(ii);

(ii) a list of State, local, Tribal, and territorial law enforcement and correctional agencies that applied for and were certified to exercise the authorities granted by subsection (a)(2);

(iii) a list of currently authorized technologies pursuant to subparagraph (A)(iii);

(iv) the frequency, location, and circumstances of State, local, Tribal, territorial, and correctional officers mitigation deployments and types of mitigation employed;

(v) a list of any aviation security or safety incidents that occurred due to State, local, Tribal, territorial, and correctional officers deployment of counter-UAS technologies;

(vi) recommendations for improving State, local, Tribal, and territorial law and correctional agencies counter-UAS training, oversight, compliance, and execution and the compliance audits required by section 8606(b)(2) of the SAFER SKIES Act; and

(vii) a determination on if State, local, Tribal, and territorial law and correctional agencies are able to fully protect critical infrastructure from the drone threat and if not, recommendations on how to expand counter-UAS authorities to critical infrastructure owners.

(3) Coordination

(A) Coordination with Department of Transportation

The Secretary and the Attorney General shall coordinate the development of their respective guidance under paragraph (1) with the Secretary of Transportation.

(B) Effect on aviation safety

The Secretary and the Attorney General shall respectively coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, if such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(e) Privacy protection

The regulations or guidance issued to carry out actions authorized under subsection (b) by each Secretary, the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency, as the case may be, shall ensure that—

(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are intercepted or acquired only to the extent necessary to support an action described in subsection (b)(1);

(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary of Homeland Security, the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency determine [1] that maintenance of such records is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, is required under Federal, State, local, Tribal, or territorial law (as applicable), or for the purpose of any litigation;

(4) such communications are not disclosed outside the Department of Homeland Security [2] the

Department of Justice, or the State, local, Tribal, or territorial law enforcement or correctional agency unless the disclosure—

(A) is necessary to investigate or prosecute a violation of law;

(B) would support the Department of Defense, a Federal law enforcement agency, or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to an action described in subsection (b)(1);

(C) is between the Department of Homeland Security and the Department of Justice in the course of a security or protection operation of either agency or a joint operation of such agencies; or

(D) is otherwise required by law; and

(5) to the extent necessary, the Department of Homeland Security and the Department of Justice are authorized to share threat information, which shall not include communications other than those of an aeronautical communications system, as allowed for in section 2511(2)(g)(ii)(IV) of title 18 or information readily available to the public referred to in subsection (b), with State, local, territorial, or Tribal law enforcement agencies in the course of a security or protection operation.

(f) Budget

The Secretary and the Attorney General shall submit to Congress, as a part of the homeland security or justice budget materials for each fiscal year after fiscal year 2019, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of Homeland Security or the Department of Justice. The funding display shall be in unclassified form, but may contain a classified annex.

(g) Semiannual briefings and notifications

(1) In general

On a semiannual basis during the period beginning 6 months after October 5, 2018, and ending on the date specified in subsection (i), the Secretary and the Attorney General shall, respectively, provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section.

(2) Requirement

Each briefing required under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

(3) Content

Each briefing required under paragraph (1) shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances in which actions described in subsection (b)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

(C) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights or civil liberties;

(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1);

(E) a description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system were held for more than 180 days or shared outside of the Department of Justice or the Department of Homeland Security;

(F) how the Secretary, the Attorney General, and the Secretary of Transportation have informed the public as to the possible use of authorities under this section; [3]

(G) how the Secretary, the Attorney General, and the Secretary of Transportation have engaged with Federal, State, Tribal, territorial, and local law enforcement agencies to implement and use such authorities, including those exercised under subsection (a)(2).

(4) Unclassified form

Each briefing required under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

(5) Notification

Within 30 days of deploying any new technology to carry out the actions described in subsection (b)(1), the Secretary and the Attorney General shall, respectively, submit a notification to the appropriate congressional committees. Such notification shall include a description of options considered to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(h) Rule of construction

Nothing in this section may be construed to—

(1) vest in the Secretary or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration;

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary or the Attorney General;

(3) vest in the Secretary of Homeland Security any authority of the Attorney General;

(4) vest in the Attorney General any authority of the Secretary of Homeland Security; or

(5) provide a new basis of liability for any State, local, territorial, or tribal law enforcement officers who participate in the protection of a mass gathering identified by the Secretary or Attorney General under subsection (k)(3)(C)(iii)(II), act within the scope of their authority, and do not exercise the authority granted to the Secretary and Attorney General by this section.

(i) Applicability of other laws to activities related to the mitigation of threats from unmanned aircraft systems or unmanned aircraft

Sections 32, 1030, and 1367 and chapters 119 and 206 of title 18 and section 46502 of title 49 may not be construed to apply to activities of the Coast Guard, whether under this section or any other provision of law, that—

(1) are conducted outside the United States; and

(2) are related to the mitigation of threats from unmanned aircraft systems or unmanned aircraft.

(j) Terminations

(1) Counter-UAS authority

The authority to carry out this section with respect to a covered facility or asset, protecting the public, and enforcing the law shall terminate on September 30, 2031.

(2) State, local, tribal, and territorial law enforcement and correctional agencies

Authority of State, local, tribal, and territorial law enforcement and correctional agencies under subsection (a)(2) shall terminate on December 31, 2031.

(k) Scope of authority

Nothing in this section shall be construed to provide the Secretary or the Attorney General with additional authorities beyond those described in subsections (a) and (k)(3)(C)(iii).

(l) Definitions

In this section:

(1) The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Homeland Security, the Committee on Transportation and Infrastructure, the Committee on Energy and Commerce, and the Committee on the Judiciary of the House of Representatives.

(2) The term "budget", with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) The term "covered facility or asset" means any facility or asset that—

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section (except that in the case of the missions described in subparagraph (C)(i)(II) and (C)(iii)(I), such missions shall be presumed to be for the protection of a facility or asset that is assessed to be high-risk and a potential target for unlawful unmanned aircraft activity);

(B) is located in the United States (including the territories and possessions, territorial seas or navigable waters of the United States); and

(C) directly relates to a Federal law enforcement, correctional, and homeland security agency mission necessary to enforce the law, protect the public or to one or more—

(i) missions authorized to be performed by the Department of Homeland Security, consistent with governing statutes, regulations, and orders issued by the Secretary, pertaining to—

(I) security or protection functions of the U.S. Customs and Border Protection, including securing or protecting facilities, aircraft, and vessels, whether moored or underway;

(II) United States Secret Service protection operations pursuant to sections 3056(a) and 3056A(a) of title 18 and the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note); or

(III) protection of facilities pursuant to section 1315(a) of title 40;

(ii) missions authorized to be performed by the Department of Justice, consistent with governing statutes, regulations, and orders issued by the Attorney General, pertaining to—

(I) personal protection operations by—

(aa) the Federal Bureau of Investigation as specified in section 533 of title 28; and

(bb) the United States Marshals Service of Federal jurists, court officers, witnesses, and other threatened persons in the interests of justice, as specified in section 566(e)(1)(A) of title 28;

(II) protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons; or

(III) protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice, and the provision of security for Federal courts, as specified in section 566(a) of title 28;

(iii) missions authorized to be performed by the Department of Homeland Security or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and orders issued by the Secretary or the Attorney General, respectively, pertaining to—

(I) protection of a National Special Security Event and Special Event Assessment Rating event;

(II) the provision of support to State, local, territorial, or tribal law enforcement, upon request of the chief executive officer of the State or territory, to ensure protection of people

and property at mass gatherings, that is limited to a specified timeframe and location, within available resources, and without delegating any authority under this section to State, local, territorial, or tribal law enforcement; or

(III) protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified timeframe and location; and [4]

(iv) missions authorized to be performed by the United States Coast Guard, including those described in clause (iii) as directed by the Secretary, and as further set forth in section 104 [5] of title 14, and consistent with governing statutes, regulations, and orders issued by the Secretary of the Department in which the Coast Guard is operating.

(4) The terms "electronic communication", "intercept", "oral communication", and "wire communication" have the meaning [6] given those terms in section 2510 of title 18.

(5) The term "homeland security or justice budget materials", with respect to a fiscal year, means the materials submitted to Congress by the Secretary and the Attorney General in support of the budget for that fiscal year.

(6)(A) For purposes of subsection (a)(1), the term "personnel" means officers, employees, contractors, detailed personnel, and deputized personnel who perform Federal law enforcement, correctional, homeland or national security duties.

(B) For purposes of subsection (a)(2), the term "personnel" means officers and employees of State, local, Tribal, and territorial law enforcement and correctional agencies.

(7) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801,[7] of title 49.

(8) For purposes of this section, the term "risk-based assessment" includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Secretary or the Attorney General, respectively, of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the use of any system or technology for carrying out the actions described in subsection (b)(1).

(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(C) Potential consequences of the impacts of any actions taken under subsection (b)(1) to the national airspace system and infrastructure if not mitigated.

(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and any potential for interference with wireless communications or for injury or damage to persons or property.

(F) The setting, character, timeframe, and national airspace system impacts of National Special Security Event and Special Event Assessment Rating events.

(G) Potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated.

(9) The term "correctional facility" means any jail, prison, or any other penal or detention facility operated by a State, local, Tribal, or territorial law enforcement agency, or by a private party that is under contract with a State, local, Tribal, or territorial law enforcement agency, and

used to house individuals who have been arrested, detained, held, or charged with or convicted of criminal offenses.

(10) The term "critical infrastructure" has the meaning given the term in subsection (e) of section 5195c of title 42.

(m) Department of Homeland Security assessment

(1) Report

Not later than 1 year after October 5, 2018, the Secretary shall conduct, in coordination with the Attorney General and the Secretary of Transportation, an assessment to the appropriate congressional committees, including—

(A) an evaluation of the threat from unmanned aircraft systems to United States critical infrastructure (as defined in this chapter) and to domestic large hub airports (as defined in section 40102 of title 49);

(B) an evaluation of current Federal and [8] State, local, territorial, or tribal law enforcement authorities to counter the threat identified in subparagraph (A), and recommendations, if any, for potential changes to existing authorities to allow State, local, territorial, and tribal law enforcement to assist Federal law enforcement to counter the threat where appropriate;

(C) an evaluation of the knowledge of, efficiency of, and effectiveness of current procedures and resources available to owners of critical infrastructure and domestic large hub airports when they believe a threat from unmanned aircraft systems is present and what additional actions, if any, the Department of Homeland Security or the Department of Transportation could implement under existing authorities to assist these entities to counter the threat identified in subparagraph (A);

(D) an assessment of what, if any, additional authorities are needed by each Department and law enforcement to counter the threat identified in subparagraph (A); and

(E) an assessment of what, if any, additional research and development the Department needs to counter the threat identified in subparagraph (A).

(2) Unclassified form

The report required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(n) Reimbursement program

Not later than 180 days of after December 18, 2025, the Secretary of Homeland Security and the Attorney General shall provide the appropriate congressional committees with a plan to establish a reimbursement program for Federal agencies providing counter-UAS protection to events that are not organized or operated by the Federal Government.

(Pub. L. 107–296, title II, §210G, as added Pub. L. 115–254, div. H, §1602(a), Oct. 5, 2018, 132 Stat. 3522; amended Pub. L. 118–15, div. B, title II, §2221, Sept. 30, 2023, 137 Stat. 86; Pub. L. 118–22, div. B, title III, §601, Nov. 17, 2023, 137 Stat. 123; Pub. L. 118–35, div. B, title III, §301, Jan. 19, 2024, 138 Stat. 7; Pub. L. 118–41, title III, §301, Mar. 8, 2024, 138 Stat. 24; Pub. L. 118–63, title XI, §1112, May 16, 2024, 138 Stat. 1419; Pub. L. 118–83, div. B, title I, §101, Sept. 26, 2024, 138 Stat. 1534; Pub. L. 118–158, div. E, §5102, Dec. 21, 2024, 138 Stat. 1771; Pub. L. 119–4, div. C, §3102, Mar. 15, 2025, 139 Stat. 46; Pub. L. 119–60, div. H, title LXXXVI, §8602, Dec. 18, 2025, 139 Stat. 1938.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 8606(b)(2) of the SAFER SKIES Act, referred to in subsec. (d)(2)(D)(vi), is section 8606(b)(2) of Pub. L. 119–60, div. H, title LXXXVI, which is set out in a note below.

The Presidential Protection Assistance Act of 1976, referred to in subsec. (l)(3)(C)(i)(II), is Pub. L. 94–524, Oct. 17, 1976, 90 Stat. 2475, which enacted and amended provisions set out as notes under section 3056 of Title 18, Crimes and Criminal Procedure. For complete classification of this Act to the Code, see Tables.

Section 104 of title 14, referred to in subsec. (l)(3)(C)(iv), was redesignated section 528 of title 14 by Pub. L. 115–282, title I, §105(b), Dec. 4, 2018, 132 Stat. 4200, and references to section 104 of title 14 deemed to refer to such redesignated section, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

This chapter, referred to in subsec. (m)(1)(A), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2025—Subsec. (a). Pub. L. 119–60, §8602(1), added subsec. (a) and struck out former subsec. (a) which related to the authorities of the Secretary and the Attorney General.

Subsec. (b)(1)(B). Pub. L. 119–60, §8602(2), substituted "electromagnetic means, and through the use of remote identification broadcast or other means" for "and electromagnetic means".

Subsec. (c). Pub. L. 119–60, §8602(3), inserted "pursuant to subsection (a)(1)" after "Attorney General", designated existing provisions as par. (1) and inserted heading, and added par. (2).

Subsec. (d)(1). Pub. L. 119–60, §8602(4)(A), substituted ", the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency" for "or the Attorney General".

Subsec. (d)(2), (3). Pub. L. 119–60, §8602(4)(B), (C), added par. (2) and redesignated former par. (2) as (3).

Subsec. (e). Pub. L. 119–60, §8602(5)(A), substituted ", the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency" for "or the Attorney General" in introductory provisions.

Subsec. (e)(3). Pub. L. 119–60, §8602(5)(B), substituted ", the Attorney General, or any State, local, Tribal, or territorial law enforcement or correctional agency" for "or the Attorney General" and inserted ", State, local, Tribal, or territorial" after "Federal" and "(as applicable)" after "law".

Subsec. (e)(4). Pub. L. 119–60, §8602(5)(C), substituted "the Department of Justice, or the State, local, Tribal, or territorial law enforcement or correctional agency" for "or the Department of Justice" in introductory provisions.

Subsec. (e)(5). Pub. L. 119–60, §8602(5)(D), substituted "Tribal" for "tribal" and inserted "other than those of an aeronautical communications system, as allowed for in section 2511(2)(g)(ii)(IV) of title 18 or information readily available to the public" after "which shall not include communications".

Subsec. (g)(3)(G). Pub. L. 119–60, §8602(6), inserted "Tribal, territorial," after "State," and ", including those exercised under subsection (a)(2)" after "authorities".

Subsec. (i). Pub. L. 119–60, §8602(8), added subsec. (i) and struck out former subsec. (i). Prior to amendment, text read as follows: "The authority to carry out this section with respect to a covered facility or asset specified in subsection (k)(3) shall terminate on September 30, 2025"

Pub. L. 119–4 substituted "September 30, 2025" for "March 14, 2025".

Subsec. (j). Pub. L. 119–60, §8602(8), added subsec. (j). Former subsec. (j) redesignated (k).

Subsecs. (k), (l). Pub. L. 119–60, §8602(7), redesignated subsecs. (j) and (k) as (k) and (l), respectively.

Subsec. (l)(3)(C). Pub. L. 119–60, §8602(9)(A), inserted "a Federal law enforcement, correctional, and homeland security agency mission necessary to enforce the law, protect the public or to" after "directly relates to".

Subsec. (l)(6). Pub. L. 119–60, §8602(9)(B), added par. (6) and struck out former par. (6) which read as follows: "For purposes of subsection (a), the term 'personnel' means officers and employees of the Department of Homeland Security or the Department of Justice."

Subsec. (l)(9), (10). Pub. L. 119–60, §8602(9)(C), added pars. (9) and (10).

Subsec. (n). Pub. L. 119–60, §8602(10), added subsec. (n).

2024—Subsec. (i). Pub. L. 118–158 substituted "March 14, 2025" for "December 20, 2024".

Pub. L. 118–83 substituted "December 20, 2024" for "October 1, 2024".

Pub. L. 118–63 substituted "October 1, 2024" for "May 11, 2024".

Pub. L. 118–41 substituted "May 11, 2024" for "March 9, 2024".

Pub. L. 118–35 substituted "March 9, 2024" for "February 3, 2024".

2023—Subsec. (i). Pub. L. 118–22 substituted "February 3, 2024" for "November 18, 2023".

Pub. L. 118–15 substituted "on November 18, 2023" for "on the date that is 4 years after October 5, 2018".

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION DATE

Pub. L. 117–328, div. F, title V, §547, Dec. 29, 2022, 136 Stat. 4758, provided that former subsec. (i) of

this section would be applied by substituting "September 30, 2023" for "the date that is 4 years after the date of enactment of this section".

RULEMAKING AND IMPLEMENTATION

Pub. L. 119–60, div. H, title LXXXVI, §8606, Dec. 18, 2025, 139 Stat. 1944, provided that:

"(a) RULEMAKING AUTHORITY.—

"(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act [Dec. 18, 2025], the Secretary of Homeland Security and the Attorney General, in coordination with the Secretary of Defense and the Secretary of Transportation, shall develop and publish regulations governing counter-UAS authority for SLTT law enforcement agencies and correctional agencies under this title [see Short Title of 2025 Amendment note set out under section 101 of this title] and the amendments made by this title.

"(2) ROLE OF FAA.—In carrying out the rulemaking in paragraph (1), the Secretary of Homeland Security and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration on any aspect of the rulemaking that affects aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

"(3) SAVING CLAUSE.—Nothing in this section shall be construed to vest in the Secretary or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration.

"(4) AUTHORIZED EQUIPMENT AND TECHNOLOGY.—The Secretary of Homeland Security, the Attorney General, the Secretary of Defense, in coordination with the Administrator of the Federal Aviation Administration, the Chairman of the Federal Communications Commission, and the Administrator of National Telecommunications and Information Administrator shall authorize equipment and technology to be used for actions in subparagraphs (B), (C), (D), and (F) of section 210G(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 124n(b)(1)].

"(b) TRAINING AND COMPLIANCE.—

"(1) IN GENERAL.—The Attorney General, in coordination with the Secretary of Homeland Security, the Secretary of Defense, and the Department of Transportation, shall approve standards for training programs for SLTT law enforcement agencies or correctional agencies for the safe and lawful interception of drones. Such training programs shall include instruction on the legal, operational, and technological aspects of counter-UAS operations.

"(2) COMPLIANCE AUDITS.—The Attorney General and the Secretary of Homeland Security shall periodically conduct compliance audits to prevent misuse of counter-UAS authority.

"(c) DEFINITIONS.—In this section:

"(1) SLTT LAW ENFORCEMENT AGENCY.—The term 'SLTT law enforcement agency' means a State, local, Tribal, or territorial law enforcement agency.

"(2) CORRECTIONAL AGENCY.—The term 'correctional agency' means a Federal, State, local, Tribal, or territorial government body responsible for operating correctional facilities or a private party that is under contract with a State, local, Tribal, or territorial law enforcement agency to operate such facilities.

"(3) CORRECTIONAL FACILITY.—The term 'correctional facility' means any jail, prison, or any other penal or detention facility operated by a State, local, Tribal, or territorial law enforcement agency, or by a private party that is under contract with a State, local, Tribal, or territorial law enforcement agency, and used to house individuals who have been arrested, detained, held, or charged with or convicted of criminal offenses."

SEVERABILITY

Pub. L. 119–60, div. H, title LXXXVI, §8607, Dec. 18, 2025, 139 Stat. 1945, provided that: "If any provision of this title [see Short Title of 2025 Amendment note set out under section 101 of this title], or the application of any provision of this title to any person or circumstance is held invalid, the application of such provision or circumstance and the remainder of this title shall not be affected thereby."

[1] So in original. Probably should be "determines".

[2] So in original. Probably should be followed by a comma.

[3] So in original. Probably should be followed by "and".

[4] So in original. Probably should be "or".

[5] *See References in Text note below.*

[6] *So in original. Probably should be "meanings".*

[7] *So in original. The comma probably should not appear.*

[8] *So in original. Probably should be "Federal,".*

§124n–1. Penalties

(a) Definition

In this section, the term "unmanned aircraft" has the meaning given the term in section 44801 of title 49.

(b) Omitted

(c) Increased penalties for operation of unmanned aircraft to facilitate felony offense

If a person who is convicted of a felony offense (other than an offense based solely on the operation of an unmanned aircraft) knowingly operated an unmanned aircraft during, in relation to, or in furtherance of such offense, the maximum imprisonment otherwise provided by law for that offense shall be doubled or increased by 5 years, whichever is less.

(d) Increased penalties for use of unmanned aircraft to introduce contraband into prisons

If a defendant who is convicted under section 1791 of title 18 knowingly used an unmanned aircraft to provide a prohibited object to an inmate of a prison, the maximum imprisonment otherwise provided by law for that offense shall be increased by 5 years.

(e) Directive to United States Sentencing Commission: enhanced sentencing range for use of unmanned aircraft

(1) In general

To carry out the purposes of this section, during the Sentencing Commission's amendment cycle in progress at the time this Act is enacted, the Commission shall, under section 994 of title 28—

(A) promulgate guidelines, or amendments to guidelines, that substantially increase the sentencing range for all offenses involving the use of an unmanned aircraft; and

(B) as necessary, promulgate policy statements, or amendments to policy statements to assist in the application of this section.

(2) Enhanced penalties

In any case in which the enhanced penalties of subsection (c) apply, the guidelines and amendments issued under paragraph (1) shall call for an increase of at least 6 levels in the base offense level and in all other cases, the base offense level shall be increased by at least 4 levels.

(f) Penalties for unauthorized counter-UAS actions

Any entity or individual authorized to take such actions to mitigate the threat posed by an unmanned aircraft system or unmanned aircraft pursuant to section 124n of this title who knowingly engages in such actions without Federal coordination as required by those statutes, shall be subject to—

(1) a civil fine up to $100,000 per violation; or

(2) suspension of counter-UAS authority pending review by the Attorney General or Secretary of Homeland Security.

(g) Civil enforcement

The Attorney General is authorized to bring a civil action in a United States district court to collect fines and enforce civil penalties imposed under this section.

(h) Effective date

This section and the amendments made by this section shall take effect 30 days after December 18, 2025.

(Pub. L. 119–60, div. H, title LXXXVI, §8605, Dec. 18, 2025, 139 Stat. 1943.)

CODIFICATION

Section was enacted as part of the SAFER SKIES Act, and also as part of the National Defense Authorization Act for Fiscal Year 2026, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Section is comprised of section 8605 of Pub. L. 119–60. Subsec. (b) of section 8605 of Pub. L. 119–60 amended section 46307 of Title 49, Transportation. Subsec. (e) of section 8605 of Pub. L. 119–60 is also listed in a table relating to sentencing guidelines set out under section 994 of Title 28, Judiciary and Judicial Procedure.

§125. Annual report on intelligence activities of the Department of Homeland Security

(a) In general

For each fiscal year and along with the budget materials submitted in support of the budget of the Department of Homeland Security pursuant to section 1105(a) of title 31, the Under Secretary for Intelligence and Analysis of the Department shall submit to the congressional intelligence committees a report for such fiscal year on each intelligence activity of each intelligence component of the Department, as designated by the Under Secretary, that includes the following:

(1) The amount of funding requested for each such intelligence activity.

(2) The number of full-time employees funded to perform each such intelligence activity.

(3) The number of full-time contractor employees (or the equivalent of full-time in the case of part-time contractor employees) funded to perform or in support of each such intelligence activity.

(4) A determination as to whether each such intelligence activity is predominantly in support of national intelligence or departmental missions.

(5) The total number of analysts of the Intelligence Enterprise of the Department that perform—

(A) strategic analysis; or

(B) operational analysis.

(b) Feasibility and advisability report

Not later than 120 days after December 19, 2014, the Secretary of Homeland Security, acting through the Under Secretary for Intelligence and Analysis, shall submit to the congressional intelligence committees a report that—

(1) examines the feasibility and advisability of including the budget request for all intelligence activities of each intelligence component of the Department that predominantly support departmental missions, as designated by the Under Secretary for Intelligence and Analysis, in the Homeland Security Intelligence Program; and

(2) includes a plan to enhance the coordination of department-wide intelligence activities to achieve greater efficiencies in the performance of the Department of Homeland Security intelligence functions.

(c) Intelligence component of the Department

In this section, the term "intelligence component of the Department" has the meaning given that term in section 101 of this title.

(Pub. L. 113–293, title III, §324, Dec. 19, 2014, 128 Stat. 4004.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

BRIEFING ON DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ACTIVITIES

Pub. L. 117–263, div. F, title LXVIII, §6819, Dec. 23, 2022, 136 Stat. 3611, provided that:

"(a) DEFINITIONS.—In this section:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means the following:

"(A) The congressional intelligence committees.

"(B) The Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate.

"(C) The Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

"(2) COMPONENT OF THE DEPARTMENT OF HOMELAND SECURITY.—The term 'component of the Department of Homeland Security' means the following components of the Department of Homeland Security:

"(A) The Cybersecurity and Infrastructure Security Agency Threat Management Division.

"(B) The Federal Emergency Management Agency Protection and National Preparedness, Office of Counterterrorism and Security Preparedness.

"(C) The Transportation Security Administration Office of Intelligence and Analysis.

"(D) The United States Citizenship and Immigration Services Fraud Detection and National Security Directorate, Field Operations Directorate, and Collateral Duty Intelligence.

"(E) The United States Customs and Border Protection Office of Intelligence.

"(F) The United States Immigration and Customs Enforcement Homeland Security Investigations, Office of Intelligence, and Special Agent in Charge Intelligence Program.

"(3) INTELLIGENCE ACTIVITY.—The term 'intelligence activity' shall be interpreted consistent with how such term is used in section 502 of the National Security Act of 1947 (50 U.S.C. 3092).

"(b) BRIEFING ON INTELLIGENCE ACTIVITIES.—Consistent with section 501 of the National Security Act of 1947 (50 U.S.C. 3091), not later than 30 days after the date of the enactment of this Act [Dec. 23, 2022], the Chief Intelligence Officer of the Department of Homeland Security shall provide the appropriate congressional committees a briefing on the intelligence activities of elements of the Department of Homeland Security that are not elements of the intelligence community. Such briefing shall include the following:

"(1) A comprehensive description of all intelligence activities conducted during the period beginning on January 1, 2018, and ending on the date of the briefing, by any component of the Department of Homeland Security that conducts intelligence activities.

"(2) With respect to each such intelligence activity, a description of the activity, including, at a minimum—

"(A) the nature of the activity;

"(B) the component undertaking the activity;

"(C) the legal authority for such activity; and

"(D) the source of funding for such activity.

"(3) A description and the quantity of any types of finished intelligence products, or intelligence information reports, produced or contributed to by a component of the Department of Homeland Security that conducts intelligence activities during the period specified in paragraph (1).

"(4) An identification of any external or internal guidelines, policies, processes, practices, or programs governing the collection, retention, analysis, or dissemination by such a component of information regarding United States citizens, lawful permanent residents of the United States, or individuals located within the United States.

"(c) FORM.—The briefing under subsection (b) may be provided in classified form.

"(d) ADDITIONAL BRIEFINGS.—Not later than 1 year after the date on which the Chief Intelligence Officer provides the briefing under subsection (b) and not less frequently than once each year thereafter, the Chief Intelligence Officer shall provide the appropriate congressional committees a briefing on any new intelligence activities commenced by any component of the Department of Homeland Security and any that have been terminated."

[For definitions of "congressional intelligence committees" and "intelligence community" as used in section

6819 of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of Title 50, War and National Defense.]

DEFINITIONS

"Congressional intelligence committees" means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives, see section 2 of Pub. L. 113–293, set out as a note under section 3003 of Title 50, War and National Defense.

§126. Department of Homeland Security data framework

(a) In general

(1) Development

The Secretary of Homeland Security shall develop a data framework to integrate existing Department of Homeland Security datasets and systems, as appropriate, for access by authorized personnel in a manner consistent with relevant legal authorities and privacy, civil rights, and civil liberties policies and protections.

(2) Requirements

In developing the framework required under paragraph (1), the Secretary of Homeland Security shall ensure, in accordance with all applicable statutory and regulatory requirements, the following information is included:

(A) All information acquired, held, or obtained by an office or component of the Department of Homeland Security that falls within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence.

(B) Any information or intelligence relevant to priority mission needs and capability requirements of the homeland security enterprise, as determined appropriate by the Secretary.

(b) Data framework access

(1) In general

The Secretary of Homeland Security shall ensure that the data framework required under this section is accessible to employees of the Department of Homeland Security who the Secretary determines—

(A) have an appropriate security clearance;

(B) are assigned to perform a function that requires access to information in such framework; and

(C) are trained in applicable standards for safeguarding and using such information.

(2) Guidance

The Secretary of Homeland Security shall—

(A) issue guidance for Department of Homeland Security employees authorized to access and contribute to the data framework pursuant to paragraph (1); and

(B) ensure that such guidance enforces a duty to share between offices and components of the Department when accessing or contributing to such framework for mission needs.

(3) Efficiency

The Secretary of Homeland Security shall promulgate data standards and instruct components of the Department of Homeland Security to make available information through the data framework required under this section in a machine-readable standard format, to the greatest extent practicable.

(c) Exclusion of information

The Secretary of Homeland Security may exclude information from the data framework required under this section if the Secretary determines inclusion of such information may—

(1) jeopardize the protection of sources, methods, or activities;
(2) compromise a criminal or national security investigation;
(3) be inconsistent with other Federal laws or regulations; or
(4) be duplicative or not serve an operational purpose if included in such framework.

(d) Safeguards

The Secretary of Homeland Security shall incorporate into the data framework required under this section systems capabilities for auditing and ensuring the security of information included in such framework. Such capabilities shall include the following:

(1) Mechanisms for identifying insider threats.
(2) Mechanisms for identifying security risks.
(3) Safeguards for privacy, civil rights, and civil liberties.

(e) Deadline for implementation

Not later than 2 years after December 19, 2018, the Secretary of Homeland Security shall ensure the data framework required under this section has the ability to include appropriate information in existence within the Department of Homeland Security to meet the critical mission operations of the Department of Homeland Security.

(f) Notice to Congress

(1) Status updates

The Secretary of Homeland Security shall submit to the appropriate congressional committees regular updates on the status of the data framework until the framework is fully operational.

(2) Operational notification

Not later than 60 days after the date on which the data framework required under this section is fully operational, the Secretary of Homeland Security shall provide notice to the appropriate congressional committees that the data framework is fully operational.

(3) Value added

The Secretary of Homeland Security shall annually brief Congress on component use of the data framework required under this section to support operations that disrupt terrorist activities and incidents in the homeland.

(g) Definitions

In this section:

(1) Appropriate congressional committee; homeland

The terms "appropriate congressional committee" and "homeland" have the meaning given those terms in section 101 of this title.

(2) Homeland security information

The term "homeland security information" has the meaning given such term in section 482 of this title.

(3) National intelligence

The term "national intelligence" has the meaning given such term in section 3003(5) of title 50.

(4) Terrorism information

The term "terrorism information" has the meaning given such term in section 485 of this title.

(Pub. L. 115–331, §2, Dec. 19, 2018, 132 Stat. 4484.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Data Framework Act of 2018, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PART B—INFORMATION SECURITY

EDITORIAL NOTES

CODIFICATION

Subtitle C of title II of Pub. L. 107–296, which was classified to part C of this subchapter, was redesignated subtitle B of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

PRIOR PROVISIONS

A prior subtitle B of title II of Pub. L. 107–296, which was classified to this part, was redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to part B (§671 et seq.) of subchapter XVIII of this chapter.

§§131 to 134. Transferred

EDITORIAL NOTES

CODIFICATION

Section 131, Pub. L. 107–296, title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961, which related to definitions, was renumbered section 2222 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 671 of this title.

Section 132, Pub. L. 107–296, title II, §213, Nov. 25, 2002, 116 Stat. 2152, which related to designation of critical infrastructure protection program, was renumbered section 2223 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 672 of this title.

Section 133, Pub. L. 107–296, title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 112–199, title I, §111, Nov. 27, 2012, 126 Stat. 1472, which related to protection of voluntarily shared critical infrastructure information, was renumbered section 2224 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 673 of this title.

Section 134, Pub. L. 107–296, title II, §215, Nov. 25, 2002, 116 Stat. 2155, which prohibited the construction of former part B as creating a private right of action for enforcement of any provision of this chapter, was renumbered section 2225 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 674 of this title.

§141. Procedures for sharing information

The Secretary shall establish procedures on the use of information shared under this subchapter that—

(1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of such information;

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(Pub. L. 107–296, title II, §221, Nov. 25, 2002, 116 Stat. 2155.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

§142. Privacy officer

(a) Appointment and responsibilities

The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. 552a];

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974 [5 U.S.C. 552a], internal controls, and other matters.

(b) Authority to investigate

(1) In general

The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

(2) Enforcement of subpoenas

Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

(3) Effect of oaths

Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an

employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

(c) Supervision and coordination

(1) In general

The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.

(2) Coordination with the Inspector General

(A) In general

Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

(B) Coordination

(i) Referral

Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

(ii) Determinations and notifications by the Inspector General

(I) In general

Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

(II) Investigation not initiated

If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this subclause shall be made not later than 3 days after the end of that 90-day period.

(iii) Investigation by senior official

The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

(iv) Privacy training

Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

(d) Notification to Congress on removal

If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

(e) Reports by senior official to Congress

The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

(Pub. L. 107–296, title II, §222, Nov. 25, 2002, 116 Stat. 2155; Pub. L. 108–458, title VIII, §8305, Dec. 17, 2004, 118 Stat. 3868; Pub. L. 110–53, title VIII, §802, Aug. 3, 2007, 121 Stat. 358.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsec. (a)(2), (6), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

AMENDMENTS

2007—Pub. L. 110–53 designated existing provisions as subsec. (a), inserted heading, and added subsecs. (b) to (e).

2004—Pub. L. 108–458, §8305(1), inserted ", who shall report directly to the Secretary," after "in the Department" in introductory provisions.

Pars. (5), (6). Pub. L. 108–458, §8305(2)–(4), added par. (5) and redesignated former par. (5) as (6).

§§143 to 145. Transferred

EDITORIAL NOTES

CODIFICATION

Section 143, Pub. L. 107–296, title II, §223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, §2(e)(3)(A), Dec. 18, 2014, 128 Stat. 3086, which related to enhancement of Federal and non-Federal cybersecurity, was renumbered section 2205 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 655 of this title.

Section 144, Pub. L. 107–296, title II, §224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334, which related to NET Guard, was renumbered section 2206 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 656 of this title.

Section 145, Pub. L. 107–296, title II, §225, Nov. 25, 2002, 116 Stat. 2156, which related to Cyber Security Enhancement Act of 2002, was renumbered section 2207 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 657 of this title.

§146. Cybersecurity workforce assessment and strategy

(a) Workforce assessment

(1) In general

Not later than 180 days after December 18, 2014, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.

(2) Contents

The assessment required under paragraph (1) shall include, at a minimum—

(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;

(B) information on where cybersecurity workforce positions are located within the Department;

(C) information on which cybersecurity workforce positions are—

(i) performed by—

(I) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about such employees;

(II) independent contractors; and

(III) individuals employed by other Federal agencies, including the National Security Agency; or

(ii) vacant; and

(D) information on—

(i) the percentage of individuals within each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(ii) in cases in which such essential training was not received, what challenges, if any, were encountered with respect to the provision of such essential training.

(b) Workforce strategy

(1) In general

The Secretary shall—

(A) not later than 1 year after December 18, 2014, develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).

(2) Contents

The comprehensive workforce strategy developed under paragraph (1) shall include a description of—

(A) a multi-phased recruitment plan, including with respect to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

(B) a 5-year implementation plan;

(C) a 10-year projection of the cybersecurity workforce needs of the Department;

(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and

(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill any such gap.

(c) Updates

The Secretary submit [1] to the appropriate congressional committees annual updates on—

(1) the cybersecurity workforce assessment required under subsection (a); and

(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required

to be developed under subsection (b).

(Pub. L. 113–246, §3, Dec. 18, 2014, 128 Stat. 2880.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Cybersecurity Workforce Assessment Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

HOMELAND SECURITY CYBERSECURITY WORKFORCE ASSESSMENT

Pub. L. 113–277, §4, Dec. 18, 2014, 128 Stat. 3008, provided that:

"(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Workforce Assessment Act'.

"(b) DEFINITIONS.—In this section:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(B) the Committee on Homeland Security of the House of Representatives; and

"(C) the Committee on House Administration of the House of Representatives.

"(2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPECIALTY AREA .—The terms 'Cybersecurity Work Category', 'Data Element Code', and 'Specialty Area' have the meanings given such terms in the Office of Personnel Management's Guide to Data Standards.

"(3) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

"(4) DIRECTOR.—The term 'Director' means the Director of the Office of Personnel Management.

"(5) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(c) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.—

"(1) IN GENERAL.—The Secretary shall—

"(A) identify all cybersecurity workforce positions within the Department;

"(B) determine the primary Cybersecurity Work Category and Specialty Area of such positions; and

"(C) assign the corresponding Data Element Code, as set forth in the Office of Personnel Management's Guide to Data Standards which is aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report, in accordance with paragraph (2).

"(2) EMPLOYMENT CODES.—

"(A) PROCEDURES.—Not later than 90 days after the date of the enactment of this Act [Dec. 18, 2014], the Secretary shall establish procedures—

"(i) to identify open positions that include cybersecurity functions (as defined in the OPM Guide to Data Standards); and

"(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

"(B) CODE ASSIGNMENTS.—Not later than 9 months after the date of the enactment of this Act, the Secretary shall assign the appropriate employment code to—

"(i) each employee within the Department who carries out cybersecurity functions; and

"(ii) each open position within the Department that have been identified as having cybersecurity functions.

"(3) PROGRESS REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director shall submit a progress report on the implementation of this subsection to the appropriate congressional committees.

"(d) IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL NEED.—

"(1) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to subsection (c)(2)(B), and annually through 2021, the Secretary, in consultation with the Director, shall—

"(A) identify Cybersecurity Work Categories and Specialty Areas of critical need in the Department's cybersecurity workforce; and

"(B) submit a report to the Director that—

"(i) describes the Cybersecurity Work Categories and Specialty Areas identified under subparagraph (A); and

"(ii) substantiates the critical need designations.

"(2) GUIDANCE.—The Director shall provide the Secretary with timely guidance for identifying Cybersecurity Work Categories and Specialty Areas of critical need, including—

"(A) current Cybersecurity Work Categories and Specialty Areas with acute skill shortages; and

"(B) Cybersecurity Work Categories and Specialty Areas with emerging skill shortages.

"(3) CYBERSECURITY CRITICAL NEEDS REPORT.—Not later than 18 months after the date of the enactment of this Act, the Secretary, in consultation with the Director, shall—

"(A) identify Specialty Areas of critical need for cybersecurity workforce across the Department; and

"(B) submit a progress report on the implementation of this subsection to the appropriate congressional committees.

"(e) GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.—The Comptroller General of the United States shall—

"(1) analyze and monitor the implementation of subsections (c) and (d); and

"(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation."

DEFINITIONS

Pub. L. 113–246, §2, Dec. 18, 2014, 128 Stat. 2880, provided that: "In this Act [enacting this section and provisions set out as a note under section 101 of this title]—

"(1) the term 'Cybersecurity Category' means a position's or incumbent's primary work function involving cybersecurity, which is further defined by Specialty Area;

"(2) the term 'Department' means the Department of Homeland Security;

"(3) the term 'Secretary' means the Secretary of Homeland Security; and

"(4) the term 'Specialty Area' means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report."

[1] *So in original.*

§§147 to 151. Transferred

EDITORIAL NOTES

CODIFICATION

Section 147, Pub. L. 107–296, title II, §226, as added Pub. L. 113–277, §3(a), Dec. 18, 2014, 128 Stat. 3005, which related to cybersecurity recruitment and retention, was renumbered section 2208 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 658 of this title.

Section 148, Pub. L. 107–296, title II, §227, formerly §226, as added Pub. L. 113–282, §3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered §227 and amended Pub. L. 114–113, div. N, title II, §§203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963; Pub. L. 114–328, div. A, title XVIII, §1841(b), Dec. 23, 2016, 130 Stat. 2663, which related to national cybersecurity and communications integration center, was renumbered section 2209 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 659 of this title.

A prior section 227 of Pub. L. 107–296, as added by Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070, was classified to section 149 of this title prior to redesignation by Pub. L. 114–113 as section 228(c) of Pub. L. 107–296, and was classified to section 149(c) of this title prior to further redesignation by Pub. L. 115–278 as section 2210(c) of Pub. L. 107–296, which is classified to section 660(c) of this title.

Section 149, Pub. L. 107–296, title II, §228, as added and amended Pub. L. 114–113, div. N, title II, §§205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964, which related to cybersecurity plans, was renumbered section 2210 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 660 of this title.

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and was classified to section 150 of

this title prior to renumbering as section 2212, which is classified to section 662 of this title.

Section 149a, Pub. L. 107–296, title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683, which related to cybersecurity strategy, was renumbered section 2211 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 661 of this title.

Section 150, Pub. L. 107–296, title II, §229, formerly §228, as added Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered §229, Pub. L. 114–113, div. N, title II, §223(a)(1), Dec. 18, 2015, 129 Stat. 2963, which related to clearances, was renumbered section 2212 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 662 of this title.

Section 151, Pub. L. 107–296, title II, §230, as added Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which related to Federal intrusion detection and prevention system, was renumbered section 2213 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 663 of this title.

PART C—OFFICE OF SCIENCE AND TECHNOLOGY

EDITORIAL NOTES

CODIFICATION

Subtitle D of title II of Pub. L. 107–296, which was classified to part D of this subchapter, was redesignated subtitle C of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

PRIOR PROVISIONS

A prior subtitle C of title II of Pub. L. 107–296, which was classified to this part, was redesignated subtitle B of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to part B (§141 et seq.) of this subchapter.

§161. Establishment of Office; Director

(a) Establishment

(1) In general

There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this subchapter referred to as the "Office").

(2) Authority

The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be established within the National Institute of Justice.

(b) Director

The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

(Pub. L. 107–296, title II, §231, Nov. 25, 2002, 116 Stat. 2159.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in subsec. (a)(1), was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review,

Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

§162. Mission of Office; duties

(a) Mission

The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) Duties

In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of chapter 10 of title 5) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113). The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical

assistance and training materials for law enforcement personnel, including prosecutors.

(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.

(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.

(12) To support research fellowships in support of its mission.

(13) To serve as a clearinghouse for information on law enforcement technologies.

(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.

(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.

(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

(c) Competition required

Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis.

(d) Information from Federal agencies

Federal agencies shall, upon request from the Office and in accordance with Federal law, provide the Office with any data, reports, or other information requested, unless compliance with such request is otherwise prohibited by law.

(e) Publications

Decisions concerning publications issued by the Office shall rest solely with the Director of the Office.

(f) Transfer of funds

The Office may transfer funds to other Federal agencies or provide funding to non-Federal entities through grants, cooperative agreements, or contracts to carry out its duties under this section: *Provided*, That any such transfer or provision of funding shall be carried out in accordance with section 605 of Public Law 107–77.

(g) Annual report

The Director of the Office shall include with the budget justification materials submitted to Congress in support of the Department of Justice budget for each fiscal year (as submitted with the budget of the President under section 1105(a) of title 31) a report on the activities of the Office. Each such report shall include the following:

(1) For the period of 5 fiscal years beginning with the fiscal year for which the budget is submitted—

(A) the Director's assessment of the needs of Federal, State, and local law enforcement agencies for assistance with respect to law enforcement technology and other matters consistent with the mission of the Office; and

(B) a strategic plan for meeting such needs of such law enforcement agencies.

(2) For the fiscal year preceding the fiscal year for which such budget is submitted, a description of the activities carried out by the Office and an evaluation of the extent to which those activities successfully meet the needs assessed under paragraph (1)(A) in previous reports.

(Pub. L. 107–296, title II, §232, Nov. 25, 2002, 116 Stat. 2159; Pub. L. 108–7, div. L, §103(1), Feb. 20, 2003, 117 Stat. 529; Pub. L. 117–286, §4(a)(13), Dec. 27, 2022, 136 Stat. 4306.)

EDITORIAL NOTES

REFERENCES IN TEXT

The National Technology Transfer and Advancement Act of 1995, referred to in subsec. (b)(3), (4), is Pub. L. 104–113, Mar. 7, 1996, 110 Stat. 775, as amended. For complete classification of this Act to the Code, see Short Title of 1996 Amendment note set out under section 3701 of Title 15, Commerce and Trade, and Tables.

Section 605 of Public Law 107–77, referred to in subsec. (f), is section 605 of Pub. L. 107–77, title VI, Nov. 28, 2001, 115 Stat. 798, which is not classified to the Code.

AMENDMENTS

2022—Subsec. (b)(2). Pub. L. 117–286 substituted "chapter 10 of title 5)" for "the Federal Advisory Committee Act (5 U.S.C. App.))".

2003—Subsec. (f). Pub. L. 108–7 inserted before period at end ": *Provided*, That any such transfer or provision of funding shall be carried out in accordance with section 605 of Public Law 107–77".

§163. Definition of law enforcement technology

For the purposes of this subchapter, the term "law enforcement technology" includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

(Pub. L. 107–296, title II, §233, Nov. 25, 2002, 116 Stat. 2161.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

§164. Abolishment of Office of Science and Technology of National Institute of Justice; transfer of functions

(a) Authority to transfer functions

The Attorney General may transfer to the Office any other program or activity of the Department of Justice that the Attorney General, in consultation with the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, determines to be consistent with the mission of the Office.

(b) Transfer of personnel and assets

With respect to any function, power, or duty, or any program or activity, that is established in the Office, those employees and assets of the element of the Department of Justice from which the transfer is made that the Attorney General determines are needed to perform that function, power, or duty, or for that program or activity, as the case may be, shall be transferred to the Office: *Provided*, That any such transfer shall be carried out in accordance with section 605 of Public Law 107–77.

(c) Report on implementation

Not later than 1 year after November 25, 2002, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the implementation of this subchapter. The report shall—

(1) provide an accounting of the amounts and sources of funding available to the Office to carry out its mission under existing authorizations and appropriations, and set forth the future funding needs of the Office; and

(2) include such other information and recommendations as the Attorney General considers

appropriate.

(Pub. L. 107–296, title II, §234, Nov. 25, 2002, 116 Stat. 2161; Pub. L. 108–7, div. L, §103(2), Feb. 20, 2003, 117 Stat. 529.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 605 of Public Law 107–77, referred to in subsec. (b), is section 605 of Pub. L. 107–77, title VI, Nov. 28, 2001, 115 Stat. 798, which is not classified to the Code.

This subchapter, referred to in subsec. (c), was in the original "this title", meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2003—Subsec. (b). Pub. L. 108–7 inserted before period at end ": *Provided*, That any such transfer shall be carried out in accordance with section 605 of Public Law 107–77".

§165. National Law Enforcement and Corrections Technology Centers

(a) In general

The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as "Centers") and, to the extent necessary, establish new centers through a merit-based, competitive process.

(b) Purpose of Centers

The purpose of the Centers shall be to—

(1) support research and development of law enforcement technology;

(2) support the transfer and implementation of technology;

(3) assist in the development and dissemination of guidelines and technological standards; and

(4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

(c) Annual meeting

Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

(d) Report

Not later than 12 months after November 25, 2002, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

(Pub. L. 107–296, title II, §235, Nov. 25, 2002, 116 Stat. 2162.)

SUBCHAPTER III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

§181. Under Secretary for Science and Technology

There shall be in the Department a Directorate of Science and Technology headed by an Under Secretary for Science and Technology.

(Pub. L. 107–296, title III, §301, Nov. 25, 2002, 116 Stat. 2163.)

§182. Responsibilities and authorities of the Under Secretary for Science and Technology

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1) advising the Secretary regarding research and development efforts and priorities in support of the Department's missions;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the Director of the Cybersecurity and Infrastructure Security Agency, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 8401 of title 7;

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as "select agents" in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 262a of title 42;

(10) supporting United States leadership in science and technology;

(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;

(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs;

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research

conducted or sponsored by the Department; and

(15) carrying out, in coordination with the Drug Enforcement Administration, research, development, testing, evaluation, and cost-benefit analyses to improve the safety, effectiveness, and efficiency of equipment and the effectiveness and efficiency of reference libraries for use by Federal, State, local, Tribal, and territorial law enforcement agencies for the accurate detection of drugs, such as fentanyl and xylazine, including—

(A) portable equipment that can detect and identify drugs with minimal or no handling of the sample;

(B) equipment that can separate complex mixtures containing low concentrations of drugs and high concentrations of cutting agents into their component parts to enable signature extraction for field identification and detection; and

(C) technologies that use machine learning or artificial intelligence (as defined in section 9401 of title 15) and other techniques to predict whether the substances in a sample are controlled substance analogues or other new psychoactive substances not yet included in available reference libraries.

(Pub. L. 107–296, title III, §302, Nov. 25, 2002, 116 Stat. 2163; Pub. L. 109–347, title V, §501(b)(2), Oct. 13, 2006, 120 Stat. 1935; Pub. L. 110–53, title V, §531(b)(1)(C), Aug. 3, 2007, 121 Stat. 334; Pub. L. 115–278, §2(g)(3)(A), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 118–186, §2, Dec. 23, 2024, 138 Stat. 2636.)

EDITORIAL NOTES

AMENDMENTS

2024—Par. (15). Pub. L. 118–186 added par. (15).

2018—Par. (2). Pub. L. 115–278, §2(g)(3)(A)(i), substituted "biological," for "biological,,".

Par. (3). Pub. L. 115–278, §2(g)(3)(A)(ii), substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Assistant Secretary for Infrastructure Protection".

Par. (5)(A). Pub. L. 115–278, §2(g)(3)(A)(i), substituted "biological," for "biological,,".

2007—Par. (3). Pub. L. 110–53 substituted "Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection" for "Under Secretary for Information Analysis and Infrastructure Protection".

2006—Pars. (2), (5)(A). Pub. L. 109–347 struck out "radiological, nuclear" after "biological,".

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 118–186, §4, Dec. 23, 2024, 138 Stat. 2637, provided that: "Nothing in this Act [amending this section and enacting provisions set out as a note below] may be construed to limit the authority of agencies currently managing, overseeing, or otherwise involved in drug equipment and reference libraries."

REQUIREMENTS

Pub. L. 118–186, §3, Dec. 23, 2024, 138 Stat. 2637, provided that: "In carrying out section 302(15) of the Homeland Security Act of 2002 [6 U.S.C. 182(15)], as added by section 2, the Under Secretary for Science and Technology shall—

"(1) follow the recommendations, guidelines, and best practices described in the Artificial Intelligence Risk Management Framework (NIST AI 100–1) or any successor document published by the National Institute of Standards and Technology; and

"(2) establish the Directorate of Science and Technology's research, development, testing, evaluation, and cost-benefit analysis priorities under such section 302(15) based on the latest available information, including specific drugs identified as threats in—

"(A) the latest Homeland Threat Assessment published by the Department of Homeland Security;

"(B) the latest State and Territory Report on Enduring and Emerging Threats published by the Drug Enforcement Administration; or

"(C) any successor documents."

§183. Functions transferred

In accordance with subchapter XII, there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of the following entities:

(1) The following programs and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto (but not including programs and activities relating to the strategic nuclear defense posture of the United States):

(A) The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program.

(B) The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program. The programs and activities described in this subparagraph may be designated by the President either for transfer to the Department or for joint operation by the Secretary and the Secretary of Energy.

(C) The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program.

(D) Such life sciences activities of the biological and environmental research program related to microbial pathogens as may be designated by the President for transfer to the Department.

(E) The Environmental Measurements Laboratory.

(F) The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.

(2) The National Bio-Weapons Defense Analysis Center of the Department of Defense, including the functions of the Secretary of Defense related thereto.

(Pub. L. 107–296, title III, §303, Nov. 25, 2002, 116 Stat. 2164.)

§184. Conduct of certain public health-related activities

(a) In general

With respect to civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities, goals, objectives, and policies and develop a coordinated strategy for such activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed pursuant to section 182(2) of this title.

(b) Evaluation of progress

In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in such subsection.

(Pub. L. 107–296, title III, §304, Nov. 25, 2002, 116 Stat. 2165.)

EDITORIAL NOTES

CODIFICATION

Section is comprised of section 304 of Pub. L. 107–296. Subsec. (c) of section 304 of Pub. L. 107–296 amended section 233 of Title 42, The Public Health and Welfare.

§185. Federally funded research and development centers

The Secretary, acting through the Under Secretary for Science and Technology, shall have the authority to establish or contract with 1 or more federally funded research and development centers

to provide independent analysis of homeland security issues, or to carry out other responsibilities under this chapter, including coordinating and integrating both the extramural and intramural programs described in section 188 of this title.

(Pub. L. 107–296, title III, §305, Nov. 25, 2002, 116 Stat. 2168.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§186. Miscellaneous provisions

(a) Classification

To the greatest extent practicable, research conducted or supported by the Department shall be unclassified.

(b) Construction

Nothing in this subchapter shall be construed to preclude any Under Secretary of the Department from carrying out research, development, demonstration, or deployment activities, as long as such activities are coordinated through the Under Secretary for Science and Technology.

(c) Regulations

The Secretary, acting through the Under Secretary for Science and Technology, may issue necessary regulations with respect to research, development, demonstration, testing, and evaluation activities of the Department, including the conducting, funding, and reviewing of such activities.

(d) Notification of Presidential life sciences designations

Not later than 60 days before effecting any transfer of Department of Energy life sciences activities pursuant to section 183(1)(D) of this title, the President shall notify the appropriate congressional committees of the proposed transfer and shall include the reasons for the transfer and a description of the effect of the transfer on the activities of the Department of Energy.

(Pub. L. 107–296, title III, §306, Nov. 25, 2002, 116 Stat. 2168.)

§187. Homeland Security Advanced Research Projects Agency

(a) Definitions

In this section:

(1) Fund

The term "Fund" means the Acceleration Fund for Research and Development of Homeland Security Technologies established in subsection (c).

(2) Homeland security research

The term "homeland security research" means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.

(3) HSARPA

The term "HSARPA" means the Homeland Security Advanced Research Projects Agency established in subsection (b).

(4) Under Secretary

The term "Under Secretary" means the Under Secretary for Science and Technology.

(b) Homeland Security Advanced Research Projects Agency

(1) Establishment

There is established the Homeland Security Advanced Research Projects Agency.

(2) Director

HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary.

(3) Responsibilities

The Director shall administer the Fund to award competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including businesses, federally funded research and development centers, and universities. The Director shall administer the Fund to—

(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;

(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies;

(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities; and

(D) conduct research and development for the purpose of advancing technology for the investigation of child exploitation crimes, including child victim identification, trafficking in persons, and child pornography, and for advanced forensics.

(4) Targeted competitions

The Director may solicit proposals to address specific vulnerabilities identified by the Director.

(5) Coordination

The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies.

(6) Personnel

In hiring personnel for HSARPA, the Secretary shall have the hiring and management authorities described in section 1101 [1] of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.

(7) Demonstrations

The Director, periodically, shall hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel.

(c) Fund

(1) Establishment

There is established the Acceleration Fund for Research and Development of Homeland Security Technologies, which shall be administered by the Director of HSARPA.

(2) Authorization of appropriations

There are authorized to be appropriated $500,000,000 to the Fund for fiscal year 2003 and such sums as may be necessary thereafter.

(3) Coast Guard

Of the funds authorized to be appropriated under paragraph (2), not less than 10 percent of such funds for each fiscal year through fiscal year 2005 shall be authorized only for the Under

Secretary, through joint agreement with the Commandant of the Coast Guard, to carry out research and development of improved ports, waterways and coastal security surveillance and perimeter protection capabilities for the purpose of minimizing the possibility that Coast Guard cutters, aircraft, helicopters, and personnel will be diverted from non-homeland security missions to the ports, waterways and coastal security mission.

(Pub. L. 107–296, title III, §307, Nov. 25, 2002, 116 Stat. 2168; Pub. L. 114–22, title III, §302(c), formerly §302(d), May 29, 2015, 129 Stat. 255; renumbered §302(d), Pub. L. 115–392, §23(c)(2), Dec. 21, 2018, 132 Stat. 5264.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, referred to in subsec. (b)(6), is section 1101 of Pub. L. 105–261, which was formerly set out as a note under section 3104 of Title 5, Government Organization and Employees, prior to repeal by Pub. L. 114–328, div. A, title XI, §1121(b), Dec. 23, 2016, 130 Stat. 2452. See section 4092 of Title 10, Armed Forces.

AMENDMENTS

2015—Subsec. (b)(3)(D). Pub. L. 114–22 added subpar. (D).

[1] *See References in Text note below.*

§188. Conduct of research, development, demonstration, testing and evaluation

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the responsibilities under section 182(4) of this title through both extramural and intramural programs.

(b) Extramural programs

(1) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—

(A) ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practicable participate;

(B) ensure that the research funded is of high quality, as determined through merit review processes developed under section 182(14) of this title; and

(C) distribute funds through grants, cooperative agreements, and contracts.

(2) University-based centers for homeland security

(A) Designation

The Secretary, acting through the Under Secretary for Science and Technology, shall designate a university-based center or several university-based centers for homeland security. The purpose of the center or these centers shall be to establish a coordinated, university-based system to enhance the Nation's homeland security.

(B) Criteria for designation

Criteria for the designation of colleges or universities as a center for homeland security, shall include, but are not limited to, demonstrated expertise in—

(i) The training of first responders.

(ii) Responding to incidents involving weapons of mass destruction and biological warfare.

(iii) Emergency and diagnostic medical services.

(iv) Chemical, biological, radiological, and nuclear countermeasures or detection.

(v) Animal and plant health and diagnostics.

(vi) Food safety.
(vii) Water and wastewater operations.
(viii) Port and waterway security.
(ix) Multi-modal transportation.
(x) Information security and information engineering.
(xi) Engineering.
(xii) Educational outreach and technical assistance.
(xiii) Border transportation and security.
(xiv) The public policy implications and public dissemination of homeland security related research and development.

(C) Discretion of Secretary

To the extent that exercising such discretion is in the interest of homeland security, and with respect to the designation of any given university-based center for homeland security, the Secretary may except certain criteria as specified in subparagraph (B) and consider additional criteria beyond those specified in subparagraph (B). Upon designation of a university-based center for homeland security, the Secretary shall that day publish in the Federal Register the criteria that were excepted or added in the selection process and the justification for the set of criteria that were used for that designation.

(D) Report to Congress

The Secretary shall report annually, from the date of enactment, to Congress concerning the implementation of this section. That report shall indicate which center or centers have been designated and how the designation or designations enhance homeland security, as well as report any decisions to revoke or modify such designations.

(E) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this paragraph.

(c) Intramural programs

(1) Consultation

In carrying out the duties under section 182 of this title, the Secretary, acting through the Under Secretary for Science and Technology, may draw upon the expertise of any laboratory of the Federal Government, whether operated by a contractor or the Government.

(2) Laboratories

The Secretary, acting through the Under Secretary for Science and Technology, may establish a headquarters laboratory for the Department at any laboratory or site and may establish additional laboratory units at other laboratories or sites.

(3) Criteria for headquarters laboratory

If the Secretary chooses to establish a headquarters laboratory pursuant to paragraph (2), then the Secretary shall do the following:

(A) Establish criteria for the selection of the headquarters laboratory in consultation with the National Academy of Sciences, appropriate Federal agencies, and other experts.
(B) Publish the criteria in the Federal Register.
(C) Evaluate all appropriate laboratories or sites against the criteria.
(D) Select a laboratory or site on the basis of the criteria.
(E) Report to the appropriate congressional committees on which laboratory was selected, how the selected laboratory meets the published criteria, and what duties the headquarters laboratory shall perform.

(4) Limitation on operation of laboratories

No laboratory shall begin operating as the headquarters laboratory of the Department until at least 30 days after the transmittal of the report required by paragraph (3)(E).

(d) Preference for United States industry

(1) Definitions

In this subsection:

(A) Country of concern

The term "country of concern" means a country that—

(i) is a covered nation, as such term is defined in section 4872(d) of title 10; or

(ii) the Secretary determines is engaged in conduct that is detrimental to the national security of the United States.

(B) Nonprofit organization; small business firm; subject invention

The terms "nonprofit organization", "small business firm", and "subject invention" have the meanings given such terms in section 201 of title 35.

(C) Manufactured substantially in the United States

The term "manufactured substantially in the United States" means an item is a domestic end product.

(D) Domestic end product

The term "domestic end product" has the meaning given such term in section 25.003 of title 48, Code of Federal Regulations, or any successor thereto.

(3) [1] Waivers

(A) In general

Subject to subparagraph (B), in individual cases, the requirements under section 204 of title 35 may be waived by the Secretary upon a showing by the small business firm, nonprofit organization, or assignee that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that under the circumstances domestic manufacture is not commercially feasible.

(B) Conditions on waivers granted by Department

(i) Before grant of waiver

Before granting a waiver under subparagraph (A), the Secretary shall comply with the procedures developed and implemented by the Department pursuant to section 70923(b)(2) of the Build America, Buy America Act (enacted as subtitle A of title IX of division G of Public Law 117–58).

(ii) Prohibition on granting certain waivers

The Secretary may not grant a waiver under subparagraph (A) if, as a result of such waiver, products embodying the applicable subject invention, or produced through the use of the applicable subject invention, would be manufactured substantially in a country of concern.

(Pub. L. 107–296, title III, §308, Nov. 25, 2002, 116 Stat. 2170; Pub. L. 108–7, div. L, §101(1), Feb. 20, 2003, 117 Stat. 526; Pub. L. 117–263, div. G, title LXXI, §7114, Dec. 23, 2022, 136 Stat. 3633.)

EDITORIAL NOTES

REFERENCES IN TEXT

The date of enactment, referred to in subsec. (b)(2)(D), probably means the date of enactment of this section by Pub. L. 107–296, which was approved Nov. 25, 2002.

Section 70923(b)(2) of the Build America, Buy America Act, referred to in subsec. (d)(3)(B)(i), is section 70923(b)(2) of Pub. L. 117–58, div. G, title IX, Nov. 15, 2021, 135 Stat. 1306, which is not classified to the Code.

AMENDMENTS

2022—Subsec. (d). Pub. L. 117–263 added subsec. (d).

2003—Subsecs. (a) to (c)(1). Pub. L. 108–7 added subsecs. (a) to (c)(1) and struck out former subsecs. (a) to (c)(1) which related to the responsibilities of the Secretary, acting through the Under Secretary for Science and Technology, to carry out the responsibilities under section 182(4) of this title through both extramural and intramural programs, to operate extramural research, development, demonstration, testing, and evaluation programs, to establish a coordinated, university-based system to enhance the Nation's homeland security, and to draw upon the expertise of any laboratory of the Federal Government.

[1] *So in original. There is no par. (2).*

§189. Utilization of Department of Energy national laboratories and sites in support of homeland security activities

(a) Authority to utilize national laboratories and sites

(1) In general

In carrying out the missions of the Department, the Secretary may utilize the Department of Energy national laboratories and sites through any 1 or more of the following methods, as the Secretary considers appropriate:

(A) A joint sponsorship arrangement referred to in subsection (b).

(B) A direct contract between the Department and the applicable Department of Energy laboratory or site, subject to subsection (c).

(C) Any "work for others" basis made available by that laboratory or site.

(D) Any other method provided by law.

(2) Acceptance and performance by labs and sites

Notwithstanding any other law governing the administration, mission, use, or operations of any of the Department of Energy national laboratories and sites, such laboratories and sites are authorized to accept and perform work for the Secretary, consistent with resources provided, and perform such work on an equal basis to other missions at the laboratory and not on a noninterference basis with other missions of such laboratory or site.

(b) Joint sponsorship arrangements

(1) Laboratories

The Department may be a joint sponsor, under a multiple agency sponsorship arrangement with the Department of Energy, of 1 or more Department of Energy national laboratories in the performance of work.

(2) Sites

The Department may be a joint sponsor of a Department of Energy site in the performance of work as if such site were a federally funded research and development center and the work were performed under a multiple agency sponsorship arrangement with the Department.

(3) Primary sponsor

The Department of Energy shall be the primary sponsor under a multiple agency sponsorship arrangement referred to in paragraph (1) or (2).

(4) Lead agent

The Secretary of Energy shall act as the lead agent in coordinating the formation and performance of a joint sponsorship arrangement under this subsection between the Department and a Department of Energy national laboratory or site.

(5) Federal Acquisition Regulation

Any work performed by a Department of Energy national laboratory or site under a joint

sponsorship arrangement under this subsection shall comply with the policy on the use of federally funded research and development centers under the Federal Acquisition Regulations.

(6) Funding

The Department shall provide funds for work at the Department of Energy national laboratories or sites, as the case may be, under a joint sponsorship arrangement under this subsection under the same terms and conditions as apply to the primary sponsor of such national laboratory under section 3303(a)(1)(C) of title 41 or of such site to the extent such section applies to such site as a federally funded research and development center by reason of this subsection.

(c) Separate contracting

To the extent that programs or activities transferred by this chapter from the Department of Energy to the Department of Homeland Security are being carried out through direct contracts with the operator of a national laboratory or site of the Department of Energy, the Secretary of Homeland Security and the Secretary of Energy shall ensure that direct contracts for such programs and activities between the Department of Homeland Security and such operator are separate from the direct contracts of the Department of Energy with such operator.

(d) Authority with respect to cooperative research and development agreements and licensing agreements

In connection with any utilization of the Department of Energy national laboratories and sites under this section, the Secretary may permit the director of any such national laboratory or site to enter into cooperative research and development agreements or to negotiate licensing agreements with any person, any agency or instrumentality, of the United States, any unit of State or local government, and any other entity under the authority granted by section 3710a of title 15. Technology may be transferred to a non-Federal party to such an agreement consistent with the provisions of sections 3710 and 3710a of title 15.

(e) Reimbursement of costs

In the case of an activity carried out by the operator of a Department of Energy national laboratory or site in connection with any utilization of such laboratory or site under this section, the Department of Homeland Security shall reimburse the Department of Energy for costs of such activity through a method under which the Secretary of Energy waives any requirement for the Department of Homeland Security to pay administrative charges or personnel costs of the Department of Energy or its contractors in excess of the amount that the Secretary of Energy pays for an activity carried out by such contractor and paid for by the Department of Energy.

(f) Laboratory directed research and development by the Department of Energy

No funds authorized to be appropriated or otherwise made available to the Department in any fiscal year may be obligated or expended for laboratory directed research and development activities carried out by the Department of Energy unless such activities support the missions of the Department of Homeland Security.

(g) Office for National Laboratories

There is established within the Directorate of Science and Technology an Office for National Laboratories, which shall be responsible for the coordination and utilization of the Department of Energy national laboratories and sites under this section in a manner to create a networked laboratory system for the purpose of supporting the missions of the Department.

(h) Department of Energy coordination on homeland security related research

The Secretary of Energy shall ensure that any research, development, test, and evaluation activities conducted within the Department of Energy that are directly or indirectly related to homeland security are fully coordinated with the Secretary to minimize duplication of effort and maximize the effective application of Federal budget resources.

(Pub. L. 107–296, title III, §309, Nov. 25, 2002, 116 Stat. 2172.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (c), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

In subsec. (b)(6), "section 3303(a)(1)(C) of title 41" substituted for "section 303(b)(1)(C) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(b)(1)(C))" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SECURING ENERGY INFRASTRUCTURE

Pub. L. 116–92, div. E, title LVII, §5726, Dec. 20, 2019, 133 Stat. 2179, provided that:

"(a) DEFINITIONS.—In this section:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the congressional intelligence committees [Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives];

"(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Energy and Natural Resources of the Senate; and

"(C) the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives.

"(2) COVERED ENTITY.—The term 'covered entity' means an entity identified pursuant to section 9(a) of Executive Order No. 13636 of February 12, 2013 (78 Fed. Reg. 11742) [6 U.S.C. 121 note], relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

"(3) EXPLOIT.—The term 'exploit' means a software tool designed to take advantage of a security vulnerability.

"(4) INDUSTRIAL CONTROL SYSTEM.—The term 'industrial control system' means an operational technology used to measure, control, or manage industrial functions, and includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

"(5) NATIONAL LABORATORY.—The term 'National Laboratory' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

"(6) PROGRAM.—The term 'Program' means the pilot program established under subsection (b).

"(7) SECRETARY.—Except as otherwise specifically provided, the term 'Secretary' means the Secretary of Energy.

"(8) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

"(b) PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

"(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

"(2) evaluating technology and standards, in partnership with covered entities, to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

"(A) analog and nondigital control systems;

"(B) purpose-built control systems; and

"(C) physical controls.

"(c) WORKING GROUP TO EVALUATE PROGRAM STANDARDS AND DEVELOP STRATEGY.—

"(1) ESTABLISHMENT.—The Secretary shall establish a working group—

"(A) to evaluate the technology and standards used in the Program under subsection (b)(2); and

"(B) to develop a national cyber-informed engineering strategy to isolate and defend covered

entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

"(2) MEMBERSHIP.—The working group established under paragraph (1) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

"(A) The Department of Energy.

"(B) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

"(C)(i) The Department of Homeland Security; or

"(ii) the Industrial Control Systems Cyber Emergency Response Team.

"(D) The North American Electric Reliability Corporation.

"(E) The Nuclear Regulatory Commission.

"(F)(i) The Office of the Director of National Intelligence; or

"(ii) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

"(G)(i) The Department of Defense; or

"(ii) the Assistant Secretary of Defense for Homeland Security and America's Security Affairs.

"(H) A State or regional energy agency.

"(I) A national research body or academic institution.

"(J) The National Laboratories.

"(d) REPORTS ON THE PROGRAM.—

"(1) INTERIM REPORT.—Not later than 180 days after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees an interim report that—

"(A) describes the results of the Program;

"(B) includes an analysis of the feasibility of each method studied under the Program; and

"(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

"(2) FINAL REPORT.—Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees a final report that—

"(A) describes the results of the Program;

"(B) includes an analysis of the feasibility of each method studied under the Program; and

"(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

"(e) EXEMPTION FROM DISCLOSURE.—Information shared by or with the Federal Government or a State, Tribal, or local government under this section—

"(1) shall be deemed to be voluntarily shared information;

"(2) shall be exempt from disclosure under section 552 of title 5, United States Code, or any provision of any State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records; and

"(3) shall be withheld from the public, without discretion, under section 552(b)(3) of title 5, United States Code, and any provision of any State, Tribal, or local law requiring the disclosure of information or records.

"(f) PROTECTION FROM LIABILITY.—

"(1) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under subsection (b)—

"(A) shall not lie or be maintained in any court; and

"(B) shall be promptly dismissed by the applicable court.

"(2) VOLUNTARY ACTIVITIES.—Nothing in this section subjects any covered entity to liability for not engaging in the voluntary activities authorized under subsection (b).

"(g) NO NEW REGULATORY AUTHORITY FOR FEDERAL AGENCIES.—Nothing in this section authorizes the Secretary or the head of any other department or agency of the Federal Government to issue new regulations.

"(h) AUTHORIZATION OF APPROPRIATIONS.—

"(1) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out subsection (b).

"(2) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out subsections (c) and (d).

"(3) AVAILABILITY.—Amounts made available under paragraphs (1) and (2) shall remain available

until expended."

§190. Transfer of Plum Island Animal Disease Center, Department of Agriculture

(a) In general

In accordance with subchapter XII, the Secretary of Agriculture shall transfer to the Secretary of Homeland Security the Plum Island Animal Disease Center of the Department of Agriculture, including the assets and liabilities of the Center.

(b) Continued Department of Agriculture access

On completion of the transfer of the Plum Island Animal Disease Center under subsection (a), the Secretary of Homeland Security and the Secretary of Agriculture shall enter into an agreement to ensure that the Department of Agriculture is able to carry out research, diagnostic, and other activities of the Department of Agriculture at the Center.

(c) Direction of activities

The Secretary of Agriculture shall continue to direct the research, diagnostic, and other activities of the Department of Agriculture at the Center described in subsection (b).

(d) Notification

(1) In general

At least 180 days before any change in the biosafety level at the Plum Island Animal Disease Center, the President shall notify Congress of the change and describe the reasons for the change.

(2) Limitation

No change described in paragraph (1) may be made earlier than 180 days after the completion of the transition period (as defined in section 541 of this title).

(Pub. L. 107–296, title III, §310, Nov. 25, 2002, 116 Stat. 2174.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

TRANSFER OF NATIONAL BIO AND AGRO-DEFENSE FACILITY

Pub. L. 117–328, div. A, title VII, §775, Dec. 29, 2022, 136 Stat. 4509, provided that: "In this or any subsequent fiscal year, the Secretary of Homeland Security shall transfer to the Secretary of Agriculture the operation of and all property required to operate the National Bio- and Agro-Defense Facility in Manhattan, Kansas: *Provided*, That, such transfer of function shall include the transfer of up to 40 full time equivalent positions, to be completed within 120 days of the effective date of the transfer of function, as jointly determined by the Secretaries."

Similar provisions were contained in the following prior acts:

Pub. L. 117–103, div. A, title VII, §730, Mar. 15, 2022, 136 Stat. 92.

Pub. L. 116–94, div. B, title VII, §766, Dec. 20, 2019, 133 Stat. 2655.

DISPOSITION OF PLUM ISLAND PROPERTY AND TRANSPORTATION ASSETS

Pub. L. 116–260, div. FF, title V, §501(c), Dec. 27, 2020, 134 Stat. 3136, provided that: "The Administrator of General Services shall ensure that—

"(1) Federal property commonly known as Plum Island, New York, including the Orient point [probably should be "Point"] facility, all real and personal property and transportation assets that support Plum Island operations and access to Plum Island, be disposed of as a single consolidated asset; and

"(2) such disposal is subject to conditions as may be necessary to protect Government interests and meet program requirements."

Pub. L. 112–74, div. D, title V, §538, Dec. 23, 2011, 125 Stat. 976, which related to disposition of property and transporation assets if the National Bio and Agro-Defense Facility were relocated from Plum Island, New York, was repealed by Pub. L. 116–260, div. FF, title V, §501(b), Dec. 27, 2020, 134 Stat. 3136.

§191. Homeland Security Science and Technology Advisory Committee

(a) Establishment

There is established within the Department a Homeland Security Science and Technology Advisory Committee (in this section referred to as the "Advisory Committee"). The Advisory Committee shall make recommendations with respect to the activities of the Under Secretary for Science and Technology, including identifying research areas of potential importance to the security of the Nation.

(b) Membership

(1) Appointment

The Advisory Committee shall consist of 20 members appointed by the Under Secretary for Science and Technology, which shall include emergency first-responders or representatives of organizations or associations of emergency first-responders. The Advisory Committee shall also include representatives of citizen groups, including economically disadvantaged communities. The individuals appointed as members of the Advisory Committee—

(A) shall be eminent in fields such as emergency response, research, engineering, new product development, business, and management consulting;

(B) shall be selected solely on the basis of established records of distinguished service;

(C) shall not be employees of the Federal Government; and

(D) shall be so selected as to provide representation of a cross-section of the research, development, demonstration, and deployment activities supported by the Under Secretary for Science and Technology.

(2) National Research Council

The Under Secretary for Science and Technology may enter into an arrangement for the National Research Council to select members of the Advisory Committee, but only if the panel used by the National Research Council reflects the representation described in paragraph (1).

(c) Terms of office

(1) In general

Except as otherwise provided in this subsection, the term of office of each member of the Advisory Committee shall be 3 years.

(2) Original appointments

The original members of the Advisory Committee shall be appointed to three classes. One class of six shall have a term of 1 year, one class of seven a term of 2 years, and one class of seven a term of 3 years.

(3) Vacancies

A member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of such term.

(d) Eligibility

A person who has completed two consecutive full terms of service on the Advisory Committee shall thereafter be ineligible for appointment during the 1-year period following the expiration of the second such term.

(e) Meetings

The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members so request in writing. Each member shall be given appropriate notice of the call of each meeting, whenever possible not less than 15 days before the meeting.

(f) Quorum

A majority of the members of the Advisory Committee not having a conflict of interest in the

matter being considered by the Advisory Committee shall constitute a quorum.

(g) Conflict of interest rules

The Advisory Committee shall establish rules for determining when 1 of its members has a conflict of interest in a matter being considered by the Advisory Committee.

(h) Reports

(1) Annual report

The Advisory Committee shall render an annual report to the Under Secretary for Science and Technology for transmittal to Congress on or before January 31 of each year. Such report shall describe the activities and recommendations of the Advisory Committee during the previous year.

(2) Additional reports

The Advisory Committee may render to the Under Secretary for transmittal to Congress such additional reports on specific policy matters as it considers appropriate.

(i) Exemption from chapter 10 of title 5

Section 1013 of title 5 shall not apply to the Advisory Committee.

(j) Termination

The Department of Homeland Security Science and Technology Advisory Committee shall terminate on December 31, 2008.

(Pub. L. 107–296, title III, §311, Nov. 25, 2002, 116 Stat. 2174; Pub. L. 108–334, title V, §520, Oct. 18, 2004, 118 Stat. 1318; Pub. L. 109–347, title III, §302(a), Oct. 13, 2006, 120 Stat. 1920; Pub. L. 117–286, §4(a)(14), Dec. 27, 2022, 136 Stat. 4306.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (i). Pub. L. 117–286 substituted "Exemption from chapter 10 of title 5" for "Federal Advisory Committee Act exemption" in heading and "Section 1013 of title 5" for "Section 14 of the Federal Advisory Committee Act" in text.

2006—Subsec. (j). Pub. L. 109–347 substituted "on December 31, 2008" for "3 years after the effective date of this chapter".

2004—Subsec. (c)(2). Pub. L. 108–334 amended heading and text of par. (2) generally. Prior to amendment, text read as follows: "The original members of the Advisory Committee shall be appointed to three classes of three members each. One class shall have a term of 1 year, 1 a term of 2 years, and the other a term of 3 years."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2006 AMENDMENT

Pub. L. 109–347, title III, §302(b), Oct. 13, 2006, 120 Stat. 1921, provided that: "The amendment made by subsection (a) [amending this section] shall be effective as if enacted on the date of the enactment of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) [Nov. 25, 2002]."

§192. Homeland Security Institute

(a) Establishment

The Secretary shall establish a federally funded research and development center to be known as the "Homeland Security Institute" (in this section referred to as the "Institute").

(b) Administration

The Institute shall be administered as a separate entity by the Secretary.

(c) Duties

The duties of the Institute shall be determined by the Secretary, and may include the following:

(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities.

(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.

(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.

(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.

(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.

(7) Design of and support for the conduct of homeland security-related exercises and simulations.

(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation's critical infrastructure and key resources.

(d) Consultation on Institute activities

In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, nonprofit institutions, other Government agencies, and federally funded research and development centers.

(e) Use of centers

The Institute shall utilize the capabilities of the National Infrastructure Simulation and Analysis Center.

(f) Annual reports

The Institute shall transmit to the Secretary and Congress an annual report on the activities of the Institute under this section.

(g) Termination

The Homeland Security Institute shall terminate 5 years after its establishment.

(Pub. L. 107–296, title III, §312, Nov. 25, 2002, 116 Stat. 2176; Pub. L. 108–334, title V, §519, Oct. 18, 2004, 118 Stat. 1318.)

EDITORIAL NOTES

AMENDMENTS

2004—Subsec. (g). Pub. L. 108–334 amended heading and text of subsec. (g) generally. Prior to amendment, text read as follows: "The Homeland Security Institute shall terminate 3 years after the effective date of this chapter."

§193. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security

(a) Establishment of program

The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 111 of this title).

(b) Elements of program

The program described in subsection (a) shall include the following components:

(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private sector entities for additional review, purchase, or use.

(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.

(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private sector efforts to evaluate and implement the use of technologies described in paragraph (1) or (2).

(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.

(c) Miscellaneous provisions

(1) In general

Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology to be used by the Department, any other executive agency, any State or local government entity, or any private sector entity.

(2) Certain proposals

The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(3) Coordination

In carrying out this section, the Secretary shall coordinate with the Technical Support Working Group (organized under the April 1982 National Security Decision Directive Numbered 30).

(Pub. L. 107–296, title III, §313, Nov. 25, 2002, 116 Stat. 2176.)

§194. Enhancement of public safety communications interoperability

(a) Coordination of public safety interoperable communications programs

(1) Program

The Secretary of Homeland Security, in consultation with the Secretary of Commerce and the Chairman of the Federal Communications Commission, shall establish a program to enhance public safety interoperable communications at all levels of government. Such program shall—

(A) establish a comprehensive national approach to achieving public safety interoperable communications;

(B) coordinate with other Federal agencies in carrying out subparagraph (A);

(C) develop, in consultation with other appropriate Federal agencies and State and local authorities, appropriate minimum capabilities for communications interoperability for Federal, State, and local public safety agencies;

(D) accelerate, in consultation with other Federal agencies, including the National Institute of Standards and Technology, the private sector, and nationally recognized standards organizations as appropriate, the development of national voluntary consensus standards for public safety interoperable communications, recognizing—

(i) the value, life cycle, and technical capabilities of existing communications infrastructure;
(ii) the need for cross-border interoperability between States and nations;
(iii) the unique needs of small, rural communities; and
(iv) the interoperability needs for daily operations and catastrophic events;

(E) encourage the development and implementation of flexible and open architectures incorporating, where possible, technologies that currently are commercially available, with appropriate levels of security, for short-term and long-term solutions to public safety communications interoperability;
(F) assist other Federal agencies in identifying priorities for research, development, and testing and evaluation with regard to public safety interoperable communications;
(G) identify priorities within the Department of Homeland Security for research, development, and testing and evaluation with regard to public safety interoperable communications;
(H) establish coordinated guidance for Federal grant programs for public safety interoperable communications;
(I) provide technical assistance to State and local public safety agencies regarding planning, acquisition strategies, interoperability architectures, training, and other functions necessary to achieve public safety communications interoperability;
(J) develop and disseminate best practices to improve public safety communications interoperability; and
(K) develop appropriate performance measures and milestones to systematically measure the Nation's progress toward achieving public safety communications interoperability, including the development of national voluntary consensus standards.

(2) Office for Interoperability and Compatibility

(A) Establishment of Office

The Secretary may establish an Office for Interoperability and Compatibility within the Directorate of Science and Technology to carry out this subsection.

(B) Functions

If the Secretary establishes such office, the Secretary shall, through such office—
(i) carry out Department of Homeland Security responsibilities and authorities relating to the SAFECOM Program; and
(ii) carry out section 510 [1] of the Homeland Security Act of 2002, as added by subsection (d).

(3) Authorization of appropriations

There are authorized to be appropriated to the Secretary to carry out this subsection—
(A) $22,105,000 for fiscal year 2005;
(B) $22,768,000 for fiscal year 2006;
(C) $23,451,000 for fiscal year 2007;
(D) $24,155,000 for fiscal year 2008; and
(E) $24,879,000 for fiscal year 2009.

(b) Report

Not later than 120 days after December 17, 2004, the Secretary shall report to the Congress on Department of Homeland Security plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications, a schedule of milestones for such development, and achievements of such development.

(c) International interoperability

Not later than 18 months after December 17, 2004, the President shall establish a mechanism for coordinating cross-border interoperability issues between—

(1) the United States and Canada; and
(2) the United States and Mexico.

(d) Omitted

(e) Multiyear interoperability grants

(1) Multiyear commitments

In awarding grants to any State, region, local government, or Indian tribe for the purposes of enhancing interoperable communications capabilities for emergency response providers, the Secretary may commit to obligate Federal assistance beyond the current fiscal year, subject to the limitations and restrictions in this subsection.

(2) Restrictions

(A) Time limit

No multiyear interoperability commitment may exceed 3 years in duration.

(B) Amount of committed funds

The total amount of assistance the Secretary has committed to obligate for any future fiscal year under paragraph (1) may not exceed $150,000,000.

(3) Letters of intent

(A) Issuance

Pursuant to paragraph (1), the Secretary may issue a letter of intent to an applicant committing to obligate from future budget authority an amount, not more than the Federal Government's share of the project's cost, for an interoperability communications project (including interest costs and costs of formulating the project).

(B) Schedule

A letter of intent under this paragraph shall establish a schedule under which the Secretary will reimburse the applicant for the Federal Government's share of the project's costs, as amounts become available, if the applicant, after the Secretary issues the letter, carries out the project before receiving amounts under a grant issued by the Secretary.

(C) Notice to Secretary

An applicant that is issued a letter of intent under this subsection shall notify the Secretary of the applicant's intent to carry out a project pursuant to the letter before the project begins.

(D) Notice to Congress

The Secretary shall transmit a written notification to the Congress no later than 3 days before the issuance of a letter of intent under this section.

(E) Limitations

A letter of intent issued under this section is not an obligation of the Government under section 1501 of title 31 and is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(F) Statutory construction

Nothing in this subsection shall be construed—

(i) to prohibit the obligation of amounts pursuant to a letter of intent under this subsection in the same fiscal year as the letter of intent is issued; or

(ii) to apply to, or replace, Federal assistance intended for interoperable communications that is not provided pursuant to a commitment under this subsection.

(f) Interoperable communications plans

Any applicant requesting funding assistance from the Secretary for interoperable communications for emergency response providers shall submit an Interoperable Communications Plan to the

Secretary for approval. Such a plan shall—

(1) describe the current state of communications interoperability in the applicable jurisdictions among Federal, State, and local emergency response providers and other relevant private resources;

(2) describe the available and planned use of public safety frequency spectrum and resources for interoperable communications within such jurisdictions;

(3) describe how the planned use of spectrum and resources for interoperable communications is compatible with surrounding capabilities and interoperable communications plans of Federal, State, and local governmental entities, military installations, foreign governments, critical infrastructure, and other relevant entities;

(4) include a 5-year plan for the dedication of Federal, State, and local government and private resources to achieve a consistent, secure, and effective interoperable communications system, including planning, system design and engineering, testing and technology development, procurement and installation, training, and operations and maintenance;

(5) describe how such 5-year plan meets or exceeds any applicable standards and grant requirements established by the Secretary;

(6) include information on the governance structure used to develop the plan, including such information about all agencies and organizations that participated in developing the plan and the scope and timeframe of the plan; and

(7) describe the method by which multi-jurisdictional, multidisciplinary input is provided from all regions of the jurisdiction, including any high-threat urban areas located in the jurisdiction, and the process for continuing to incorporate such input.

(g) Definitions

In this section:

(1) Interoperable communications

The term "interoperable communications" means the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, and video with one another on demand, in real time, as necessary.

(2) Emergency response providers

The term "emergency response providers" has the meaning that term has under section 101 of this title.

(h) Omitted

(i) Sense of Congress regarding interoperable communications

(1) Finding

The Congress finds that—

(A) many first responders working in the same jurisdiction or in different jurisdictions cannot effectively and efficiently communicate with one another; and

(B) their inability to do so threatens the public's safety and may result in unnecessary loss of lives and property.

(2) Sense of Congress

It is the sense of Congress that interoperable emergency communications systems and radios should continue to be deployed as soon as practicable for use by the first responder community, and that upgraded and new digital communications systems and new digital radios must meet prevailing national, voluntary consensus standards for interoperability.

(Pub. L. 108–458, title VII, §7303, Dec. 17, 2004, 118 Stat. 3843; Pub. L. 110–53, title III, §301(c), Aug. 3, 2007, 121 Stat. 299.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 510 of the Homeland Security Act of 2002, as added by subsection (d), referred to in subsec. (a)(2)(B)(ii), means section 510 of Pub. L. 107–296, which was added by Pub. L. 108–458, title VII, §7303(d), Dec. 17, 2004, 118 Stat. 3844, and was classified to section 321 of this title, prior to repeal by Pub. L. 109–295, title VI, §611(5), Oct. 4, 2006, 120 Stat. 1395. See Prior Provisions note set out under section 321 of this title.

CODIFICATION

Section is comprised of section 7303 of Pub. L. 108–458. Subsec. (d) of section 7303 of Pub. L. 108–458 enacted section 321 of this title. Subsec. (h) of section 7303 of Pub. L. 108–458 amended sections 238 and 314 of this title.

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the 9/11 Commission Implementation Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Section 301(c) of Pub. L. 110–53, which directed the amendment of section 7303 of the "Intelligence Reform and Terrorist Prevention Act of 2004", was executed to this section, which is section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004, to reflect the probable intent of Congress. See 2007 Amendment notes below.

AMENDMENTS

2007—Subsec. (f)(6), (7). Pub. L. 110–53, §301(c)(1), added pars. (6) and (7). See Codification note above.

Subsec. (g)(1). Pub. L. 110–53, §301(c)(2), substituted "and video" for "or video". See Codification note above.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Pub. L. 108–458, title VII, §7308, Dec. 17, 2004, 118 Stat. 3849, provided that: "Notwithstanding any other provision of this Act [see Tables for classification], this subtitle [subtitle C (§§7301–7308) of title VII of Pub. L. 108–458, enacting this section and section 321 of this title, amending sections 238 and 312 of this title, and enacting provisions set out as notes under this section and section 5196 of Title 42, The Public Health and Welfare] shall take effect on the date of enactment of this Act [Dec. 17, 2004]."

TRANSFER OF FUNCTIONS

For transfer of the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards, to the Assistant Director for Emergency Communications, see section 571(d)(1) of this title.

DEPARTMENT OF HOMELAND SECURITY INTEROPERABLE COMMUNICATIONS

Pub. L. 114–120, title II, §212, Feb. 8, 2016, 130 Stat. 42, provided that:

"(a) IN GENERAL.—If the Secretary of Homeland Security determines that there are at least two communications systems described under paragraph (1)(B) and certified under paragraph (2), the Secretary shall establish and carry out a pilot program across not less than three components of the Department of Homeland Security to assess the effectiveness of a communications system that—

"(1) provides for—

"(A) multiagency collaboration and interoperability; and

"(B) wide-area, secure, and peer-invitation- and-acceptance-based multimedia communications;

"(2) is certified by the Department of Defense Joint Interoperability Test Center; and

"(3) is composed of commercially available, off-the-shelf technology.

"(b) ASSESSMENT.—Not later than 6 months after the date on which the pilot program is completed, the Secretary shall submit to the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation and the Committee [on] Homeland Security and Governmental Affairs of the Senate an assessment of the pilot program, including the impacts of the program with respect to interagency and Coast Guard response capabilities.

"(c) STRATEGY.—The pilot program shall be consistent with the strategy required by the Department of

Homeland Security Interoperable Communications Act (Public Law 114–29) [set out below].

"(d) TIMING.—The pilot program shall commence within 90 days after the date of the enactment of this Act [Feb. 8, 2016] or within 60 days after the completion of the strategy required by the Department of Homeland Security Interoperable Communications Act (Public Law 114–29), whichever is later."

Pub. L. 114–29, July 6, 2015, 129 Stat. 421, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Department of Homeland Security Interoperable Communications Act' or the 'DHS Interoperable Communications Act'.

"SEC. 2. DEFINITIONS.

"In this Act—

"(1) the term 'Department' means the Department of Homeland Security;

"(2) the term 'interoperable communications' has the meaning given that term in section 701(d) [now 701(e)] of the Homeland Security Act of 2002 [6 U.S.C. 341(e)], as added by section 3; and

"(3) the term 'Under Secretary for Management' means the Under Secretary for Management of the Department of Homeland Security.

"SEC. 3. INCLUSION OF INTEROPERABLE COMMUNICATIONS CAPABILITIES IN RESPONSIBILITIES OF UNDER SECRETARY FOR MANAGEMENT.

[Amended section 341 of this title.]

"SEC. 4. STRATEGY.

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act [July 6, 2015], the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a strategy, which shall be updated as necessary, for achieving and maintaining interoperable communications among the components of the Department, including for daily operations, planned events, and emergencies, with corresponding milestones, that includes the following:

"(1) An assessment of interoperability gaps in radio communications among the components of the Department, as of the date of enactment of this Act.

"(2) Information on efforts and activities, including current and planned policies, directives, and training, of the Department since November 1, 2012, to achieve and maintain interoperable communications among the components of the Department, and planned efforts and activities of the Department to achieve and maintain such interoperable communications.

"(3) An assessment of obstacles and challenges to achieving and maintaining interoperable communications among the components of the Department.

"(4) Information on, and an assessment of, the adequacy of mechanisms available to the Under Secretary for Management to enforce and compel compliance with interoperable communications policies and directives of the Department.

"(5) Guidance provided to the components of the Department to implement interoperable communications policies and directives of the Department.

"(6) The total amount of funds expended by the Department since November 1, 2012, and projected future expenditures, to achieve interoperable communications, including on equipment, infrastructure, and maintenance.

"(7) Dates upon which Department-wide interoperability is projected to be achieved for voice, data, and video communications, respectively, and interim milestones that correspond to the achievement of each such mode of communication.

"(b) SUPPLEMENTARY MATERIAL.—Together with the strategy required under subsection (a), the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on—

"(1) any intra-agency effort or task force that has been delegated certain responsibilities by the Under Secretary for Management relating to achieving and maintaining interoperable communications among the components of the Department by the dates referred to in subsection (a)(7); and

"(2) who, within each such component, is responsible for implementing policies and directives issued by the Under Secretary for Management to so achieve and maintain such interoperable communications.

"SEC. 5. REPORT.

"Not later than 100 days after the date on which the strategy required under section 4(a) is submitted, and

every 2 years thereafter for 6 years, the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the status of efforts to implement the strategy required under section 4(a), including the following:

"(1) Progress on each interim milestone referred to in section 4(a)(7) toward achieving and maintaining interoperable communications among the components of the Department.

"(2) Information on any policies, directives, guidance, and training established by the Under Secretary for Management.

"(3) An assessment of the level of compliance, adoption, and participation among the components of the Department with the policies, directives, guidance, and training established by the Under Secretary for Management to achieve and maintain interoperable communications among the components.

"(4) Information on any additional resources or authorities needed by the Under Secretary for Management.

"SEC. 6. APPLICABILITY.

"Sections 4 and 5 shall only apply with respect to the interoperable communications capabilities within the Department and components of the Department to communicate within the Department."

CROSS BORDER INTEROPERABILITY REPORTS

Pub. L. 110–53, title XXII, §2203, Aug. 3, 2007, 121 Stat. 541, provided that:

"(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Aug. 3, 2007], the Federal Communications Commission, in consultation with the Department of Homeland Security's Office of Emergency Communications [now Emergency Communications Division], the Office of Management of [sic] Budget, and the Department of State shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce on—

"(1) the status of the mechanism established by the President under section 7303(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(c)) for coordinating cross border interoperability issues between—

"(A) the United States and Canada; and

"(B) the United States and Mexico;

"(2) the status of treaty negotiations with Canada and Mexico regarding the coordination of the re-banding of 800 megahertz radios, as required under the final rule of the Federal Communication Commission in the 'Private Land Mobile Services; 800 MHz Public Safety Interface Proceeding' (WT Docket No. 02–55; ET Docket No. 00–258; ET Docket No. 95–18, RM–9498; RM–10024; FCC 04–168) including the status of any outstanding issues in the negotiations between—

"(A) the United States and Canada; and

"(B) the United States and Mexico;

"(3) communications between the Commission and the Department of State over possible amendments to the bilateral legal agreements and protocols that govern the coordination process for license applications seeking to use channels and frequencies above Line A;

"(4) the annual rejection rate for the last 5 years by the United States of applications for new channels and frequencies by Canadian private and public entities; and

"(5) any additional procedures and mechanisms that can be taken by the Commission to decrease the rejection rate for applications by United States private and public entities seeking licenses to use channels and frequencies above Line A.

"(b) UPDATED REPORTS TO BE FILED ON THE STATUS OF TREATY OF [SIC] NEGOTIATIONS .—The Federal Communications Commission, in conjunction with the Department of Homeland Security, the Office of Management of Budget, and the Department of State shall continually provide updated reports to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives on the status of treaty negotiations under subsection (a)(2) until the appropriate United States treaty has been revised with each of—

"(1) Canada; and

"(2) Mexico.

"(c) INTERNATIONAL NEGOTIATIONS TO REMEDY SITUATION.—Not later than 90 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of the Department of State shall report to Congress on—

"(1) the current process for considering applications by Canada for frequencies and channels by United States communities above Line A;

"(2) the status of current negotiations to reform and revise such process;

"(3) the estimated date of conclusion for such negotiations;

"(4) whether the current process allows for automatic denials or dismissals of initial applications by the Government of Canada, and whether such denials or dismissals are currently occurring; and

"(5) communications between the Department of State and the Federal Communications Commission pursuant to subsection (a)(3)."

SUBMISSION OF REPORTS TO APPROPRIATE CONGRESSIONAL COMMITTEES

Pub. L. 110–53, title XXII, §2205, Aug. 3, 2007, 121 Stat. 543, provided that: "In addition to the committees specifically enumerated to receive reports under this title [enacting provisions set out as note under this section, section 701 of this title, and section 247d–3a of Title 42, The Public Health and Welfare, and amending provisions set out as a note under section 309 of Title 47, Telecommunications], any report transmitted under the provisions of this title shall also be transmitted to the appropriate congressional committees (as defined in section 2(2) of the Homeland Security Act of 2002 (6 U.S.C. 101(2)))."

REGIONAL MODEL STRATEGIC PLAN PILOT PROJECTS

Pub. L. 108–458, title VII, §7304, Dec. 17, 2004, 118 Stat. 3847, directed the Secretary of Homeland Security, not later than 90 days after Dec. 17, 2004, to establish not fewer than 2 pilot projects in high threat urban areas or regions likely to implement a national model strategic plan in order to develop a regional strategic plan to foster interagency communication and coordinate the gathering of all Federal, State, and local first responders in that area, consistent with the national strategic plan developed by the Department of Homeland Security, and to submit to Congress an interim report regarding the progress of the interagency communications pilot projects 6 months after Dec. 17, 2004, and a final report 18 months after Dec. 17, 2004.

[1] *See References in Text note below.*

§195. Office for Interoperability and Compatibility

(a) Clarification of responsibilities

The Director of the Office for Interoperability and Compatibility shall—

(1) assist the Secretary in developing and implementing the science and technology aspects of the program described in subparagraphs (D), (E), (F), and (G) of section 194(a)(1) of this title;

(2) in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies with responsibility for standards, support the creation of national voluntary consensus standards for interoperable emergency communications;

(3) establish a comprehensive research, development, testing, and evaluation program for improving interoperable emergency communications;

(4) establish, in coordination with the Director for Emergency Communications,[1] requirements for interoperable emergency communications capabilities, which shall be nonproprietary where standards for such capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance administered by the Department, excluding any alert and warning device, technology, or system;

(5) carry out the Department's responsibilities and authorities relating to research, development, testing, evaluation, or standards-related elements of the SAFECOM Program;

(6) evaluate and assess new technology in real-world environments to achieve interoperable emergency communications capabilities;

(7) encourage more efficient use of existing resources, including equipment, to achieve interoperable emergency communications capabilities;

(8) test public safety communications systems that are less prone to failure, support new nonvoice services, use spectrum more efficiently, and cost less than existing systems;

(9) coordinate with the private sector to develop solutions to improve emergency communications capabilities and achieve interoperable emergency communications capabilities; and

(10) conduct pilot projects, in coordination with the Director for Emergency Communications,[1]

to test and demonstrate technologies, including data and video, that enhance—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications capabilities.

(b) Coordination

The Director of the Office for Interoperability and Compatibility shall coordinate with the Director for Emergency Communications [1] with respect to the SAFECOM program.

(c) Sufficiency of resources

The Secretary shall provide the Office for Interoperability and Compatibility the resources and staff necessary to carry out the responsibilities under this section.

(Pub. L. 107–296, title III, §314, as added Pub. L. 109–295, title VI, §672(a), Oct. 4, 2006, 120 Stat. 1441.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to Director for Emergency Communications deemed to be a reference to Assistant Director for Emergency Communications, see section 2(c)(2) of Pub. L. 115–278, set out as a note under section 571 of this title.

[1] *See Change of Name note below.*

§195a. Emergency communications interoperability research and development

(a) In general

The Under Secretary for Science and Technology, acting through the Director of the Office for Interoperability and Compatibility, shall establish a comprehensive research and development program to support and promote—

(1) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) interoperable emergency communications capabilities among emergency response providers and relevant government officials, including by—

(A) supporting research on a competitive basis, including through the Directorate of Science and Technology and Homeland Security Advanced Research Projects Agency; and

(B) considering the establishment of a Center of Excellence under the Department of Homeland Security Centers of Excellence Program focused on improving emergency response providers' communication capabilities.

(b) Purposes

The purposes of the program established under subsection (a) include—

(1) supporting research, development, testing, and evaluation on emergency communication capabilities;

(2) understanding the strengths and weaknesses of the public safety communications systems in use;

(3) examining how current and emerging technology can make emergency response providers more effective, and how Federal, State, local, and tribal government agencies can use this technology in a coherent and cost-effective manner;

(4) investigating technologies that could lead to long-term advancements in emergency communications capabilities and supporting research on advanced technologies and potential systemic changes to dramatically improve emergency communications; and

(5) evaluating and validating advanced technology concepts, and facilitating the development and deployment of interoperable emergency communication capabilities.

(c) Definitions

For purposes of this section, the term "interoperable", with respect to emergency communications, has the meaning given the term in section 578 of this title.

(Pub. L. 107–296, title III, §315, as added Pub. L. 109–295, title VI, §673(a), Oct. 4, 2006, 120 Stat. 1443.)

§195b. National Biosurveillance Integration Center

(a) Establishment

The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall establish, operate, and maintain a National Biosurveillance Integration Center (referred to in this section as the "NBIC"), which shall be headed by a Directing Officer, under an office or directorate of the Department that is in existence as of August 3, 2007.

(b) Primary mission

The primary mission of the NBIC is to—

(1) enhance the capability of the Federal Government to—

(A) rapidly identify, characterize, localize, and track a biological event of national concern by integrating and analyzing data relating to human health, animal, plant, food, and environmental monitoring systems (both national and international); and

(B) disseminate alerts and other information to Member Agencies and, in coordination with (and where possible through) Member Agencies, to agencies of State, local, and tribal governments, as appropriate, to enhance the ability of such agencies to respond to a biological event of national concern; and

(2) oversee development and operation of the National Biosurveillance Integration System.

(c) Requirements

The NBIC shall detect, as early as possible, a biological event of national concern that presents a risk to the United States or the infrastructure or key assets of the United States, including by—

(1) consolidating data from all relevant surveillance systems maintained by Member Agencies to detect biological events of national concern across human, animal, and plant species;

(2) seeking private sources of surveillance, both foreign and domestic, when such sources would enhance coverage of critical surveillance gaps;

(3) using an information technology system that uses the best available statistical and other analytical tools to identify and characterize biological events of national concern in as close to real-time as is practicable;

(4) providing the infrastructure for such integration, including information technology systems and space, and support for personnel from Member Agencies with sufficient expertise to enable analysis and interpretation of data;

(5) working with Member Agencies to create information technology systems that use the minimum amount of patient data necessary and consider patient confidentiality and privacy issues at all stages of development and apprise the Privacy Officer of such efforts; and

(6) alerting Member Agencies and, in coordination with (and where possible through) Member Agencies, public health agencies of State, local, and tribal governments regarding any incident that could develop into a biological event of national concern.

(d) Responsibilities of the Directing Officer of the NBIC

(1) In general

The Directing Officer of the NBIC shall—

(A) on an ongoing basis, monitor the availability and appropriateness of surveillance systems used by the NBIC and those systems that could enhance biological situational awareness or the overall performance of the NBIC;

(B) on an ongoing basis, review and seek to improve the statistical and other analytical methods used by the NBIC;

(C) receive and consider other relevant homeland security information, as appropriate; and

(D) provide technical assistance, as appropriate, to all Federal, regional, State, local, and tribal government entities and private sector entities that contribute data relevant to the operation of the NBIC.

(2) Assessments

The Directing Officer of the NBIC shall—

(A) on an ongoing basis, evaluate available data for evidence of a biological event of national concern; and

(B) integrate homeland security information with NBIC data to provide overall situational awareness and determine whether a biological event of national concern has occurred.

(3) Information sharing

(A) In general

The Directing Officer of the NBIC shall—

(i) establish a method of real-time communication with the National Operations Center;

(ii) in the event that a biological event of national concern is detected, notify the Secretary and disseminate results of NBIC assessments relating to that biological event of national concern to appropriate Federal response entities and, in coordination with relevant Member Agencies, regional, State, local, and tribal governmental response entities in a timely manner;

(iii) provide any report on NBIC assessments to Member Agencies and, in coordination with relevant Member Agencies, any affected regional, State, local, or tribal government, and any private sector entity considered appropriate that may enhance the mission of such Member Agencies, governments, or entities or the ability of the Nation to respond to biological events of national concern; and

(iv) share NBIC incident or situational awareness reports, and other relevant information, consistent with the information sharing environment established under section 485 of this title and any policies, guidelines, procedures, instructions, or standards established under that section.

(B) Consultation

The Directing Officer of the NBIC shall implement the activities described in subparagraph (A) consistent with the policies, guidelines, procedures, instructions, or standards established under section 485 of this title and in consultation with the Director of National Intelligence, the Under Secretary for Intelligence and Analysis, and other offices or agencies of the Federal Government, as appropriate.

(e) Responsibilities of the NBIC member agencies

(1) [1] In general

Each Member Agency shall—

(A) use its best efforts to integrate biosurveillance information into the NBIC, with the goal of promoting information sharing between Federal, State, local, and tribal governments to detect biological events of national concern;

(B) provide timely information to assist the NBIC in maintaining biological situational awareness for accurate detection and response purposes;

(C) enable the NBIC to receive and use biosurveillance information from member agencies to carry out its requirements under subsection (c);

(D) connect the biosurveillance data systems of that Member Agency to the NBIC data system under mutually agreed protocols that are consistent with subsection (c)(5);

(E) participate in the formation of strategy and policy for the operation of the NBIC and its information sharing;

(F) provide personnel to the NBIC under an interagency personnel agreement and consider the qualifications of such personnel necessary to provide human, animal, and environmental data analysis and interpretation support to the NBIC; and

(G) retain responsibility for the surveillance and intelligence systems of that department or agency, if applicable.

(f) Administrative authorities

(1) Hiring of experts

The Directing Officer of the NBIC shall hire individuals with the necessary expertise to develop and operate the NBIC.

(2) Detail of personnel

Upon the request of the Directing Officer of the NBIC, the head of any Federal department or agency may detail, on a reimbursable basis, any of the personnel of that department or agency to the Department to assist the NBIC in carrying out this section.

(g) NBIC interagency working group

The Directing Officer of the NBIC shall—

(1) establish an interagency working group to facilitate interagency cooperation and to advise the Directing Officer of the NBIC regarding recommendations to enhance the biosurveillance capabilities of the Department; and

(2) invite Member Agencies to serve on that working group.

(h) Relationship to other departments and agencies

The authority of the Directing Officer of the NBIC under this section shall not affect any authority or responsibility of any other department or agency of the Federal Government with respect to biosurveillance activities under any program administered by that department or agency.

(i) Authorization of appropriations

There are authorized to be appropriated such sums as are necessary to carry out this section.

(j) Definitions

In this section:

(1) The terms "biological agent" and "toxin" have the meanings given those terms in section 178 of title 18.

(2) The term "biological event of national concern" means—

(A) an act of terrorism involving a biological agent or toxin; or

(B) a naturally occurring outbreak of an infectious disease that may result in a national epidemic.

(3) The term "homeland security information" has the meaning given that term in section 482 of this title.

(4) The term "Member Agency" means any Federal department or agency that, at the discretion of the head of that department or agency, has entered a memorandum of understanding regarding participation in the NBIC.

(5) The term "Privacy Officer" means the Privacy Officer appointed under section 142 of this title.

(Pub. L. 107–296, title III, §316, as added Pub. L. 110–53, title XI, §1101(a), Aug. 3, 2007, 121 Stat. 375; amended Pub. L. 115–387, §2(f)(2), Dec. 21, 2018, 132 Stat. 5168.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–387 substituted "Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall" for "Secretary shall".

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEADLINE FOR IMPLEMENTATION

Pub. L. 110–53, title XI, §1101(c), Aug. 3, 2007, 121 Stat. 378, provided that: "The National Biosurveillance Integration Center under section 316 of the Homeland Security Act [of 2002, 6 U.S.C. 195b], as added by subsection (a), shall be fully operational by not later than September 30, 2008."

[1] *So in original. No par. (2) has been enacted.*

§195c. Promoting antiterrorism through international cooperation program

(a) Definitions

In this section:

(1) Director

The term "Director" means the Director selected under subsection (b)(2).

(2) International cooperative activity

The term "international cooperative activity" includes—

(A) coordinated research projects, joint research projects, or joint ventures;
(B) joint studies or technical demonstrations;
(C) coordinated field exercises, scientific seminars, conferences, symposia, and workshops;
(D) training of scientists and engineers;
(E) visits and exchanges of scientists, engineers, or other appropriate personnel;
(F) exchanges or sharing of scientific and technological information; and
(G) joint use of laboratory facilities and equipment.

(b) Science and Technology Homeland Security International Cooperative Programs Office

(1) Establishment

The Under Secretary shall establish the Science and Technology Homeland Security International Cooperative Programs Office.

(2) Director

The Office shall be headed by a Director, who—

(A) shall be selected, in consultation with the Assistant Secretary for International Affairs, by and shall report to the Under Secretary; and
(B) may be an officer of the Department serving in another position.

(3) Responsibilities

(A) Development of mechanisms

The Director shall be responsible for developing, in coordination with the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other Federal agencies, understandings and agreements to allow and to support international cooperative activity in support of homeland security.

(B) Priorities

The Director shall be responsible for developing, in coordination with the Office of International Affairs and other Federal agencies, strategic priorities for international cooperative activity for the Department in support of homeland security.

(C) Activities

The Director shall facilitate the planning, development, and implementation of international cooperative activity to address the strategic priorities developed under subparagraph (B) through mechanisms the Under Secretary considers appropriate, including grants, cooperative agreements, or contracts to or with foreign public or private entities, governmental organizations, businesses (including small businesses and socially and economically disadvantaged small businesses (as those terms are defined in sections 632 and 637 of title 15, respectively)), federally funded research and development centers, and universities.

(D) Identification of partners

The Director shall facilitate the matching of United States entities engaged in homeland security research with non-United States entities engaged in homeland security research so that they may partner in homeland security research activities.

(4) Coordination

The Director shall ensure that the activities under this subsection are coordinated with the Office of International Affairs and the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other relevant Federal agencies or interagency bodies. The Director may enter into joint activities with other Federal agencies.

(c) Matching funding

(1) In general

(A) Equitability

The Director shall ensure that funding and resources expended in international cooperative activity will be equitably matched by the foreign partner government or other entity through direct funding, funding of complementary activities, or the provision of staff, facilities, material, or equipment.

(B) Grant matching and repayment

(i) In general

The Secretary may require a recipient of a grant under this section—

(I) to make a matching contribution of not more than 50 percent of the total cost of the proposed project for which the grant is awarded; and

(II) to repay to the Secretary the amount of the grant (or a portion thereof), interest on such amount at an appropriate rate, and such charges for administration of the grant as the Secretary determines appropriate.

(ii) Maximum amount

The Secretary may not require that repayment under clause (i)(II) be more than 150 percent of the amount of the grant, adjusted for inflation on the basis of the Consumer Price Index.

(2) Foreign partners

Partners may include Israel, the United Kingdom, Canada, Australia, Singapore, and other allies in the global war on terrorism as determined to be appropriate by the Secretary of Homeland Security and the Secretary of State.

(3) Loans of equipment

The Director may make or accept loans of equipment for research and development and comparative testing purposes.

(d) Foreign reimbursements

If the Science and Technology Homeland Security International Cooperative Programs Office participates in an international cooperative activity with a foreign partner on a cost-sharing basis, any reimbursements or contributions received from that foreign partner to meet its share of the project may be credited to appropriate current appropriations accounts of the Directorate of Science and Technology.

(e) Report to Congress on international cooperative activities

Not later than one year after August 3, 2007, and every 5 years thereafter, the Under Secretary, acting through the Director, shall submit to Congress a report containing—

(1) a brief description of each grant, cooperative agreement, or contract made or entered into under subsection (b)(3)(C), including the participants, goals, and amount and sources of funding;

(2) a list of international cooperative activities underway, including the participants, goals, expected duration, and amount and sources of funding, including resources provided to support the activities in lieu of direct funding; and [1]

(3) for international cooperative activities identified in the previous reporting period, a status update on the progress of such activities, including whether goals were realized, explaining any lessons learned, and evaluating overall success; and

(4) a discussion of obstacles encountered in the course of forming, executing, or implementing agreements for international cooperative activities, including administrative, legal, or diplomatic challenges or resource constraints.

(f) Animal and zoonotic diseases

As part of the international cooperative activities authorized in this section, the Under Secretary, in coordination with the Assistant Secretary for the Countering Weapons of Mass Destruction Office, the Department of State, and appropriate officials of the Department of Agriculture, the Department of Defense, and the Department of Health and Human Services, may enter into cooperative activities with foreign countries, including African nations, to strengthen American preparedness against foreign animal and zoonotic diseases overseas that could harm the Nation's agricultural and public health sectors if they were to reach the United States.

(g) Cybersecurity

As part of the international cooperative activities authorized in this section, the Under Secretary, in coordination with the Department of State and appropriate Federal officials, may enter into cooperative research activities with Israel to strengthen preparedness against cyber threats and enhance capabilities in cybersecurity.

(h) Construction; authorities of the Secretary of State

Nothing in this section shall be construed to alter or affect the following provisions of law:

(1) Title V of the Foreign Relations Authorization Act, Fiscal Year 1979 (22 U.S.C. 2656a et seq.).

(2) Section 112b(g) of title 1.

(3) Section 2651a(e)(2) of title 22.

(4) Sections 2752 and 2767 of title 22.

(5) Section 2382(c) of title 22.

(i) Authorization of appropriations

There are authorized to be appropriated to carry out this section such sums as are necessary.

(Pub. L. 107–296, title III, §317, as added Pub. L. 110–53, title XIX, §1901(b)(1), Aug. 3, 2007, 121 Stat. 505; amended Pub. L. 114–304, §2(a), Dec. 16, 2016, 130 Stat. 1519; Pub. L. 115–387, §2(f)(3), Dec. 21, 2018, 132 Stat. 5168; Pub. L. 117–263, div. E, title LIX, §5947(a)(3), Dec. 23, 2022, 136 Stat. 3481.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Foreign Relations Authorization Act, Fiscal Year 1979, referred to in subsec. (h)(1), is Pub. L. 95–426, Oct. 7, 1978, 92 Stat. 963. Title V of the Act is classified generally to sections 2656a to 2656d of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2022—Subsec. (h)(2). Pub. L. 117–263 substituted "Section 112b(g)" for "Section 112b(c)".

2018—Subsec. (f). Pub. L. 115–387 substituted "the Assistant Secretary for the Countering Weapons of Mass Destruction Office," for "the Chief Medical Officer,".

2016—Subsec. (e)(3), (4). Pub. L. 114–304, §2(a)(1), added pars. (3) and (4).

Subsecs. (g) to (i). Pub. L. 114–304, §2(a)(2), (3), added subsec. (g) and redesignated former subsecs. (g) and (h) as (h) and (i), respectively.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2022 AMENDMENT

Amendment by Pub. L. 117–263 effective 270 days after Dec. 23, 2022, see section 5947(c) of Pub. L. 117–263, set out as a note under section 112a of Title 1, General Provisions.

FINDINGS

Pub. L. 110–53, title XIX, §1901(a), Aug. 3, 2007, 121 Stat. 505, provided that: "Congress finds the following:

"(1) The development and implementation of technology is critical to combating terrorism and other high consequence events and implementing a comprehensive homeland security strategy.

"(2) The United States and its allies in the global war on terrorism share a common interest in facilitating research, development, testing, and evaluation of equipment, capabilities, technologies, and services that will aid in detecting, preventing, responding to, recovering from, and mitigating against acts of terrorism.

"(3) Certain United States allies in the global war on terrorism, including Israel, the United Kingdom, Canada, Australia, and Singapore have extensive experience with, and technological expertise in, homeland security.

"(4) The United States and certain of its allies in the global war on terrorism have a history of successful collaboration in developing mutually beneficial equipment, capabilities, technologies, and services in the areas of defense, agriculture, and telecommunications.

"(5) The United States and its allies in the global war on terrorism will mutually benefit from the sharing of technological expertise to combat domestic and international terrorism.

"(6) The establishment of an office to facilitate and support cooperative endeavors between and among government agencies, for-profit business entities, academic institutions, and nonprofit entities of the United States and its allies will safeguard lives and property worldwide against acts of terrorism and other high consequence events."

TRANSPARENCY OF FUNDS

Pub. L. 110–53, title XIX, §1902, Aug. 3, 2007, 121 Stat. 508, provided that: "For each Federal award (as that term is defined in section 2 of the Federal Funding Accountability and Transparency Act of 2006 [Pub. L. 109–282] (31 U.S.C. 6101 note)) under this title [enacting this section and provisions set out as notes under this section] or an amendment made by this title, the Director of the Office of Management and Budget shall ensure full and timely compliance with the requirements of the Federal Funding Accountability and Transparency Act of 2006 (31 U.S.C. 6101 note)."

[1] So in original. The word "and" probably should not appear.

§195d. Social media working group

(a) Establishment

The Secretary shall establish within the Department a social media working group (in this section referred to as the "Group").

(b) Purpose

In order to enhance the dissemination of information through social media technologies between the Department and appropriate stakeholders and to improve use of social media technologies in support of preparedness, response, and recovery, the Group shall identify, and provide guidance and

best practices to the emergency preparedness and response community on, the use of social media technologies before, during, and after a natural disaster or an act of terrorism or other man-made disaster.

(c) Membership

(1) In general

Membership of the Group shall be composed of a cross section of subject matter experts from Federal, State, local, tribal, territorial, and nongovernmental organization practitioners, including representatives from the following entities:

(A) The Office of Public Affairs of the Department.
(B) The Office of the Chief Information Officer of the Department.
(C) The Privacy Office of the Department.
(D) The Federal Emergency Management Agency.
(E) The Office of Disability Integration and Coordination of the Federal Emergency Management Agency.
(F) The American Red Cross.
(G) The Forest Service.
(H) The Centers for Disease Control and Prevention.
(I) The United States Geological Survey.
(J) The National Oceanic and Atmospheric Administration.

(2) Chairperson; co-chairperson

(A) Chairperson

The Secretary, or a designee of the Secretary, shall serve as the chairperson of the Group.

(B) Co-chairperson

The chairperson shall designate, on a rotating basis, a representative from a State or local government who is a member of the Group to serve as the co-chairperson of the Group.

(3) Additional members

The chairperson shall appoint, on a rotating basis, qualified individuals to the Group. The total number of such additional members shall—

(A) be equal to or greater than the total number of regular members under paragraph (1); and
(B) include—
(i) not fewer than 3 representatives from the private sector; and
(ii) representatives from—
(I) State, local, tribal, and territorial entities, including from—
(aa) law enforcement;
(bb) fire services;
(cc) emergency management; and
(dd) public health entities;

(II) universities and academia; and
(III) nonprofit disaster relief organizations.

(4) Term limits

The chairperson shall establish term limits for individuals appointed to the Group under paragraph (3).

(d) Consultation with non-members

To the extent practicable, the Group shall work with entities in the public and private sectors to carry out subsection (b).

(e) Meetings

(1) Initial meeting

Not later than 90 days after November 5, 2015, the Group shall hold its initial meeting.

(2) Subsequent meetings

After the initial meeting under paragraph (1), the Group shall meet—

(A) at the call of the chairperson; and

(B) not less frequently than twice each year.

(3) Virtual meetings

Each meeting of the Group may be held virtually.

(f) Reports

During each year in which the Group meets, the Group shall submit to the appropriate congressional committees a report that includes the following:

(1) A review and analysis of current and emerging social media technologies being used to support preparedness and response activities related to natural disasters and acts of terrorism and other man-made disasters.

(2) A review of best practices and lessons learned on the use of social media technologies during the response to natural disasters and acts of terrorism and other man-made disasters that occurred during the period covered by the report at issue.

(3) Recommendations to improve the Department's use of social media technologies for emergency management purposes.

(4) Recommendations to improve public awareness of the type of information disseminated through social media technologies, and how to access such information, during a natural disaster or an act of terrorism or other man-made disaster.

(5) A review of available training for Federal, State, local, tribal, and territorial officials on the use of social media technologies in response to a natural disaster or an act of terrorism or other man-made disaster.

(6) A review of coordination efforts with the private sector to discuss and resolve legal, operational, technical, privacy, and security concerns.

(g) Duration of group

(1) In general

The Group shall terminate on the date that is 5 years after November 5, 2015, unless the chairperson renews the Group for a successive 5-year period, prior to the date on which the Group would otherwise terminate, by submitting to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a certification that the continued existence of the Group is necessary to fulfill the purpose described in subsection (b).

(2) Continued renewal

The chairperson may continue to renew the Group for successive 5-year periods by submitting a certification in accordance with paragraph (1) prior to the date on which the Group would otherwise terminate.

(Pub. L. 107–296, title III, §318, as added Pub. L. 114–80, §2(a), Nov. 5, 2015, 129 Stat. 646.)

§195e. Transparency in research and development

(a) Requirement to list research and development programs

(1) In general

The Secretary shall maintain a detailed list of the following:

(A) Each classified and unclassified research and development project, and all appropriate details for each such project, including the component of the Department responsible for each such project.

(B) Each task order for a Federally Funded Research and Development Center not associated with a research and development project.

(C) Each task order for a University-based center of excellence not associated with a research and development project.

(D) The indicators developed and tracked by the Under Secretary for Science and Technology with respect to transitioned projects pursuant to subsection (c).

(2) Exception for certain completed projects

Paragraph (1) shall not apply to a project completed or otherwise terminated before December 23, 2016.

(3) Updates

The list required under paragraph (1) shall be updated as frequently as possible, but not less frequently than once per quarter.

(4) Research and development defined

For purposes of the list required under paragraph (1), the Secretary shall provide a definition for the term "research and development".

(b) Requirement to report to Congress on all projects

Not later than January 1, 2017, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified and unclassified report, as applicable, that lists each ongoing classified and unclassified project at the Department, including all appropriate details of each such project.

(c) Indicators of success of transitioned projects

(1) In general

For each project that has been transitioned to practice from research and development, the Under Secretary for Science and Technology shall develop and track indicators to demonstrate the uptake of the technology or project among customers or end-users.

(2) Requirement

To the fullest extent possible, the tracking of a project required under paragraph (1) shall continue for the three-year period beginning on the date on which such project was transitioned to practice from research and development.

(d) Definitions

In this section:

(1) All appropriate details

The term "all appropriate details" means, with respect to a research and development project—

(A) the name of such project, including both classified and unclassified names if applicable;

(B) the name of the component of the Department carrying out such project;

(C) an abstract or summary of such project;

(D) funding levels for such project;

(E) project duration or timeline;

(F) the name of each contractor, grantee, or cooperative agreement partner involved in such project;

(G) expected objectives and milestones for such project; and

(H) to the maximum extent practicable, relevant literature and patents that are associated with such project.

(2) Classified

The term "classified" means anything containing—

(A) classified national security information as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order;

(B) Restricted Data or data that was formerly Restricted Data, as defined in section 2014(y) of title 42;

(C) material classified at the Sensitive Compartmented Information (SCI) level, as defined in section 3345 of title 50; or

(D) information relating to a special access program, as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order.

(3) Controlled unclassified information

The term "controlled unclassified information" means information described as "Controlled Unclassified Information" under Executive Order 13556 (50 U.S.C. 3501 note) [1] or any successor order.

(4) Project

The term "project" means a research or development project, program, or activity administered by the Department, whether ongoing, completed, or otherwise terminated.

(e) Limitation

Nothing in this section overrides or otherwise affects the requirements specified in section 468 of this title.

(Pub. L. 107–296, title III, §319, as added Pub. L. 114–328, div. A, title XIX, §1906(a), Dec. 23, 2016, 130 Stat. 2676.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order 13556, referred to in subsec. (d)(3), is set out as a note under section 3501 of Title 44, Public Printing and Documents.

PRIOR PROVISIONS

A prior section 319 of Pub. L. 107–296 was renumbered section 320 and is classified to section 195f of this title.

[1] *See References in Text note below.*

§195f. EMP and GMD mitigation research and development and threat assessment, response, and recovery

(a) In general

In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of threats of EMP and GMD.

(b) Scope

The scope of the research and development under subsection (a) shall include the following:

(1) An objective scientific analysis—

(A) evaluating the risks to critical infrastructure from a range of threats of EMP and GMD; and

(B) which shall—

(i) be conducted in conjunction with the Office of Intelligence and Analysis; and

(ii) include a review and comparison of the range of threats and hazards facing critical infrastructure of the electrical grid.

(2) Determination of the critical utilities and national security assets and infrastructure that are at risk from threats of EMP and GMD.

(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, which shall include a review of the feasibility of rapidly isolating one or more portions of the electrical grid from the main electrical grid.

(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to threats of EMP and GMD, including an analysis of neutral current blocking devices that may protect high-voltage transmission lines.

(5) The restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption from various threats of EMP and GMD, as informed by the objective scientific analysis conducted under paragraph (1).

(6) An analysis of the feasibility of a real-time alert system to inform electrical grid operators and other stakeholders within milliseconds of a high-altitude nuclear explosion.

(c) Exemption from disclosure

(1) Information shared with the Federal Government

Section 673 of this title, and any regulations issued pursuant to such section, shall apply to any information shared with the Federal Government under this section.

(2) Information shared by the Federal Government

Information shared by the Federal Government with a State, local, or tribal government under this section shall be exempt from disclosure under any provision of State, local, or tribal freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

(d) Threat assessment, response, and recovery

(1) Roles and responsibilities

(A) Distribution of information

(i) In general

Beginning not later than June 19, 2020, the Secretary shall provide timely distribution of information on EMPs and GMDs to Federal, State, and local governments, owners and operators of critical infrastructure, and other persons determined appropriate by the Secretary.

(ii) Briefing

The Secretary shall brief the appropriate congressional committees on the effectiveness of the distribution of information under clause (i).

(B) Response and recovery

(i) In general

The Administrator of the Federal Emergency Management Agency shall—

(I) coordinate the response to and recovery from the effects of EMPs and GMDs on critical infrastructure, in coordination with the heads of appropriate Sector-Specific Agencies, and on matters related to the bulk power system, in consultation with the Secretary of Energy and the Federal Energy Regulatory Commission; and

(II) to the extent practicable, incorporate events that include EMPs and extreme GMDs as a factor in preparedness scenarios and exercises.

(ii) Implementation

The Administrator of the Federal Emergency Management Agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, and on matters related to the bulk power system, the Secretary of Energy and the Federal Energy Regulatory

Commission, shall—

(I) not later than June 19, 2020, develop plans and procedures to coordinate the response to and recovery from EMP and GMD events; and

(II) not later than December 21, 2020, conduct a national exercise to test the preparedness and response of the Nation to the effect of an EMP or extreme GMD event.

(C) Research and development

(i) In general

The Secretary, in coordination with the heads of relevant Sector-Specific Agencies, shall—

(I) without duplication of existing or ongoing efforts, conduct research and development to better understand and more effectively model the effects of EMPs and GMDs on critical infrastructure (which shall not include any system or infrastructure of the Department of Defense or any system or infrastructure of the Department of Energy associated with nuclear weapons activities); and

(II) develop technologies to enhance the resilience of and better protect critical infrastructure.

(ii) Plan

Not later than March 26, 2020, and in coordination with the heads of relevant Sector-Specific Agencies, the Secretary shall submit to the appropriate congressional committees a research and development action plan to rapidly address modeling shortfall and technology development.

(D) Emergency information system

(i) In general

The Administrator of the Federal Emergency Management Agency, in coordination with relevant stakeholders, shall maintain a network of systems, such as the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title, that are capable of providing appropriate emergency information to the public before (if possible), during, and in the aftermath of an EMP or GMD.

(ii) Briefing

Not later than December 21, 2020, the Administrator of the Federal Emergency Management Agency, shall brief the appropriate congressional committees regarding the maintenance of systems, including the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title.

(E) Quadrennial risk assessments

(i) In general

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce, and informed by intelligence-based threat assessments, shall conduct a quadrennial EMP and GMD risk assessment.

(ii) Briefings

Not later than March 26, 2020, and every four years thereafter until 2032, the Secretary, the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce shall provide a briefing to the appropriate congressional committees regarding the quadrennial EMP and GMD risk assessment.

(iii) Enhancing resilience

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other relevant Sector-Specific Agencies, shall use the results of the quadrennial EMP and GMD risk assessments to better understand and to

improve resilience to the effects of EMPs and GMDs across all critical infrastructure sectors, including coordinating the prioritization of critical infrastructure at greatest risk to the effects of EMPs and GMDs.

(2) Coordination

(A) Report on technological options

Not later than December 21, 2020, and every four years thereafter until 2032, the Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the heads of other appropriate agencies, and, as appropriate, private-sector partners, shall submit to the appropriate congressional committees, a report that—

(i) assesses the technological options available to improve the resilience of critical infrastructure to the effects of EMPs and GMDs; and

(ii) identifies gaps in available technologies and opportunities for technological developments to inform research and development activities.

(B) Test data

(i) In general

Not later than December 20, 2020, the Secretary, in coordination with the heads of Sector-Specific Agencies, the Secretary of Defense, and the Secretary of Energy, shall—

(I) review test data regarding the effects of EMPs and GMDs on critical infrastructure systems, networks, and assets representative of those throughout the Nation; and

(II) identify any gaps in the test data.

(ii) Plan

Not later than 180 days after identifying gaps in test data under clause (i), the Secretary, in coordination with the heads of Sector-Specific Agencies and in consultation with the Secretary of Defense and the Secretary of Energy, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps.

(iii) Implementation

The heads of each agency identified in the plan developed under clause (ii) shall implement the plan in collaboration with the voluntary efforts of the private sector, as appropriate.

(3) Definitions

In this subsection:

(A) The term "appropriate congressional committees" means—

(i) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Energy and Natural Resources, and the Committee on Commerce, Science, and Transportation of the Senate; and

(ii) the Committee on Transportation and Infrastructure, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Science, Space and Technology of the House of Representatives.

(B) The terms "prepare" and "preparedness" mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the homeland, including the prediction and notification of impending EMPs and GMDs.

(C) The term "Sector Risk Management Agency" has the meaning given that term in section 650 of this title.

(e) Rule of construction

Nothing in this section may be construe— [1]

(1) to affect in any manner the authority of the executive branch to implement Executive Order 13865, dated March 26, 2019, and entitled "Coordinating National Resilience to Electromagnetic Pulses", or any other authority existing on the day before December 20, 2019, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note), including the authority under section 824o of title 16, and including the authority of independent agencies to be independent; or

(2) as diminishing or transferring any authorities vested in the Administrator of the Federal Emergency Management Agency or in the Agency prior to December 20, 2019.

(Pub. L. 107–296, title III, §320, formerly §319, as added Pub. L. 114–328, div. A, title XIX, §1913(a)(3), Dec. 23, 2016, 130 Stat. 2685; renumbered §320 and amended Pub. L. 115–278, §2(g)(3)(B), (C), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 116–92, div. A, title XVII, §1740(a)(1), Dec. 20, 2019, 133 Stat. 1821; Pub. L. 116–283, div. H, title XC, §9002(c)(2)(A), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(A), Dec. 23, 2022, 136 Stat. 3659.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order 13865, referred to in subsec. (e)(1), is Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, which is set out as a note under this section.

Section 61003(c) of division F of the Fixing America's Surface Transportation Act, referred to in subsec. (e)(1), is section 61003(c) of Pub. L. 114–94, div. F, Dec. 4, 2015, 129 Stat. 1778, which is set out as a note under section 121 of this title.

AMENDMENTS

2022—Subsec. (d)(3)(C). Pub. L. 117–263 substituted "section 650 of this title" for "section 651 of this title".

2021—Subsec. (d)(3)(C). Pub. L. 116–283, §9002(c)(2)(A)(i), substituted "Sector Risk Management Agency" for "Sector-Specific Agency".

Subsec. (e)(1). Pub. L. 116–283, §9002(c)(2)(A)(ii), substituted "Sector Risk Management Agency" for "Sector-Specific Agency".

2019—Pub. L. 116–92, §1740(a)(1)(A), inserted "and threat assessment, response, and recovery" after "development" in section catchline.

Subsecs. (d), (e). Pub. L. 116–92, §1740(a)(1)(B), added subsecs. (d) and (e).

2018—Subsec. (c)(1). Pub. L. 115–278, §2(g)(3)(C), substituted "Section 673 of this title" for "Section 133 of this title".

STATUTORY NOTES AND RELATED SUBSIDIARIES

BENCHMARKS; DEFINITIONS

Pub. L. 116–92, div. A, title XVII, §1740(d), (h), Dec. 20, 2019, 133 Stat. 1824, 1825, provided that:

"(d) BENCHMARKS.—Not later than March 26, 2020, and as appropriate thereafter, the Secretary of Energy, in consultation with the Secretary of Defense, the Secretary of Homeland Security, and, as appropriate, the private sector, may develop or update, as necessary, quantitative and voluntary benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure. Nothing in this subsection shall affect the authority of the Electric Reliability Organization to develop and enforce, or the authority of the Federal Energy Regulatory Commission to approve, reliability standards.

"(h) DEFINITIONS.—In this section [amending this section and section 347 of this title and enacting this note and provisions not set out in the Code]:

"(1) The term 'appropriate congressional committees' has the meaning given that term in subsection (d) of section 320 of the Homeland Security Act of 2002 [6 U.S.C. 195f(d)], as added by subsection (a) of this section; and

"(2) The terms 'critical infrastructure', 'EMP', and 'GMD' have the meanings given such terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)."

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13865. COORDINATING NATIONAL RESILIENCE TO ELECTROMAGNETIC PULSES

Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Purpose*. An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs.

SEC. 2. *Definitions*. As used in this order:

(a) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) "Electromagnetic pulse" is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth. A geomagnetic disturbance (GMD) is a type of natural EMP driven by a temporary disturbance of Earth's magnetic field resulting from interactions with solar eruptions. Both HEMPs and GMDs can affect large geographic areas.

(c) "National Critical Functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(d) "National Essential Functions" means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as an EMP that adversely affects the performance of Government.

(e) "Prepare" and "preparedness" mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. These terms include the prediction and notification of impending EMPs.

(f) A "Sector-Specific Agency" (SSA) is the Federal department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

SEC. 3. *Policy*. (a) It is the policy of the United States to prepare for the effects of EMPs through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement. The Federal Government must provide warning of an impending EMP; protect against, respond to, and recover from the effects of an EMP through public and private engagement, planning, and investment; and prevent adversarial events through deterrence, defense, and nuclear nonproliferation efforts. To achieve these goals, the Federal Government shall engage in risk-informed planning, prioritize research and development (R&D) to address the needs of critical infrastructure stakeholders, and, for adversarial threats, consult Intelligence Community assessments.

(b) To implement the actions directed in this order, the Federal Government shall promote collaboration and facilitate information sharing, including the sharing of threat and vulnerability assessments, among executive departments and agencies (agencies), the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate. The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innovation that strengthens critical infrastructure against the effects of EMPs through the development and implementation of best practices, regulations, and appropriate guidance.

SEC. 4. *Coordination*. (a) The Assistant to the President for National Security Affairs (APNSA), through National Security Council staff and in consultation with the Director of the Office of Science and Technology Policy (OSTP), shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of EMPs. The APNSA shall, on an annual basis, submit a report to the President summarizing progress on the implementation of this order, identifying gaps in capability, and recommending how to address those gaps.

(b) To further the Federal R&D necessary to prepare the Nation for the effects of EMPs, the Director of OSTP shall coordinate efforts of agencies through the National Science and Technology Council (NSTC). The Director of OSTP, through the NSTC, shall annually review and assess the R&D needs of agencies conducting preparedness activities for EMPs, consistent with this order.

SEC. 5. *Roles and Responsibilities*. (a) The Secretary of State shall:

(i) lead the coordination of diplomatic efforts with United States allies and international partners regarding enhancing resilience to the effects of EMPs; and

(ii) in coordination with the Secretary of Defense and the heads of other relevant agencies, strengthen nuclear nonproliferation and deterrence efforts, which would reduce the likelihood of an EMP attack on the United States or its allies and partners by limiting the availability of nuclear devices.

(b) The Secretary of Defense shall:

(i) in cooperation with the heads of relevant agencies and with United States allies, international partners, and private-sector entities as appropriate, improve and develop the ability to rapidly characterize, attribute, and provide warning of EMPs, including effects on space systems of interest to the United States;

(ii) provide timely operational observations, analyses, forecasts, and other products for naturally occurring EMPs to support the mission of the Department of Defense along with United States allies and international partners, including the provision of alerts and warnings for natural EMPs that may affect weapons systems, military operations, or the defense of the United States;

(iii) conduct R&D and testing to understand the effects of EMPs on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of EMPs, and develop technologies to protect Department of Defense systems and infrastructure from the effects of EMPs to ensure the successful execution of Department of Defense missions;

(iv) review and update existing EMP-related standards for Department of Defense systems and infrastructure, as appropriate;

(v) share technical expertise and data regarding EMPs and their potential effects with other agencies and with the private sector, as appropriate;

(vi) incorporate attacks that include EMPs as a factor in defense planning scenarios; and

(vii) defend the Nation from adversarial EMPs originating outside of the United States through defense and deterrence, consistent with the mission and national security policy of the Department of Defense.

(c) The Secretary of the Interior shall support the research, development, deployment, and operation of capabilities that enhance understanding of variations of Earth's magnetic field associated with EMPs.

(d) The Secretary of Commerce shall:

(i) provide timely and accurate operational observations, analyses, forecasts, and other products for natural EMPs, exclusive of the responsibilities of the Secretary of Defense set forth in subsection (b)(ii) of this section; and

(ii) use the capabilities of the Department of Commerce, the private sector, academia, and nongovernmental organizations to continuously improve operational forecasting services and the development of standards for commercial EMP technology.

(e) The Secretary of Energy shall conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize sources of EMPs and their couplings to the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.

(f) The Secretary of Homeland Security shall:

(i) provide timely distribution of information on EMPs and credible associated threats to Federal, State, and local governments, critical infrastructure owners and operators, and other stakeholders;

(ii) in coordination with the heads of any relevant SSAs, use the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs;

(iii) coordinate response to and recovery from the effects of EMPs on critical infrastructure, in coordination with the heads of appropriate SSAs;

(iv) incorporate events that include EMPs as a factor in preparedness scenarios and exercises;

(v) in coordination with the heads of relevant SSAs, conduct R&D to better understand and more effectively model the effects of EMPs on national critical functions and associated critical infrastructure—excluding Department of Defense systems and infrastructure—and develop technologies and guidelines to enhance these functions and better protect this infrastructure;

(vi) maintain survivable means to provide necessary emergency information to the public during and after EMPs; and

(vii) in coordination with the Secretaries of Defense and Energy, and informed by intelligence-based threat assessments, develop quadrennial risk assessments on EMPs, with the first risk assessment delivered within 1 year of the date of this order [Mar. 26, 2019].

(g) The Director of National Intelligence shall:

(i) coordinate the collection, analysis, and promulgation, as appropriate, of intelligence-based assessments on adversaries' capabilities to conduct an attack utilizing an EMP and the likelihood of such an attack; and

(ii) provide intelligence-based threat assessments to support the heads of relevant SSAs in the development of quadrennial risk assessments on EMPs.

(h) The heads of all SSAs, in coordination with the Secretary of Homeland Security, shall enhance and facilitate information sharing with private-sector counterparts, as appropriate, to enhance preparedness for the effects of EMPs, to identify and share vulnerabilities, and to work collaboratively to reduce vulnerabilities.

(i) The heads of all agencies that support National Essential Functions shall ensure that their all-hazards preparedness planning sufficiently addresses EMPs, including through mitigation, response, and recovery, as directed by national preparedness policy.

SEC. 6. *Implementation*. (a) Identifying national critical functions and associated priority critical infrastructure at greatest risk.

(i) Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security. The Secretary of Homeland Security shall update this list as necessary.

(ii) Within 1 year of the identification described in subsection (a)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies as appropriate, shall, using appropriate government and private-sector standards for EMPs, assess which identified critical infrastructure systems, networks, and assets are most vulnerable to the effects of EMPs. The Secretary of Homeland Security shall provide this list to the President, through the APNSA. The Secretary of Homeland Security shall update this list using the results produced pursuant to subsection (b) of this section, and as necessary thereafter.

(b) Improving understanding of the effects of EMPs.

(i) Within 180 days of the identification described in subsection (a)(ii) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall review test data—identifying any gaps in such data—regarding the effects of EMPs on critical infrastructure systems, networks, and assets representative of those throughout the Nation.

(ii) Within 180 days of identifying the gaps in existing test data, as directed by subsection (b)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps. The heads of agencies identified in the plan shall implement the plan in collaboration with the private sector, as appropriate.

(iii) Within 1 year of the date of this order, and as appropriate thereafter, the Secretary of Energy, in consultation with the heads of other agencies and the private sector, as appropriate, shall review existing standards for EMPs and develop or update, as necessary, quantitative benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure.

(iv) Within 4 years of the date of this order, the Secretary of the Interior shall complete a magnetotelluric survey of the contiguous United States to help critical infrastructure owners and operators conduct EMP vulnerability assessments.

(c) Evaluating approaches to mitigate the effects of EMPs.

(i) Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, and in consultation with the Director of OSTP, the heads of other appropriate agencies, and private-sector partners as appropriate, shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of EMPs. The Secretaries of Defense, Energy, and Homeland Security shall also identify gaps in available technologies and opportunities for future technological developments to inform R&D activities.

(ii) Within 180 days of the completion of the activities directed by subsections (b)(iii) and (c)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies and in

consultation with the private sector as appropriate, shall develop and implement a pilot test to evaluate available engineering approaches for mitigating the effects of EMPs on the most vulnerable critical infrastructure systems, networks, and assets, as identified in subsection (a)(ii) of this section.

(iii) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of relevant SSAs, and in consultation with appropriate regulatory and utility commissions and other stakeholders, shall identify regulatory and non-regulatory mechanisms, including cost recovery measures, that can enhance private-sector engagement to address the effects of EMPs.

(d) Strengthening critical infrastructure to withstand the effects of EMPs.

(i) Within 90 days of completing the actions directed in subsection (c)(ii) of this section, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy and in consultation with the heads of other appropriate agencies and with the private sector as appropriate, shall develop a plan to mitigate the effects of EMPs on the vulnerable priority critical infrastructure systems, networks, and assets identified under subsection (a)(ii) of this section. The plan shall align with and build on actions identified in reports required by Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) [6 U.S.C. 1500 note prec.]. The Secretary of Homeland Security shall implement those elements of the plan that are consistent with Department of Homeland Security authorities and resources, and report to the APNSA regarding any additional authorities and resources needed to complete its implementation. The Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, shall update the plan as necessary based on results from the actions directed in subsections (b) and (c) of this section.

(ii) Within 180 days of the completion of the actions identified in subsection (c)(i) of this section, the Secretary of Defense, in consultation with the Secretaries of Homeland Security and Energy, shall conduct a pilot test to evaluate engineering approaches used to harden a strategic military installation, including infrastructure that is critical to supporting that installation, against the effects of EMPs.

(iii) Within 180 days of completing the pilot test described in subsection (d)(ii) of this section, the Secretary of Defense shall report to the President, through the APNSA, regarding the cost and effectiveness of the evaluated approaches.

(e) Improving response to EMPs.

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, in coordination with the heads of appropriate SSAs, shall review and update Federal response plans, programs, and procedures to account for the effects of EMPs.

(ii) Within 180 days of the completion of actions directed by subsection (e)(i) of this section, agencies that support National Essential Functions shall update operational plans documenting their procedures and responsibilities to prepare for, protect against, and mitigate the effects of EMPs.

(iii) Within 180 days of identifying vulnerable priority critical infrastructure systems, networks, and assets as directed by subsection (a)(ii) of this section, the Secretary of Homeland Security, in consultation with the Secretaries of Defense and Commerce, and the Chairman of the Federal Communications Commission, shall provide the Deputy Assistant to the President for Homeland Security and Counterterrorism and the Director of OSTP with an assessment of the effects of EMPs on critical communications infrastructure, and recommend changes to operational plans to enhance national response and recovery efforts after an EMP.

SEC. 7. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

[1] So in original. Probably should be "construed—".

§195g. Countering Unmanned Aircraft Systems Coordinator

(a) Coordinator

(1) In general

The Secretary shall designate an individual in a Senior Executive Service position (as defined in section 3132 of title 5) of the Department within the Office of Strategy, Policy, and Plans as the Countering Unmanned Aircraft Systems Coordinator (in this section referred to as the "Coordinator") and provide appropriate staff to carry out the responsibilities of the Coordinator.

(2) Responsibilities

The Coordinator shall—

(A) oversee and coordinate with relevant Department offices and components, including the Office of Civil Rights and Civil Liberties and the Privacy Office, on the development of guidance and regulations to counter threats associated with unmanned aircraft systems (in this section referred to as "UAS") as described in section 124n of this title;

(B) promote research and development of counter UAS technologies in coordination within the Science and Technology Directorate;

(C) coordinate with the relevant components and offices of the Department, including the Office of Intelligence and Analysis, to ensure the sharing of information, guidance, and intelligence relating to countering UAS threats, counter UAS threat assessments, and counter UAS technology, including the retention of UAS and counter UAS incidents within the Department;

(D) serve as the Department liaison, in coordination with relevant components and offices of the Department, to the Department of Defense, Federal, State, local, and Tribal law enforcement entities, and the private sector regarding the activities of the Department relating to countering UAS;

(E) maintain the information required under section 124n(g)(3) of this title; and

(F) carry out other related counter UAS authorities and activities under section 124n of this title, as directed by the Secretary.

(b) Coordination with applicable Federal laws

The Coordinator shall, in addition to other assigned duties, coordinate with relevant Department components and offices to ensure testing, evaluation, or deployment of a system used to identify, assess, or defeat a UAS is carried out in accordance with applicable Federal laws.

(c) Coordination with private sector

The Coordinator shall, among other assigned duties, working with the Office of Partnership and Engagement and other relevant Department offices and components, or other Federal agencies, as appropriate, serve as the principal Department official responsible for sharing to the private sector information regarding counter UAS technology, particularly information regarding instances in which counter UAS technology may impact lawful private sector services or systems.

(Pub. L. 107–296, title III, §321, as added Pub. L. 116–260, div. U, title VII, §701(b)(1), Dec. 27, 2020, 134 Stat. 2295.)

§195h. National Urban Security Technology Laboratory

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 188(c)(2) of this title. Such laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

(b) Laboratory described

The laboratory described in this subsection is the laboratory—

(1) known, as of December 27, 2021, as the National Urban Security Technology Laboratory; and

(2) transferred to the Department pursuant to section 183(1)(E) of this title.

(c) Laboratory activities

The National Urban Security Technology Laboratory shall—

(1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of such technologies that can connect to the internet, for emergency response providers;

(2) act as a technical advisor to emergency response providers; and

(3) carry out other such activities as the Secretary determines appropriate.

(d) Rule of construction

Nothing in this section may be construed as affecting in any manner the authorities or responsibilities of the Countering Weapons of Mass Destruction Office of the Department.

(Pub. L. 107–296, title III, §322, as added Pub. L. 117–81, div. F, title LXIV, §6406(a), Dec. 27, 2021, 135 Stat. 2402.)

§195i. Chemical Security Analysis Center

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 188(c)(2) of this title, which shall be used to conduct studies, analyses, and research to assess and address domestic chemical security events.

(b) Laboratory described

The laboratory described in this subsection is the laboratory known, as of December 23, 2022, as the Chemical Security Analysis Center.

(c) Laboratory activities

Pursuant to the authority under section 182(4) of this title, the Chemical Security Analysis Center shall—

(1) identify and develop approaches and mitigation strategies to domestic chemical security threats, including the development of comprehensive, research-based definable goals relating to such approaches and mitigation strategies;

(2) provide an enduring science-based chemical threat and hazard analysis capability;

(3) provide expertise regarding risk and consequence modeling, chemical sensing and detection, analytical chemistry, acute chemical toxicology, synthetic chemistry and reaction characterization, and nontraditional chemical agents and emerging chemical threats;

(4) staff and operate a technical assistance program that provides operational support and subject matter expertise, design and execute laboratory and field tests, and provide a comprehensive knowledge repository of chemical threat information that is continuously updated with data from scientific, intelligence, operational, and private sector sources;

(5) consult, as appropriate, with the Countering Weapons of Mass Destruction Office of the Department to mitigate, prepare, and respond to threats, hazards, and risks associated with domestic chemical security events; and

(6) carry out such other activities authorized under this section as the Secretary determines appropriate.

(d) Special rule

Nothing in this section amends, alters, or affects—

(1) the responsibilities of the Countering Weapons of Mass Destruction Office of the Department; or

(2) the activities or requirements authorized to other entities within the Federal Government, including the activities and requirements of the Environmental Protection Agency under section 7412(r) of title 42, the Toxic Substances Control Act (15 U.S.C. 2601 et seq.), and the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (commonly referred to as "Superfund"; 42 U.S.C. 9601 et seq.).

(Pub. L. 107–296, title III, §323, as added Pub. L. 117–263, div. G, title LXXI, §7106(a), Dec. 23, 2022, 136 Stat. 3624.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Toxic Substances Control Act, referred to in subsec. (d)(2), is Pub. L. 94–469, Oct. 11, 1976, 90 Stat. 2003, which is classified generally to chapter 53 (§2601 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 2601 of Title 15 and Tables.

The Comprehensive Environmental Response, Compensation, and Liability Act of 1980, referred to in subsec. (d)(2), is Pub. L. 96–510, Dec. 11, 1980, 94 Stat. 2767, which is classified principally to chapter 103 (§9601 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 9601 of Title 42 and Tables.

SUBCHAPTER IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

EDITORIAL NOTES

CODIFICATION

Pub. L. 114–125, title VIII, §802(g)(1)(B)(i), Feb. 24, 2016, 130 Stat. 211, substituted "BORDER, MARITIME, AND TRANSPORTATION SECURITY" for "DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY" in subchapter heading.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEPARTMENT OF HOMELAND SECURITY NORTHERN BORDER MISSION CENTER

Pub. L. 118–159, div. E, title LVI, §5611, Dec. 23, 2024, 138 Stat. 2457, provided that:

"(a) ESTABLISHMENT.—Not later than 1 year after the date of the enactment of this Act [Dec. 23, 2024], the Secretary shall establish the Department of Homeland Security Northern Border Mission Center.

"(b) PURPOSE.—The purpose of the Center shall be to serve as the Department's forward deployed centralized operations support center for domain awareness, information sharing, intelligence, training, and stakeholder engagement with Federal, State, tribal, local, and international government partners along the northern border of the United States.

"(c) LOCATION.—The Center shall be placed along the northern border at a location that is collocated with an existing U.S. Border Patrol sector headquarters, an Air and Marine Operations branch, and a United States Coast Guard air station, and other existing Department activities.

"(d) COMPONENTS.—

"(1) IN GENERAL.—The Center shall collocate personnel and activities of—

"(A) U.S. Customs and Border Protection;

"(B) the United States Coast Guard;

"(C) U.S. Immigration and Customs Enforcement's Homeland Security Investigations; and

"(D) other components and offices of the Department that the Secretary determines to be necessary, including to support the training, technology testing, and development described in subsection (e).

"(2) ADDITIONAL PERSONNEL.—Additional Federal, State, tribal, local, and international government partners may be collocated as the Secretary determines to be necessary and appropriate to support the operations described in this section.

"(e) FUNCTIONS.—

"(1) IN GENERAL.—The Center shall perform the functions described in this subsection in addition to any other functions assigned by the Secretary. In carrying out these functions, the Center shall support the Department's northern border security operations.

"(2) NORTHERN BORDER STRATEGY.—The Center, in collaboration with relevant offices and components of the Department, shall—

"(A) serve as a coordination mechanism for operational components for the implementation of the Department of Homeland Security Northern Border Strategy and any successor strategy and support appropriate offices of the Department in the evaluation and updating of the Department of Homeland Security Northern Border Strategy and any successor strategy; and

"(B) support the development of best practices and policies for personnel at the northern border to support such implementation.

"(3) TRAINING.—The Center shall serve as a training location to support the delivery of training or exercises for Department personnel and Federal, State, tribal, local, and international government partners.

"(4) RESOURCE AND TECHNOLOGICAL NEEDS AND CHALLENGES.—The Center, in collaboration with relevant offices and components of the Department, shall—

"(A) identify resource and technological needs or challenges affecting security along the northern border; and

"(B) serve as a testing ground and demonstration location for the testing of border security technology, including determining such technology's suitability and performance in the northern border and maritime environments.

"(5) AIR AND MARINE OPERATIONS.—

"(A) QUICK REACTION CAPABILITIES.—In support of the Center, U.S. Customs and Border Protection's Air and Marine Operations shall establish and maintain capability that is collocated with the Center and available for quick deployment in support of the northern border missions, U.S. Customs and Border Protection, and the Department, including missions in the Great Lakes region.

"(B) NORTHERN BORDER DOMAIN AWARENESS.—In order to coordinate with the Center and support its operations, the Air and Marine Operations Center shall collocate personnel and resources with the Center to enhance the Department's capabilities to—

"(i) support air and maritime domain awareness and information sharing efforts along the northern border;

"(ii) provide dedicated monitoring of northern border systems; and

"(iii) lead, in coordination with other U.S. Customs and Border Protection components, Federal, State, tribal, local, and international governments, and private sector partners, the Center's efforts to track and monitor legitimate cross-border traffic involving unmanned aircraft and unmanned aircraft systems.

"(6) COUNTER-UNMANNED AIRCRAFT SYSTEMS.—

"(A) IN GENERAL.—Pursuant to policies established by the Secretary, consistent with section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n), the Center shall support counter-unmanned aircraft systems operations along the northern border to respond to the increased use of unmanned aircraft systems.

"(B) RULE OF CONSTRUCTION.—Nothing in this section may be construed to provide additional authority related to detection, mitigation, research, development, or testing of unmanned aircraft systems or counter-unmanned aircraft systems.

"(7) PRIVACY AND CIVIL RIGHTS.—The Center, in collaboration with the Chief Privacy Officer and the Office for Civil Rights and Civil Liberties of the Department, shall ensure that operations and practices of the Center comply with the privacy and civil rights policies of the Department and its components, and as necessary, ensure there are resources or personnel available to support the Center's mission onsite.

"(8) NONCONTIGUOUS NORTHERN BORDER.—The Center, in collaboration with relevant offices and components of the Department, shall identify the specific challenges that exist along the noncontiguous international land border with Canada and the maritime border with Russia, including resource, technological challenges, and domain awareness.

"(f) ANNUAL REPORTING.—Not later than 180 days after the establishment of the Center, and annually thereafter, the Secretary shall submit a report, that may include a classified annex or a sensitive but

unclassified annex, to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives that describes the activities of the Center during the most recently concluded fiscal year, including—

"(1) personnel levels;

"(2) additional resources that are needed to support the operations of the Center and northern border operations of the Department; and

"(3) any additional assets or authorities that are needed to increase security and domain awareness along the northern border.

"(g) TEMPORARY DUTY ASSIGNMENTS.—The Secretary shall submit a quarterly report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding temporary duty assignments of U.S. Border Patrol agents during the reporting period, including—

"(1) the number of agents on temporary duty assignment;

"(2) the duration of the temporary duty assignment;

"(3) the sectors from which the agents were assigned; and

"(4) the sectors to which the agents were assigned.

"(h) REPORT ON LARGE UNMANNED AIRCRAFT SYSTEMS OPERATIONS.—Not later than 1 year after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Homeland Security shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives on the Department's operation of large unmanned aircraft systems. The report shall include information on existing large unmanned aircraft systems, as well as recommendations on how to enable the operations of large unmanned aircraft systems based at the Center established pursuant to subsection (a) of this section.

"(i) RULES OF CONSTRUCTION.—

"(1) AUTHORITY TO ESTABLISH CENTER.—The Center established pursuant to subsection (a) shall be established separate and distinct from the Secretary's authorities under section 708 of the Homeland Security Act of 2002 (6 U.S.C. 348).

"(2) COMMANDANT AUTHORITY.—Nothing in this section shall be construed to affect, impinge, or alter any authority of the Commandant of the Coast Guard under title 14 or title 46, United States Code, or limit the Commandant's discretion and ability to deploy Coast Guard assets and personnel.

"(j) SUNSET.—This section shall cease to be effective beginning on October 1, 2027.

"(k) NO ADDITIONAL FUNDS.—No additional funds are authorized to be appropriated for the purpose of carrying out this section.

"(l) DEFINITIONS.—In this section:

"(1) CENTER.—The term 'Center' means the Department of Homeland Security Northern Border Mission Center established pursuant to subsection (a).

"(2) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

"(3) NORTHERN BORDER.—The term 'northern border' means—

"(A) the international border between the United States and Canada; and

"(B) the maritime border between Alaska and the Russian Federation.

"(4) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security."

PART A—BORDER, MARITIME, AND TRANSPORTATION SECURITY RESPONSIBILITIES AND FUNCTIONS

EDITORIAL NOTES

CODIFICATION

Pub. L. 114–125, title VIII, §802(g)(1)(B)(ii)(I), Feb. 24, 2016, 130 Stat. 211, substituted "Border, Maritime, and Transportation Security Responsibilities and Functions" for "Under Secretary for Border and Transportation Security" in part heading.

§201. Repealed. Pub. L. 114–125, title VIII, §802(g)(2), Feb. 24, 2016, 130 Stat. 212

Section, Pub. L. 107–296, title IV, §401, Nov. 25, 2002, 116 Stat. 2177, established the Directorate of Border and Transportation Security headed by an Under Secretary for Border and Transportation Security.

§202. Border, maritime, and transportation responsibilities

The Secretary shall be responsible for the following:

(1) Preventing the entry of terrorists and the instruments of terrorism into the United States.

(2) Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.

(3) Carrying out the immigration enforcement functions vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or any officer, employee, or component of the Immigration and Naturalization Service) immediately before the date on which the transfer of functions specified under section 251 of this title takes effect.

(4) Establishing and administering rules, in accordance with section 236 of this title, governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States.

(5) Establishing national immigration enforcement policies and priorities.

(6) Except as provided in part C of this subchapter, administering the customs laws of the United States.

(7) Conducting the inspection and related administrative functions of the Department of Agriculture transferred to the Secretary of Homeland Security under section 231 of this title.

(8) In carrying out the foregoing responsibilities, ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce.

(Pub. L. 107–296, title IV, §402, Nov. 25, 2002, 116 Stat. 2177; Pub. L. 114–125, title VIII, §802(g)(1)(B)(ii)(II), Feb. 24, 2016, 130 Stat. 211.)

EDITORIAL NOTES

REFERENCES IN TEXT

Part C of this subchapter, referred to in par. (6), was in the original "subtitle C", meaning subtitle C (§421 et seq.) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2182, which enacted part C (§231 et seq.) of this subchapter and amended sections 2279e and 2279f of Title 7, Agriculture, and sections 115, 44901, and 47106 of Title 49, Transportation. For complete classification of subtitle C to the Code, see Tables.

The customs laws of the United States, referred to in par. (6), are classified generally to Title 19, Customs Duties.

AMENDMENTS

2016—Pub. L. 114–125 substituted "Border, maritime, and transportation responsibilities" for "Responsibilities" in section catchline and struck out ", acting through the Under Secretary for Border and Transportation Security," after "The Secretary" in introductory provisions.

§203. Functions transferred

In accordance with subchapter XII (relating to transition provisions), there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of—

(1) the United States Customs Service of the Department of the Treasury, including the functions of the Secretary of the Treasury relating thereto;

(2) the Transportation Security Administration of the Department of Transportation, including the functions of the Secretary of Transportation, and of the Under Secretary of Transportation for Security, relating thereto;

(3) the Federal Protective Service of the General Services Administration, including the functions of the Administrator of General Services relating thereto;

(4) the Federal Law Enforcement Training Center of the Department of the Treasury; and

(5) the Office for Domestic Preparedness of the Office of Justice Programs, including the functions of the Attorney General relating thereto.

(Pub. L. 107–296, title IV, §403, Nov. 25, 2002, 116 Stat. 2178.)

§204. Surface Transportation Security Advisory Committee

(a) Establishment

The Administrator of the Transportation Security Administration (referred to in this section as "Administrator") shall establish within the Transportation Security Administration the Surface Transportation Security Advisory Committee (referred to in this section as the "Advisory Committee").

(b) Duties

(1) In general

The Advisory Committee may advise, consult with, report to, and make recommendations to the Administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

(2) Risk-based security

The Advisory Committee shall consider risk-based security approaches in the performance of its duties.

(c) Membership

(1) Composition

The Advisory Committee shall be composed of—

(A) voting members appointed by the Administrator under paragraph (2); and

(B) nonvoting members, serving in an advisory capacity, who shall be designated by—

(i) the Transportation Security Administration;

(ii) the Department of Transportation;

(iii) the Coast Guard; and

(iv) such other Federal department or agency as the Administrator considers appropriate.

(2) Appointment

The Administrator shall appoint voting members from among stakeholders representing each mode of surface transportation, such as passenger rail, freight rail, mass transit, pipelines, highways, over-the-road bus, school bus industry, and trucking, including representatives from—

(A) associations representing such modes of surface transportation;

(B) labor organizations representing such modes of surface transportation;

(C) groups representing the users of such modes of surface transportation, including asset manufacturers, as appropriate;

(D) relevant law enforcement, first responders, and security experts; and

(E) such other groups as the Administrator considers appropriate.

(3) Chairperson

The Advisory Committee shall select a chairperson from among its voting members.

(4) Term of office

(A) Terms

(i) In general

The term of each voting member of the Advisory Committee shall be 2 years, but a voting member may continue to serve until the Administrator appoints a successor.

(ii) Reappointment

A voting member of the Advisory Committee may be reappointed.

(B) Removal

(i) In general

The Administrator may review the participation of a member of the Advisory Committee and remove such member for cause at any time.

(ii) Access to information

The Administrator may remove any member of the Advisory Committee that the Administrator determines should be restricted from reviewing, discussing, or possessing classified information or sensitive security information.

(5) Prohibition on compensation

The members of the Advisory Committee shall not receive any compensation from the Government by reason of their service on the Advisory Committee.

(6) Meetings

(A) In general

The Administrator shall require the Advisory Committee to meet at least semiannually in person or through web conferencing and may convene additional meetings as necessary.

(B) Public meetings

At least 1 of the meetings of the Advisory Committee each year shall be—

(i) announced in the Federal Register;

(ii) announced on a public website; and

(iii) open to the public.

(C) Attendance

The Advisory Committee shall maintain a record of the persons present at each meeting.

(D) Minutes

(i) In general

Unless otherwise prohibited by other Federal law, minutes of the meetings shall be published on the public website under subsection (e)(5).

(ii) Protection of classified and sensitive information

The Advisory Committee may redact or summarize, as necessary, minutes of the meetings to protect classified or other sensitive information in accordance with law.

(7) Voting member access to classified and sensitive security information

(A) Determinations

Not later than 60 days after the date on which a voting member is appointed to the Advisory Committee and before that voting member may be granted any access to classified information or sensitive security information, the Administrator shall determine if the voting member should be restricted from reviewing, discussing, or possessing classified information or sensitive security information.

(B) Access

(i) Sensitive security information

If a voting member is not restricted from reviewing, discussing, or possessing sensitive security information under subparagraph (A) and voluntarily signs a nondisclosure agreement, the voting member may be granted access to sensitive security information that is relevant to the voting member's service on the Advisory Committee.

(ii) Classified information

Access to classified materials shall be managed in accordance with Executive Order 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive order.

(C) Protections

(i) Sensitive security information

Voting members shall protect sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

(ii) Classified information

Voting members shall protect classified information in accordance with the applicable requirements for the particular level of classification.

(8) Joint committee meetings

The Advisory Committee may meet with 1 or more of the following advisory committees to discuss multimodal security issues and other security-related issues of common concern:

(A) Aviation Security Advisory Committee established under section 44946 of title 49.

(B) Maritime Security Advisory Committee established under section 70112 of title 46.

(C) Railroad Safety Advisory Committee established by the Federal Railroad Administration.

(9) Subject matter experts

The Advisory Committee may request the assistance of subject matter experts with expertise related to the jurisdiction of the Advisory Committee.

(d) Reports

(1) Periodic reports

The Advisory Committee shall periodically submit reports to the Administrator on matters requested by the Administrator or by a majority of the members of the Advisory Committee.

(2) Annual report

(A) Submission

The Advisory Committee shall submit to the Administrator and the appropriate congressional committees an annual report that provides information on the activities, findings, and recommendations of the Advisory Committee during the preceding year.

(B) Publication

Not later than 6 months after the date that the Administrator receives an annual report under subparagraph (A), the Administrator shall publish a public version of the report, in accordance with section 552a(b) of title 5.

(e) Administration response

(1) Consideration

The Administrator shall consider the information, advice, and recommendations of the Advisory Committee in formulating policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

(2) Feedback

Not later than 90 days after the date that the Administrator receives a recommendation from the Advisory Committee under subsection (d)(2), the Administrator shall submit to the Advisory Committee written feedback on the recommendation, including—

(A) if the Administrator agrees with the recommendation, a plan describing the actions that

the Administrator has taken, will take, or recommends that the head of another Federal department or agency take to implement the recommendation; or

(B) if the Administrator disagrees with the recommendation, a justification for that determination.

(3) Notices

Not later than 30 days after the date the Administrator submits feedback under paragraph (2), the Administrator shall—

(A) notify the appropriate congressional committees of the feedback, including the determination under subparagraph (A) or subparagraph (B) of that paragraph, as applicable; and

(B) provide the appropriate congressional committees with a briefing upon request.

(4) Updates

Not later than 90 days after the date the Administrator receives a recommendation from the Advisory Committee under subsection (d)(2) that the Administrator agrees with, and quarterly thereafter until the recommendation is fully implemented, the Administrator shall submit a report to the appropriate congressional committees or post on the public website under paragraph (5) an update on the status of the recommendation.

(5) Website

The Administrator shall maintain a public website that—

(A) lists the members of the Advisory Committee; and

(B) provides the contact information for the Advisory Committee.

(f) Nonapplicability of FACA

The Federal Advisory Committee Act (5 U.S.C. App.) [1] shall not apply to the Advisory Committee or any subcommittee established under this section.

(Pub. L. 107–296, title IV, §404, as added Pub. L. 115–254, div. K, title I, §1969(a), Oct. 5, 2018, 132 Stat. 3609.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order 13526, referred to in subsec. (c)(7)(B)(ii), is set out as a note under section 3161 of Title 50, War and National Defense.

The Federal Advisory Committee Act, referred to in subsec. (f), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SURFACE TRANSPORTATION SECURITY ADVISORY COMMITTEE MEMBERS

Pub. L. 115–254, div. K, title I, §1969(b), Oct. 5, 2018, 132 Stat. 3612, provided that:

"(1) VOTING MEMBERS.—Not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration] shall appoint the voting members of the Surface Transportation Security Advisory Committee established under section 404 of the Homeland Security Act of 2002 [6 U.S.C. 204], as added by subsection (a) of this section.

"(2) NONVOTING MEMBERS.—Not later than 90 days after the date of enactment of this Act, each Federal Government department and agency with regulatory authority over a mode of surface or maritime transportation, as the Administrator considers appropriate, shall designate an appropriate representative to serve as a nonvoting member of the Surface Transportation Security Advisory Committee."

[1] *See References in Text note below.*

§205. Ombudsman for immigration detention

(a) In general

Within the Department, there shall be a position of Immigration Detention Ombudsman (in this section referred to as the "Ombudsman"). The Ombudsman shall be independent of Department agencies and officers and shall report directly to the Secretary. The Ombudsman shall be a senior official with a background in civil rights enforcement, civil detention care and custody, and immigration law.

(b) Functions

The functions of the Ombudsman shall be to—

(1) Establish and administer an independent, neutral, and confidential process to receive, investigate, resolve, and provide redress, including referral for investigation to the Office of the Inspector General, referral to U.S. Citizenship and Immigration Services for immigration relief, or any other action determined appropriate, for cases in which Department officers or other personnel, or contracted, subcontracted, or cooperating entity personnel, are found to have engaged in misconduct or violated the rights of individuals in immigration detention;

(2) Establish an accessible and standardized process regarding complaints against any officer or employee of U.S. Customs and Border Protection or U.S. Immigration and Customs Enforcement, or any contracted, subcontracted, or cooperating entity personnel, for violations of law, standards of professional conduct, contract terms, or policy related to immigration detention;

(3) Conduct unannounced inspections of detention facilities holding individuals in federal immigration custody, including those owned or operated by units of State or local government and privately-owned or operated facilities;

(4) Review, examine, and make recommendations to address concerns or violations of contract terms identified in reviews, audits, investigations, or detainee interviews regarding immigration detention facilities and services;

(5) Provide assistance to individuals affected by potential misconduct, excessive force, or violations of law or detention standards by Department of Homeland Security officers or other personnel, or contracted, subcontracted, or cooperating entity personnel; and

(6) Ensure that the functions performed by the Ombudsman are complementary to existing functions within the Department of Homeland Security.

(c) Access to detention facilities

The Ombudsman or designated personnel of the Ombudsman, shall be provided unfettered access to any location within each such detention facility and shall be permitted confidential access to any detainee at the detainee's request and any departmental records concerning such detainee.

(d) Coordination with department components

(1) In general

The Director of U.S. Immigration and Customs Enforcement and the Commissioner of U.S. Customs and Border Protection shall each establish procedures to provide formal responses to recommendations submitted to such officials by the Ombudsman within 60 days of receiving such recommendations.

(2) Access to information

The Secretary shall establish procedures to provide the Ombudsman access to all departmental records necessary to execute the responsibilities of the Ombudsman under subsection (b) or (c) not later than 60 days after a request from the Ombudsman for such information.

(e) Annual report

The Ombudsman shall prepare a report to Congress on an annual basis on its activities, findings, and recommendations.

(Pub. L. 107–296, title IV, §405, as added Pub. L. 116–93, div. D, title I, §106(a), Dec. 20, 2019, 133 Stat. 2504.)

PART B—U.S. CUSTOMS AND BORDER PROTECTION

EDITORIAL NOTES

CODIFICATION

Pub. L. 114–125, title VIII, §802(g)(1)(B)(iii)(I), Feb. 24, 2016, 130 Stat. 211, substituted "U.S. Customs and Border Protection" for "United States Customs Service" in part heading.

§211. Establishment of U.S. Customs and Border Protection; Commissioner, Deputy Commissioner, and operational offices

(a) In general

There is established in the Department an agency to be known as U.S. Customs and Border Protection.

(b) Commissioner of U.S. Customs and Border Protection

(1) In general

There shall be at the head of U.S. Customs and Border Protection a Commissioner of U.S. Customs and Border Protection (in this section referred to as the "Commissioner").

(2) Committee referral

As an exercise of the rulemaking power of the Senate, any nomination for the Commissioner submitted to the Senate for confirmation, and referred to a committee, shall be referred to the Committee on Finance.

(c) Duties

The Commissioner shall—

(1) coordinate and integrate the security, trade facilitation, and trade enforcement functions of U.S. Customs and Border Protection;

(2) ensure the interdiction of persons and goods illegally entering or exiting the United States;

(3) facilitate and expedite the flow of legitimate travelers and trade;

(4) direct and administer the commercial operations of U.S. Customs and Border Protection, and the enforcement of the customs and trade laws of the United States;

(5) detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States, in cases in which such persons are entering, or have recently entered, the United States;

(6) safeguard the borders of the United States to protect against the entry of dangerous goods;

(7) ensure the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland;

(8) in coordination with U.S. Immigration and Customs Enforcement and United States Citizenship and Immigration Services, enforce and administer all immigration laws, as such term is defined in paragraph (17) of section 1101(a) of title 8, including—

(A) the inspection, processing, and admission of persons who seek to enter or depart the United States; and

(B) the detection, interdiction, removal, departure from the United States, short-term detention, and transfer of persons unlawfully entering, or who have recently unlawfully entered, the United States;

(9) develop and implement screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound;

(10) in coordination with the Secretary, deploy technology to collect the data necessary for the Secretary to administer the biometric entry and exit data system pursuant to section 1365b of title 8;

(11) enforce and administer the laws relating to agricultural import and entry inspection referred to in section 231 of this title;

(12) in coordination with the Under Secretary for Management of the Department, ensure U.S. Customs and Border Protection complies with Federal law, the Federal Acquisition Regulation, and the Department's acquisition management directives for major acquisition programs of U.S. Customs and Border Protection;

(13) ensure that the policies and regulations of U.S. Customs and Border Protection are consistent with the obligations of the United States pursuant to international agreements;

(14) enforce and administer—

(A) the Container Security Initiative program under section 205 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 945); and

(B) the Customs–Trade Partnership Against Terrorism program under subtitle B of title II of such Act (6 U.S.C. 961 et seq.);

(15) conduct polygraph examinations in accordance with section 221(1) of this title;

(16) establish the standard operating procedures described in subsection (k);

(17) carry out the training required under subsection (l);

(18) carry out section 218 of this title, relating to the issuance of Asia-Pacific Economic Cooperation Business Travel Cards; and

(19) carry out other duties and powers prescribed by law or delegated by the Secretary.

(d) Deputy Commissioner

There shall be in U.S. Customs and Border Protection a Deputy Commissioner who shall assist the Commissioner in the management of U.S. Customs and Border Protection.

(e) U.S. Border Patrol

(1) In general

There is established in U.S. Customs and Border Protection the U.S. Border Patrol.

(2) Chief

There shall be at the head of the U.S. Border Patrol a Chief, who shall—

(A) be at the level of Executive Assistant Commissioner within U.S. Customs and Border Protection; and

(B) report to the Commissioner.

(3) Duties

The U.S. Border Patrol shall—

(A) serve as the law enforcement office of U.S. Customs and Border Protection with primary responsibility for interdicting persons attempting to illegally enter or exit the United States or goods being illegally imported into or exported from the United States at a place other than a designated port of entry;

(B) deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband; and

(C) carry out other duties and powers prescribed by the Commissioner.

(f) Air and Marine Operations

(1) In general

There is established in U.S. Customs and Border Protection an office known as Air and Marine

Operations.

(2) Executive Assistant Commissioner

There shall be at the head of Air and Marine Operations an Executive Assistant Commissioner, who shall report to the Commissioner.

(3) Duties

Air and Marine Operations shall—

(A) serve as the law enforcement office within U.S. Customs and Border Protection with primary responsibility to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illicit drugs, and other contraband across the borders of the United States in the air and maritime environment;

(B) conduct joint aviation and marine operations with U.S. Immigration and Customs Enforcement;

(C) conduct aviation and marine operations with international, Federal, State, and local law enforcement agencies, as appropriate;

(D) administer the Air and Marine Operations Center established under paragraph (4); and

(E) carry out other duties and powers prescribed by the Commissioner.

(4) Air and Marine Operations Center

(A) In general

There is established in Air and Marine Operations an Air and Marine Operations Center.

(B) Executive Director

There shall be at the head of the Air and Marine Operations Center an Executive Director, who shall report to the Executive Assistant Commissioner of Air and Marine Operations.

(C) Duties

The Air and Marine Operations Center shall—

(i) manage the air and maritime domain awareness of the Department, as directed by the Secretary;

(ii) monitor and coordinate the airspace for unmanned aerial systems operations of Air and Marine Operations in U.S. Customs and Border Protection;

(iii) detect, identify, and coordinate a response to threats to national security in the air domain, in coordination with other appropriate agencies, as determined by the Executive Assistant Commissioner;

(iv) provide aviation and marine support to other Federal, State, tribal, and local agencies; and

(v) carry out other duties and powers prescribed by the Executive Assistant Commissioner.

(g) Office of Field Operations

(1) In general

There is established in U.S. Customs and Border Protection an Office of Field Operations.

(2) Executive Assistant Commissioner

There shall be at the head of the Office of Field Operations an Executive Assistant Commissioner, who shall report to the Commissioner.

(3) Duties

The Office of Field Operations shall coordinate the enforcement activities of U.S. Customs and Border Protection at United States air, land, and sea ports of entry to—

(A) deter and prevent terrorists and terrorist weapons from entering the United States at such ports of entry;

(B) conduct inspections at such ports of entry to safeguard the United States from terrorism and illegal entry of persons;

(C) prevent illicit drugs, agricultural pests, and contraband from entering the United States;

(D) in coordination with the Commissioner, facilitate and expedite the flow of legitimate travelers and trade;

(E) administer the National Targeting Center established under paragraph (4);

(F) coordinate with the Executive Assistant Commissioner for the Office of Trade with respect to the trade facilitation and trade enforcement activities of U.S. Customs and Border Protection; and

(G) carry out other duties and powers prescribed by the Commissioner.

(4) National Targeting Center

(A) In general

There is established in the Office of Field Operations a National Targeting Center.

(B) Executive Director

There shall be at the head of the National Targeting Center an Executive Director, who shall report to the Executive Assistant Commissioner of the Office of Field Operations.

(C) Duties

The National Targeting Center shall—

(i) serve as the primary forum for targeting operations within U.S. Customs and Border Protection to collect and analyze traveler and cargo information in advance of arrival in the United States to identify and address security risks and strengthen trade enforcement;

(ii) identify, review, and target travelers and cargo for examination;

(iii) coordinate the examination of entry and exit of travelers and cargo;

(iv) develop and conduct commercial risk assessment targeting with respect to cargo destined for the United States;

(v) coordinate with the Transportation Security Administration, as appropriate;

(vi) issue Trade Alerts pursuant to section 4318(b) of title 19; and

(vii) carry out other duties and powers prescribed by the Executive Assistant Commissioner.

(5) Annual report on staffing

(A) In general

Not later than 30 days after February 24, 2016, and annually thereafter, the Executive Assistant Commissioner shall submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate a report on the staffing model for the Office of Field Operations, including information on how many supervisors, front-line U.S. Customs and Border Protection officers, and support personnel are assigned to each Field Office and port of entry.

(B) Form

The report required under subparagraph (A) shall, to the greatest extent practicable, be submitted in unclassified form, but may be submitted in classified form, if the Executive Assistant Commissioner determines that such is appropriate and informs the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate of the reasoning for such.

(h) Office of Intelligence

(1) In general

There is established in U.S. Customs and Border Protection an Office of Intelligence.

(2) Assistant Commissioner

There shall be at the head of the Office of Intelligence an Assistant Commissioner, who shall report to the Commissioner.

(3) Duties

The Office of Intelligence shall—

(A) develop, provide, coordinate, and implement intelligence capabilities into a cohesive intelligence enterprise to support the execution of the duties and responsibilities of U.S. Customs and Border Protection;

(B) manage the counterintelligence operations of U.S. Customs and Border Protection;

(C) establish, in coordination with the Chief Intelligence Officer of the Department, as appropriate, intelligence-sharing relationships with Federal, State, local, and tribal agencies and intelligence agencies;

(D) conduct risk-based covert testing of U.S. Customs and Border Protection operations, including for nuclear and radiological risks; and

(E) carry out other duties and powers prescribed by the Commissioner.

(i) Office of International Affairs

(1) In general

There is established in U.S. Customs and Border Protection an Office of International Affairs.

(2) Assistant Commissioner

There shall be at the head of the Office of International Affairs an Assistant Commissioner, who shall report to the Commissioner.

(3) Duties

The Office of International Affairs, in collaboration with the Office of Policy of the Department, shall—

(A) coordinate and support U.S. Customs and Border Protection's foreign initiatives, policies, programs, and activities;

(B) coordinate and support U.S. Customs and Border Protection's personnel stationed abroad;

(C) maintain partnerships and information-sharing agreements and arrangements with foreign governments, international organizations, and United States agencies in support of U.S. Customs and Border Protection's duties and responsibilities;

(D) provide necessary capacity building, training, and assistance to foreign customs and border control agencies to strengthen border, global supply chain, and travel security, as appropriate;

(E) coordinate mission support services to sustain U.S. Customs and Border Protection's global activities;

(F) coordinate with customs authorities of foreign countries with respect to trade facilitation and trade enforcement;

(G) coordinate U.S. Customs and Border Protection's engagement in international negotiations;

(H) advise the Commissioner with respect to matters arising in the World Customs Organization and other international organizations as such matters relate to the policies and procedures of U.S. Customs and Border Protection;

(I) advise the Commissioner regarding international agreements to which the United States is a party as such agreements relate to the policies and regulations of U.S. Customs and Border Protection; and

(J) carry out other duties and powers prescribed by the Commissioner.

(j) Office of Professional Responsibility

(1) In general

There is established in U.S. Customs and Border Protection an Office of Professional Responsibility.

(2) Assistant Commissioner

There shall be at the head of the Office of Professional Responsibility an Assistant

Commissioner, who shall report to the Commissioner.

(3) Duties

The Office of Professional Responsibility shall—

(A) investigate criminal and administrative matters and misconduct by officers, agents, and other employees of U.S. Customs and Border Protection;

(B) manage integrity-related programs and policies of U.S. Customs and Border Protection;

(C) conduct research and analysis regarding misconduct of officers, agents, and other employees of U.S. Customs and Border Protection; and

(D) carry out other duties and powers prescribed by the Commissioner.

(k) Standard operating procedures

(1) In general

The Commissioner shall establish—

(A) standard operating procedures for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered by U.S. Customs and Border Protection personnel at United States ports of entry;

(B) standard use of force procedures that officers and agents of U.S. Customs and Border Protection may employ in the execution of their duties, including the use of deadly force;

(C) uniform, standardized, and publicly-available procedures for processing and investigating complaints against officers, agents, and employees of U.S. Customs and Border Protection for violations of professional conduct, including the timely disposition of complaints and a written notification to the complainant of the status or outcome, as appropriate, of the related investigation, in accordance with section 552a of title 5 (commonly referred to as the "Privacy Act" or the "Privacy Act of 1974");

(D) an internal, uniform reporting mechanism regarding incidents involving the use of deadly force by an officer or agent of U.S. Customs and Border Protection, including an evaluation of the degree to which the procedures required under subparagraph (B) were followed; and

(E) standard operating procedures, acting through the Executive Assistant Commissioner for Air and Marine Operations and in coordination with the Office for Civil Rights and Civil Liberties and the Office of Privacy of the Department, to provide command, control, communication, surveillance, and reconnaissance assistance through the use of unmanned aerial systems, including the establishment of—

(i) a process for other Federal, State, and local law enforcement agencies to submit mission requests;

(ii) a formal procedure to determine whether to approve or deny such a mission request;

(iii) a formal procedure to determine how such mission requests are prioritized and coordinated; and

(iv) a process regarding the protection and privacy of data and images collected by U.S. Customs and Border Protection through the use of unmanned aerial systems.

(2) Requirements regarding certain notifications

The standard operating procedures established pursuant to subparagraph (A) of paragraph (1) shall require—

(A) in the case of a search of information conducted on an electronic device by U.S. Customs and Border Protection personnel, the Commissioner to notify the individual subject to such search of the purpose and authority for such search, and how such individual may obtain information on reporting concerns about such search; and

(B) in the case of information collected by U.S. Customs and Border Protection through a search of an electronic device, if such information is transmitted to another Federal agency for subject matter assistance, translation, or decryption, the Commissioner to notify the individual subject to such search of such transmission.

(3) Exceptions

The Commissioner may withhold the notifications required under paragraphs (1)(C) and (2) if the Commissioner determines, in the sole and unreviewable discretion of the Commissioner, that such notifications would impair national security, law enforcement, or other operational interests.

(4) Update and review

The Commissioner shall review and update every three years the standard operating procedures required under this subsection.

(5) Audits

The Inspector General of the Department of Homeland Security shall develop and annually administer, during each of the three calendar years beginning in the calendar year that begins after February 24, 2016, an auditing mechanism to review whether searches of electronic devices at or between United States ports of entry are being conducted in conformity with the standard operating procedures required under subparagraph (A) of paragraph (1). Such audits shall be submitted to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and shall include the following:

(A) A description of the activities of officers and agents of U.S. Customs and Border Protection with respect to such searches.

(B) The number of such searches.

(C) The number of instances in which information contained in such devices that were subjected to such searches was retained, copied, shared, or entered in an electronic database.

(D) The number of such devices detained as the result of such searches.

(E) The number of instances in which information collected from such devices was subjected to such searches and was transmitted to another Federal agency, including whether such transmissions resulted in a prosecution or conviction.

(6) Requirements regarding other notifications

The standard use of force procedures established pursuant to subparagraph (B) of paragraph (1) shall require—

(A) in the case of an incident of the use of deadly force by U.S. Customs and Border Protection personnel, the Commissioner to notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Commissioner to provide to such committees a copy of the evaluation pursuant to subparagraph (D) of such paragraph not later than 30 days after completion of such evaluation.

(7) Report on unmanned aerial systems

The Commissioner shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report, for each of the three calendar years beginning in the calendar year that begins after February 24, 2016, that reviews whether the use of unmanned aerial systems is being conducted in conformity with the standard operating procedures required under subparagraph (E) of paragraph (1). Such reports—

(A) shall be submitted with the annual budget of the United States Government submitted by the President under section 1105 of title 31;

(B) may be submitted in classified form if the Commissioner determines that such is appropriate; and

(C) shall include—

(i) a detailed description of how, where, and for how long data and images collected through the use of unmanned aerial systems by U.S. Customs and Border Protection are collected and stored; and

(ii) a list of Federal, State, and local law enforcement agencies that submitted mission requests in the previous year and the disposition of such requests.

(l) Training

The Commissioner shall require all officers and agents of U.S. Customs and Border Protection to participate in a specified amount of continuing education (to be determined by the Commissioner) to maintain an understanding of Federal legal rulings, court decisions, and departmental policies, procedures, and guidelines.

(m) Short-term detention standards

(1) Access to food and water

The Commissioner shall make every effort to ensure that adequate access to food and water is provided to an individual apprehended and detained at a United States port of entry or between ports of entry as soon as practicable following the time of such apprehension or during subsequent short-term detention.

(2) Access to information on detainee rights at border patrol processing centers

(A) In general

The Commissioner shall ensure that an individual apprehended by a U.S. Border Patrol agent or an Office of Field Operations officer is provided with information concerning such individual's rights, including the right to contact a representative of such individual's government for purposes of United States treaty obligations.

(B) Form

The information referred to in subparagraph (A) may be provided either verbally or in writing, and shall be posted in the detention holding cell in which such individual is being held. The information shall be provided in a language understandable to such individual.

(3) Short-term detention defined

In this subsection, the term "short-term detention" means detention in a U.S. Customs and Border Protection processing center for 72 hours or less, before repatriation to a country of nationality or last habitual residence.

(4) Daytime repatriation

When practicable, repatriations shall be limited to daylight hours and avoid locations that are determined to have high indices of crime and violence.

(5) Report on procurement process and standards

Not later than 180 days after February 24, 2016, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the procurement process and standards of entities with which U.S. Customs and Border Protection has contracts for the transportation and detention of individuals apprehended by agents or officers of U.S. Customs and Border Protection. Such report should also consider the operational efficiency of contracting the transportation and detention of such individuals.

(6) Report on inspections of short-term custody facilities

The Commissioner shall—

(A) annually inspect all facilities utilized for short-term detention; and

(B) make publicly available information collected pursuant to such inspections, including information regarding the requirements under paragraphs (1) and (2) and, where appropriate, issue recommendations to improve the conditions of such facilities.

(n) Wait times transparency

(1) In general

The Commissioner shall—

(A) publish live wait times for travelers entering the United States at the 20 United States airports that support the highest volume of international travel (as determined by available

Federal flight data);

(B) make information about such wait times available to the public in real time through the U.S. Customs and Border Protection website;

(C) submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate, for each of the five calendar years beginning in the calendar year that begins after February 24, 2016, a report that includes compilations of all such wait times and a ranking of such United States airports by wait times; and

(D) provide adequate staffing at the U.S. Customs and Border Protection information center to ensure timely access for travelers attempting to submit comments or speak with a representative about their entry experiences.

(2) Calculation

The wait times referred to in paragraph (1)(A) shall be determined by calculating the time elapsed between an individual's entry into the U.S. Customs and Border Protection inspection area and such individual's clearance by a U.S. Customs and Border Protection officer.

(o) Other authorities

(1) In general

The Secretary may establish such other offices or positions of Assistant Commissioners (or other similar officers or officials) as the Secretary determines necessary to carry out the missions, duties, functions, and authorities of U.S. Customs and Border Protection.

(2) Notification

If the Secretary exercises the authority provided under paragraph (1), the Secretary shall notify the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate not later than 30 days before exercising such authority.

(3) Rescue beacons

Beginning in fiscal year 2019, in carrying out subsection (c)(8), the Commissioner shall purchase, deploy, and maintain not more than 250 self-powering, 9–1–1 cellular relay rescue beacons along the southern border of the United States at locations determined appropriate by the Commissioner to mitigate migrant deaths.

(p) Reports to Congress

The Commissioner shall, on and after February 24, 2016, continue to submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate any report required, on the day before February 24, 2016, to be submitted under any provision of law.

(q) Other Federal agencies

Nothing in this section may be construed as affecting in any manner the authority, existing on the day before February 24, 2016, of any other Federal agency or component of the Department.

(r) Definitions

In this section, the terms "commercial operations", "customs and trade laws of the United States", "trade enforcement", and "trade facilitation" have the meanings given such terms in section 4301 of title 19.

(Pub. L. 107–296, title IV, §411, Nov. 25, 2002, 116 Stat. 2178; Pub. L. 114–125, title VIII, §802(a), Feb. 24, 2016, 130 Stat. 199; Pub. L. 115–79, §4(a), Nov. 2, 2017, 131 Stat. 1260; Pub. L. 116–277, §3, Dec. 31, 2020, 134 Stat. 3370; Pub. L. 117–103, div. F, title II, §212, Mar. 15, 2022, 136 Stat. 322.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Security and Accountability for Every Port Act of 2006, referred to in subsec. (c)(14)(B), is Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1884, also known as the SAFE Port Act. Subtitle B of title II of the Act is classified generally to part B (§961 et seq.) of subchapter II of chapter 3 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 901 of this title and Tables.

CODIFICATION

Section is comprised of section 411 of Pub. L. 107–296. Former subsec. (b)(2) of section 411 of Pub. L. 107–296 amended section 5314 of Title 5, Government Organization and Employees.

AMENDMENTS

2022—Subsec. (o)(3). Pub. L. 117–103 substituted "250" for "170".

2020—Subsec. (o)(3). Pub. L. 116–277 added par. (3).

2017—Subsec. (c)(18), (19). Pub. L. 115–79 added par. (18) and redesignated former par. (18) as (19).

2016—Pub. L. 114–125 amended section generally. Prior to amendment, section established the United States Customs Service headed by a Commissioner of Customs.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Pub. L. 114–125, title VIII, §802(d)(2), Feb. 24, 2016, 130 Stat. 210, provided that: "On and after the date of the enactment of this Act [Feb. 24, 2016], any reference in law or regulations to the 'Commissioner of Customs' or the 'Commissioner of the Customs Service' shall be deemed to be a reference to the Commissioner of U.S. Customs and Border Protection."

EFFECTIVE DATE OF 2016 AMENDMENT; CONTINUITY OF FUNCTIONS, RULES, AND ACTIONS

Pub. L. 114–125, title VIII, §802(b), Feb. 24, 2016, 130 Stat. 209, provided that:

"(1) TREATMENT.—Section 411 of the Homeland Security Act of 2002 [6 U.S.C. 211], as amended by subsection (a) of this section, shall be treated as if included in such Act [Pub. L. 107–296] as of the date of the enactment of such Act [Nov. 25, 2002], and, in addition to the functions, missions, duties, and authorities specified in such amended section 411, U.S. Customs and Border Protection shall continue to perform and carry out the functions, missions, duties, and authorities under section 411 of such Act as in existence on the day before the date of the enactment of this Act [Feb. 24, 2016], and section 415 of the Homeland Security Act of 2002 [6 U.S.C. 215].

"(2) RULES OF CONSTRUCTION.—

"(A) RULES AND REGULATIONS.—Notwithstanding paragraph (1), nothing in this title [see Tables for classification] or any amendment made by this title may be construed as affecting in any manner any rule or regulation issued or promulgated pursuant to any provision of law, including section 411 of the Homeland Security Act of 2002 as in existence on the day before the date of the enactment of this Act [Feb. 24, 2016], and any such rule or regulation shall continue to have full force and effect on and after such date.

"(B) OTHER ACTIONS.—Notwithstanding paragraph (1), nothing in this Act [see Tables for classification] may be construed as affecting in any manner any action, determination, policy, or decision pursuant to section 411 of the Homeland Security Act of 2002 as in existence on the day before the date of the enactment of this Act, and any such action, determination, policy, or decision shall continue to have full force and effect on and after such date."

LARGE-SCALE NON-INTRUSIVE INSPECTION SCANNING

Pub. L. 116–299, Jan. 5, 2021, 134 Stat. 4906, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Securing America's Ports Act'.

"SEC. 2. LARGE-SCALE NON-INTRUSIVE INSPECTION SCANNING PLAN.

"(a) DEFINITIONS.—In this section:

"(1) LARGE-SCALE NON-INTRUSIVE INSPECTION SYSTEM.—The term 'large-scale, non-intrusive inspection system' means a technology, including x-ray, gamma-ray, and passive imaging systems, capable of producing an image of the contents of a commercial or passenger vehicle or freight rail car in 1 pass of such vehicle or car.

"(2) SCANNING.—The term 'scanning' means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a commercial or passenger vehicle or freight rail car.

"(b) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Jan. 5, 2021], the Secretary of Homeland Security shall submit a plan to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives for increasing to 100 percent the rate of high-throughput scanning of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border using large-scale non-intrusive inspection systems or similar technology to enhance border security.

"(c) BASELINE INFORMATION.—The plan under subsection (b) shall include, at a minimum, the following information regarding large-scale non-intrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at land ports of entry and rail-border crossings as of the date of the enactment of this Act:

"(1) An inventory of large-scale non-intrusive inspection systems or similar technology in use at each land port of entry.

"(2) For each system or technology identified in the inventory under paragraph (1)—

"(A) the scanning method of such system or technology;

"(B) the location of such system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of such areas;

"(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by such system or technology;

"(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic; and

"(E) the number of personnel required to operate each system or technology.

"(3) Information regarding the continued use of other technology and tactics used for scanning, such as canines and human intelligence in conjunction with large scale, nonintrusive inspection systems.

"(d) ELEMENTS.—The plan under subsection (b) shall include the following information:

"(1) Benchmarks for achieving incremental progress towards 100 percent high-throughput scanning within the next 6 years of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border with corresponding projected incremental improvements in scanning rates by fiscal year and rationales for the specified timeframes for each land port of entry.

"(2) Estimated costs, together with an acquisition plan, for achieving the 100 percent high-throughput scanning rate within the timeframes specified in paragraph (1), including acquisition, operations, and maintenance costs for large-scale, nonintrusive inspection systems or similar technology, and associated costs for any necessary infrastructure enhancements or configuration changes at each port of entry. Such acquisition plan shall promote, to the extent practicable, opportunities for entities that qualify as small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

"(3) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on the total number of commercial and passenger vehicles and freight rail traffic entering at land ports of entry and rail-border crossings where such systems are in use, and average wait times at peak and non-peak travel times, by lane type if applicable, as scanning rates are increased.

"(4) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings border security operations as a result of implementation actions, including any changes to the number of U.S. Customs and Border Protection officers or their duties and assignments.

"(e) ANNUAL REPORT.—Not later than 1 year after the submission of the plan under subsection (b), and biennially thereafter for the following 6 years, the Secretary of Homeland Security shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that describes the progress implementing the plan and includes—

"(1) an inventory of large-scale, nonintrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at each land port of entry;

"(2) for each system or technology identified in the inventory required under paragraph (1)—

"(A) the scanning method of such system or technology;

"(B) the location of such system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of such areas;

"(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by such system or technology; and

"(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic;

"(3) the total number of commercial and passenger vehicles and freight rail traffic entering at each land port of entry at which each system or technology is in use, and information on average wait times at peak and non-peak travel times, by lane type if applicable;

"(4) a description of the progress towards reaching the benchmarks referred to in subsection (d)(1), and an explanation if any of such benchmarks are not achieved as planned;

"(5) a comparison of actual costs (including information on any awards of associated contracts) to estimated costs set forth in subsection (d)(2);

"(6) any realized impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings operations as a result of implementation actions, including any changes to the number of U.S. Customs and Border Protection officers or their duties and assignments;

"(7) any proposed changes to the plan and an explanation for such changes, including changes made in response to any Department of Homeland Security research and development findings or changes in terrorist or transnational criminal organizations tactics, techniques, or procedures; and

"(8) any challenges to implementing the plan or meeting the benchmarks, and plans to mitigate any such challenges."

DHS OPIOID DETECTION RESILIENCE

Pub. L. 116–254, Dec. 23, 2020, 134 Stat. 1137, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'DHS Opioid Detection Resilience Act of 2019'.

"SEC. 2. STRATEGY TO ENSURE DETECTION OF ALL OPIOID PURITY LEVELS AT PORTS OF ENTRY.

"Not later than 180 days after the date of the enactment of this section [Dec. 23, 2020], the Commissioner of U.S. Customs and Border Protection (CBP) shall—

"(1) implement a strategy to ensure deployed chemical screening devices are able to identify in an operational environment narcotics at purity levels less than or equal to 10 percent, or provide ports of entry with an alternate method for identifying narcotics at lower purity levels; and

"(2) require testing of any new chemical screening devices to understand the abilities and limitations of such devices relating to identifying narcotics at various purity levels before CBP commits to the acquisition of such devices.

"SEC. 3. PLAN TO ENSURE OPIOID DETECTION EQUIPMENT RESILIENCY.

"Not later than 180 days after the date of the enactment of this section, the Secretary of Homeland Security shall implement a plan for the long-term development of a centralized spectral database for chemical screening devices. Such plan shall address the following:

"(1) How newly identified spectra will be collected, stored, and distributed to such devices in their operational environment, including at ports of entry.

"(2) Identification of parties responsible for updates and maintenance of such database."

PROTECTING AMERICA'S FOOD AND AGRICULTURE

Pub. L. 116–122, Mar. 3, 2020, 134 Stat. 143, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Protecting America's Food and Agriculture Act of 2019'.

"SEC. 2. FINDING.

"Congress finds that—

"(1) it is in the national security interest of the United States to ensure that the Nation's food supply is sufficiently protected; and

"(2) a vital part of such protection is the availability of adequate resources at the border to conduct inspections of incoming food and agricultural goods.

"SEC. 3. DEFINITIONS.

"In this Act:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(B) the Committee on Agriculture, Nutrition, and Forestry of the Senate;

"(C) the Committee on Homeland Security of the House of Representatives; and

"(D) the Committee on Agriculture of the House of Representatives.

"(2) CBP.—The term 'CBP' means U.S. Customs and Border Protection.

"SEC. 4. ADDITIONAL U.S. CUSTOMS AND BORDER PROTECTION PERSONNEL.

"(a) CBP AGRICULTURE SPECIALISTS.—The Commissioner of U.S. Customs and Border Protection may hire, train, and assign 240 new CBP Agriculture Specialists above the current attrition level during every fiscal year until the total number of CBP Agriculture Specialists equals and sustains the requirements identified each year in the Agriculture Resource Allocation Model.

"(b) MISSION AND OPERATIONAL SUPPORT STAFF.—

"(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection may hire, train, and assign support staff to support CBP Agriculture Specialists.

"(2) CBP AGRICULTURE TECHNICIANS.—The Commissioner of U.S. Customs and Border Protection may hire, train, and assign 200 new CBP Agriculture Technicians during each fiscal year until the total number of CBP Agriculture Technicians equals and sustains the requirements identified each year in the Mission and Operational Support Resource Allocation Model.

"(c) CBP AGRICULTURE CANINE TEAMS.—The Commissioner of U.S. Customs and Border Protection may hire, train, and assign 20 new CBP agriculture canine teams during each of the first 3 fiscal years beginning after the date of the enactment of this Act [Mar. 3, 2020].

"(d) TRAFFIC FORECASTS.—In calculating the number of CBP Agriculture Specialists needed at each port of entry through the Agriculture Resource Allocation Model, the Office of Field Operations shall—

"(1) rely on data collected regarding the inspections and other activities conducted at each such port of entry; and

"(2) consider volume from seasonal surges, other projected changes in commercial and passenger volumes, the most current commercial forecasts, and other relevant information.

"(e) AUTHORIZATION OF APPROPRIATIONS.—

"(1) CBP AGRICULTURE SPECIALISTS.—There is authorized to be appropriated to carry out subsection (a)—

"(A) $29,900,000 for fiscal year 2020;

"(B) $36,100,000 for fiscal year 2021; and

"(C) $40,500,000 for fiscal year 2022.

"(2) CBP AGRICULTURE TECHNICIANS.—There is authorized to be appropriated to carry out subsection (b)—

"(A) $11,000,000 for fiscal year 2020;

"(B) $25,000,000 for fiscal year 2021; and

"(C) $38,000,000 for fiscal year 2022.

"(3) CBP AGRICULTURE CANINE TEAMS.—There is authorized to be appropriated to carry out subsection (c)—

"(A) $3,500,000 for fiscal year 2020;

"(B) $7,400,000 for fiscal year 2021; and

"(C) $12,200,000 for fiscal year 2022.

"(4) TRAINING.—There is authorized to be appropriated for training costs associated with the new CBP personnel and canine teams hired pursuant to subsections (a), (b), and (c) $6,000,000 for each of the fiscal years 2020, 2021, and 2022.

"SEC. 5. GAO STUDY, BRIEFING, AND REPORT.

"(a) STUDY.—The Comptroller General of the United States, after consultation with the appropriate congressional committees, shall conduct a review of the efforts of the Department of Homeland Security, the Department of Agriculture, and other Federal agencies to address risks to the agricultural supply that analyzes—

"(1) interagency coordination and the distribution of responsibilities among Federal agencies with respect to the inspection of agricultural commodities entering the United States;

"(2) the effectiveness of such inspection responsibilities among Federal agencies; and

"(3) the training provided to, and working conditions of, CBP Agriculture Specialists.

"(b) BRIEFING.—Not later than 1 year after the date of the enactment of this Act [Mar. 3, 2020], the Comptroller General shall brief the appropriate congressional committees regarding the results of the study conducted pursuant to subsection (a).

"(c) REPORT.—Not later than 90 days after the briefing required under subsection (b), the Comptroller General shall complete the study required under subsection (a) and make the results of the study available to the public."

USE OF FUNDS TO CONTINUE DETENTION SERVICES CONTRACTS

Pub. L. 118–47, div. C, title II, §213, Mar. 23, 2024, 138 Stat. 603, provided that:

"(a) None of the funds provided under the heading 'U.S. Immigration and Customs Enforcement—Operations and Support' may be used to continue any contract for the provision of detention services if the two most recent overall performance evaluations received by the contracted facility are less than 'adequate' or the equivalent median score in any subsequent performance evaluation system.

"(b) The performance evaluations referenced in subsection (a) shall be conducted by the U.S. Immigration and Customs Enforcement Office of Professional Responsibility."

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 117–328, div. F, title II, §214, Dec. 29, 2022, 136 Stat. 4736.

Pub. L. 117–103, div. F, title II, §215, Mar. 15, 2022, 136 Stat. 322.

Pub. L. 116–260, div. F, title II, §215, Dec. 27, 2020, 134 Stat. 1457.

Pub. L. 116–93, div. D, title II, §215, Dec. 20, 2019, 133 Stat. 2513.

PORTS OF ENTRY THREAT AND OPERATIONAL REVIEW

Pub. L. 115–372, Dec. 21, 2018, 132 Stat. 5107, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'United States Ports of Entry Threat and Operational Review Act'.

"SEC. 2. PORTS OF ENTRY THREAT AND OPERATIONAL ANALYSIS.

"(a) IN GENERAL.—

"(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act [Dec. 21, 2018], the Secretary of Homeland Security, acting through the Commissioner of U.S. Customs and Border Protection, shall submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate a threat and operational analysis of ports of entry.

"(2) CONTENTS.—The threat and operational analysis required under paragraph (1) shall include an assessment of the following:

"(A) Current and potential threats posed by individuals and organized groups seeking—

"(i) to exploit security vulnerabilities at ports of entry; or

"(ii) to unlawfully enter the United States through such ports of entry.

"(B) Methods and pathways used to exploit security vulnerabilities at ports of entry.

"(C) Improvements needed at ports of entry to prevent the unlawful movement of people, illicit drugs, and other contraband across the borders of the United States.

"(D) Improvements needed to enhance travel and trade facilitation and reduce wait times at ports of entry, including—

"(i) security vulnerabilities associated with prolonged wait times;

"(ii) current technology at ports of entry that can be adapted to handle more volume, increase efficiency, and improve accuracy of detection efforts; and

"(iii) infrastructure additions and upgrades.

"(E) Processes conducted at ports of entry that do not require law enforcement training and could be—

"(i) filled with—

"(I) non-law enforcement staff; or

"(II) the private sector, for processes or activities determined to not be inherently governmental (as such term is defined in section 5 of the Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; [31 U.S.C. 501 note])); or

"(ii) automated.

"(3) ANALYSIS REQUIREMENTS.—In compiling the threat and operational analysis required under paragraph (1), the Secretary of Homeland Security, acting through the Commissioner of U.S. Customs and

Border Protection, shall consider and examine the following:

"(A) Personnel needs, including K–9 Units, and estimated costs, at each port of entry, including such needs and challenges associated with recruitment and hiring.

"(B) Technology needs, including radiation portal monitors and non-intrusive inspection technology, and estimated costs at each port of entry.

"(C) Infrastructure needs and estimated costs at each port of entry.

"(b) PORTS OF ENTRY STRATEGY AND IMPLEMENTATION PLAN.—

"(1) IN GENERAL.—Not later than 270 days after the submission of the threat and operational analysis required under subsection (a) and every 5 years thereafter for 10 years, the Secretary of Homeland Security, acting through the Commissioner of U.S. Customs and Border Protection (CBP), shall provide to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate a ports of entry strategy and implementation plan.

"(2) CONTENTS.—The ports of entry strategy and implementation plan required under paragraph (1) shall include a consideration of the following:

"(A) The ports of entry threat and operational analysis required under subsection (a), with an emphasis on efforts to mitigate threats and challenges identified in such analysis.

"(B) Efforts to reduce wait times at ports of entry and standards against which the effectiveness of such efforts may be determined.

"(C) Efforts to prevent the unlawful movement of people, illicit drugs, and other contraband across the borders of the United States at the earliest possible point at ports of entry and standards against which the effectiveness of such efforts may be determined.

"(D) Efforts to focus intelligence collection and information analysis to disrupt transnational criminal organizations attempting to exploit vulnerabilities at ports of entry and standards against which the effectiveness of such efforts may be determined.

"(E) Efforts to verify that any new port of entry technology acquisition can be operationally integrated with existing technologies in use by the Department of Homeland Security.

"(F) Lessons learned from reports on the business transformation initiative under section 802(i)(1) of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125).

"(G) CBP staffing requirements for all ports of entry.

"(H) Efforts to identify and detect fraudulent documents at ports of entry and standards against which the effectiveness of such efforts may be determined.

"(I) Efforts to prevent, detect, investigate, and mitigate corruption at ports of entry and standards against which the effectiveness of such efforts may be determined.

"(c) PORTS OF ENTRY DESCRIBED.—In this section, the term 'ports of entry' means United States air, land, and sea ports of entry."

REQUIRED NOTICE OF AIRCRAFT TRANSFERS

Pub. L. 115–141, div. F, title II, §203, Mar. 23, 2018, 132 Stat. 612, provided that: "Hereafter, no U.S. Customs and Border Protection aircraft or other related equipment, with the exception of aircraft that are one of a kind and have been identified as excess to U.S. Customs and Border Protection requirements and aircraft that have been damaged beyond repair, shall be transferred to any other Federal agency, department, or office outside of the Department of Homeland Security without prior notice to the Committees on Appropriations of the Senate and the House of Representatives."

DETECTING INCOMING CONTRABAND WITH TECHNOLOGY

Pub. L. 115–112, Jan. 10, 2018, 131 Stat. 2274, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'International Narcotics Trafficking Emergency Response by Detecting Incoming Contraband with Technology Act' or the 'INTERDICT Act'.

"SEC. 2. DEFINITIONS.

"In this Act:

"(1) CHEMICAL SCREENING DEVICE.—The term 'chemical screening device' means an immunoassay, narcotics field test kit, infrared spectrophotometer, mass spectrometer, nuclear magnetic resonance spectrometer, Raman spectrophotometer, or other scientific instrumentation able to collect data that can be interpreted to determine the presence of fentanyl, other synthetic opioids, and other narcotics and psychoactive substances.

"(2) COMMISSIONER.—The term 'Commissioner' means the Commissioner of U.S. Customs and Border Protection.

"(3) EXPRESS CONSIGNMENT OPERATOR OR CARRIER.—The term 'express consignment operator or carrier' has the meaning given that term in section 128.1 of title 19, Code of Federal Regulations (or any similar successor regulation).

"SEC. 3. INTERDICTION OF FENTANYL, OTHER SYNTHETIC OPIOIDS, AND OTHER NARCOTICS AND PSYCHOACTIVE SUBSTANCES.

"(a) CHEMICAL SCREENING DEVICES.—The Commissioner shall—

"(1) increase the number of chemical screening devices available to U.S. Customs and Border Protection officers over the number of such devices that are available on the date of the enactment of this Act [Jan. 10, 2018]; and

"(2) make such additional chemical screening devices available to U.S. Customs and Border Protection officers as the Commissioner determines are necessary to interdict fentanyl, other synthetic opioids, and other narcotics and psychoactive substances that are illegally imported into the United States, including such substances that are imported through the mail or by an express consignment operator or carrier.

"(b) PERSONNEL TO INTERPRET DATA.—The Commissioner shall dedicate the appropriate number of U.S. Customs and Border Protection personnel, including scientists, so that such personnel are available during all operational hours to interpret data collected by chemical screening devices.

"SEC. 4. AUTHORIZATION OF APPROPRIATIONS.

"There is authorized to be appropriated to the Commissioner $9,000,000 to ensure that U.S. Customs and Border Protection has resources, including chemical screening devices, personnel, and scientists, available during all operational hours to prevent, detect, and interdict the unlawful importation of fentanyl, other synthetic opioids, and other narcotics and psychoactive substances."

CONTINUATION IN OFFICE

Pub. L. 114–125, title VIII, §802(c), Feb. 24, 2016, 130 Stat. 210, provided that:

"(1) COMMISSIONER.—The individual serving as the Commissioner of Customs on the day before the date of the enactment of this Act [Feb. 24, 2016] may serve as the Commissioner of U.S. Customs and Border Protection on and after such date of enactment until a Commissioner of U.S. Customs and Border Protection is appointed under section 411 of the Homeland Security Act of 2002 [6 U.S.C. 211], as amended by subsection (a) of this section.

"(2) OTHER POSITIONS.—The individual serving as Deputy Commissioner, and the individuals serving as Assistant Commissioners and other officers and officials, under section 411 of the Homeland Security Act of 2002 on the day before the date of the enactment of this Act [Feb. 24, 2016] may serve as the Executive Assistant Commissioners, Deputy Commissioner, Assistant Commissioners, and other officers and officials, as appropriate, under such section 411 as amended by subsection (a) of this section unless the Commissioner of U.S. Customs and Border Protection determines that another individual should hold such position or positions."

BORDER JOBS FOR VETERANS

Pub. L. 114–68, Oct. 16, 2015, 129 Stat. 555, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Border Jobs for Veterans Act of 2015'.

"SEC. 2. FINDINGS.

"Congress finds the following:

"(1) Customs and Border Protection officers at United States ports of entry carry out critical law enforcement duties associated with screening foreign visitors, returning United States citizens, and imported cargo entering the United States.

"(2) It is in the national interest for United States ports of entry to be adequately staffed with Customs and Border Protection officers in a timely fashion, including meeting the congressionally funded staffing target of 23,775 officers for fiscal year 2015.

"(3) An estimated 250,000 to 300,000 members of the Armed Forces separate from military service every year.

"(4) Recruiting efforts and expedited hiring procedures must be enhanced to ensure that individuals separating from military service are aware of, and partake in, opportunities to fill vacant Customs and Border Protection officer positions.

"SEC. 3. EXPEDITED HIRING OF APPROPRIATE SEPARATING SERVICE MEMBERS.

"The Secretary of Homeland Security shall consider the expedited hiring of qualified candidates who have the ability to perform the essential functions of the position of a Customs and Border Protection officer and who are eligible for a veterans recruitment appointment authorized under section 4214 of title 38, United States Code.

"SEC. 4. ENHANCEMENTS TO EXISTING PROGRAMS TO RECRUIT SERVICE MEMBERS SEPARATING FROM MILITARY SERVICE FOR CUSTOMS AND BORDER PROTECTION OFFICER VACANCIES.

"(a) IN GENERAL.—The Secretary of Homeland Security, in consultation with the Secretary of Defense, and acting through existing programs, authorities, and agreements, where applicable, shall enhance the efforts of the Department of Homeland Security to recruit members of the Armed Forces who are separating from military service to serve as Customs and Border Protection officers.

"(b) ELEMENTS.—The enhanced recruiting efforts under subsection (a) shall—

"(1) include Customs and Border Protection officer opportunities in relevant job assistance efforts under the Transition Assistance Program;

"(2) place U.S. Customs and Border Protection officials or other relevant Department of Homeland Security officials at recruiting events and jobs fairs involving members of the Armed Forces who are separating from military service;

"(3) provide opportunities for local U.S. Customs and Border Protection field offices to partner with military bases in the region;

"(4) include outreach efforts to educate members of the Armed Forces with Military Occupational Specialty Codes and Officer Branches, Air Force Specialty Codes, Naval Enlisted Classifications and Officer Designators, and Coast Guard competencies that are transferable to the requirements, qualifications, and duties assigned to Customs and Border Protection officers of available hiring opportunities to become Customs and Border Protection officers;

"(5) identify shared activities and opportunities for reciprocity related to steps in hiring Customs and Border Protection officers with the goal of minimizing the time required to hire qualified applicants;

"(6) ensure the streamlined interagency transfer of relevant background investigations and security clearances; and

"(7) include such other elements as may be necessary to ensure that members of the Armed Forces who are separating from military service are aware of opportunities to fill vacant Customs and Border Protection officer positions.

"SEC. 5. REPORT TO CONGRESS.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Oct. 16, 2015], and by December 31 of each of the next 3 years thereafter, the Secretary of Homeland Security, in consultation with the Secretary of Defense, shall submit a report to the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate that includes a description and assessment of the efforts of the Department of Homeland Security to hire members of the Armed Forces who are separating from military service as Customs and Border Protection officers under section 4.

"(b) CONTENT.—The report required under subsection (a) shall include—

"(1) a detailed description of the efforts to implement section 4, including—

"(A) elements of the enhanced recruiting efforts and the goals associated with such elements; and

"(B) a description of how the elements and goals referred to in subparagraph (A) will assist in meeting statutorily mandated staffing levels and agency hiring benchmarks;

"(2) a detailed description of the efforts that have been undertaken under section 4;

"(3) the estimated number of separating service members made aware of Customs and Border Protection officer vacancies;

"(4) the number of Customs and Border Protection officer vacancies filled with separating service members; and

"(5) the number of Customs and Border Protection officer vacancies filled with separating service members under Veterans Recruitment Appointment authorized under section 4214 of title 38, United States Code.

"SEC. 6. RULES OF CONSTRUCTION.

"Nothing in this Act may be construed—

"(1) as superseding, altering, or amending existing Federal veterans' hiring preferences or Federal

hiring authorities; or

"(2) to authorize the appropriation of additional amounts to carry out this Act."

PORT OF ENTRY PARTNERSHIP PILOT PROGRAM

Pub. L. 113–76, div. F, title V, §559, Jan. 17, 2014, 128 Stat. 279, as amended by Pub. L. 114–4, title V, §552(a), Mar. 4, 2015, 129 Stat. 71; Pub. L. 114–113, div. F, title V, §550, Dec. 18, 2015, 129 Stat. 2519, which established a pilot program to permit U.S. Customs and Border Protection to enter into partnerships with private sector and government entities at ports of entry for certain services and to accept certain donations, was repealed by Pub. L. 114–279, §4(b), Dec. 16, 2016, 130 Stat. 1422.

REDUCING PASSENGER PROCESSING TIMES

Pub. L. 113–76, div. F, title V, §571, Jan. 17, 2014, 128 Stat. 287, provided that:

"(a) The Commissioner of U.S. Customs and Border Protection shall develop metrics that support a goal of reducing passenger processing times at air, land, and sea ports of entry, taking into consideration the capacity of an air or land port's physical infrastructure, airline arrival schedules, peak processing periods, and security requirements.

"(b) Not later than 240 days after the date of enactment of this Act [Jan. 17, 2014], the Commissioner of U.S. Customs and Border Protection shall develop and implement operational work plans to meet the goals of subsection (a) at United States air, land, and sea ports with the highest passenger volume and longest wait times. In developing such plans, the Commissioner of U.S. Customs and Border Protection shall consult with appropriate stakeholders, including, but not limited to, airlines and airport operators, port authorities, and importers."

§212. Retention of Customs revenue functions by Secretary of the Treasury

(a) Retention of Customs revenue functions by Secretary of the Treasury

(1) Retention of authority

Notwithstanding section 203(a)(1) [1] of this title, authority related to Customs revenue functions that was vested in the Secretary of the Treasury by law before the effective date of this chapter under those provisions of law set forth in paragraph (2) shall not be transferred to the Secretary by reason of this chapter, and on and after the effective date of this chapter, the Secretary of the Treasury may delegate any such authority to the Secretary at the discretion of the Secretary of the Treasury. The Secretary of the Treasury shall consult with the Secretary regarding the exercise of any such authority not delegated to the Secretary.

(2) Statutes

The provisions of law referred to in paragraph (1) are the following: the Tariff Act of 1930 [19 U.S.C. 1202 et seq.]; section 249 of the Revised Statutes of the United States (19 U.S.C. 3); section 2 of the Act of March 4, 1923 (19 U.S.C. 6); section 13031 of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c); section 251 of the Revised Statutes of the United States (19 U.S.C. 66); section 1 of the Act of June 26, 1930 (19 U.S.C. 68); the Foreign Trade Zones Act (19 U.S.C. 81a et seq.); section 1 of the Act of March 2, 1911 (19 U.S.C. 198); the Trade Act of 1974 [19 U.S.C. 2101 et seq.]; the Trade Agreements Act of 1979; the North American Free Trade Area Implementation Act; the Uruguay Round Agreements Act; the Caribbean Basin Economic Recovery Act [19 U.S.C. 2701 et seq.]; the Andean Trade Preference Act [19 U.S.C. 3201 et seq.]; the African Growth and Opportunity Act [19 U.S.C. 3701 et seq.]; and any other provision of law vesting customs revenue functions in the Secretary of the Treasury.

(b) Maintenance of Customs revenue functions

(1) Maintenance of functions

Notwithstanding any other provision of this chapter, the Secretary may not consolidate, discontinue, or diminish those functions described in paragraph (2) performed by U.S. Customs and Border Protection (as established under section 211 of this title) on or after the effective date of this chapter, reduce the staffing level, or reduce the resources attributable to such functions, and

the Secretary shall ensure that an appropriate management structure is implemented to carry out such functions.

(2) Functions

The functions referred to in paragraph (1) are those functions performed by the following personnel, and associated support staff, of U.S. Customs and Border Protection on the day before the effective date of this chapter: Import Specialists, Entry Specialists, Drawback Specialists, National Import Specialist, Fines and Penalties Specialists, attorneys of the Office of Regulations and Rulings, Customs Auditors, International Trade Specialists, Financial Systems Specialists.

(c) New personnel

The Secretary of the Treasury is authorized to appoint up to 20 new personnel to work with personnel of the Department in performing customs revenue functions.

(Pub. L. 107–296, title IV, §412, Nov. 25, 2002, 116 Stat. 2179; Pub. L. 114–125, title VIII, §802(g)(1)(B)(iii)(II), Feb. 24, 2016, 130 Stat. 211.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsecs. (a)(1) and (b), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

This chapter, referred to in subsecs. (a)(1) and (b)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The Tariff Act of 1930, referred to in subsec. (a)(2), is act June 17, 1930, ch. 497, 46 Stat. 590, which is classified generally to chapter 4 (§1202 et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see section 1654 of Title 19 and Tables.

The Foreign Trade Zones Act, referred to in subsec. (a)(2), is act June 18, 1934, ch. 590, 48 Stat. 998, which is classified generally to chapter 1A (§81a et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see Tables.

The Trade Act of 1974, referred to in subsec. (a)(2), is Pub. L. 93–618, Jan. 3, 1975, 88 Stat. 1978, which is classified principally to chapter 12 (§2101 et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see References in Text note set out under section 2101 of Title 19 and Tables.

The Trade Agreements Act of 1979, referred to in subsec. (a)(2), is Pub. L. 96–39, July 26, 1979, 93 Stat. 144. For complete classification of this Act to the Code, see References in Text note set out under section 2501 of Title 19, Customs Duties, and Tables.

The North American Free Trade Area Implementation Act, referred to in subsec. (a)(2), probably means the North American Free Trade Agreement Implementation Act, Pub. L. 103–182, Dec. 8, 1993, 107 Stat. 2057. For complete classification of this Act to the Code, see Short Title note under section 3301 of Title 19, Customs Duties, and Tables.

The Uruguay Round Agreements Act, referred to in subsec. (a)(2), is Pub. L. 103–465, Dec. 8, 1994, 108 Stat. 4809. For complete classification of this Act to the Code, see Short Title note set out under section 3501 of Title 19, Customs Duties, and Tables.

The Caribbean Basin Economic Recovery Act, referred to in subsec. (a)(2), is title II of Pub. L. 98–67, Aug. 5, 1983, 97 Stat. 384, which is classified principally to chapter 15 (§2701 et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see Short Title note set out under section 2701 of Title 19 and Tables.

The Andean Trade Preference Act, referred to in subsec. (a)(2), is title II of Pub. L. 102–182, Dec. 4, 1991, 105 Stat. 1236, which is classified generally to chapter 20 (§3201 et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see Short Title note set out under section 3201 of Title 19 and Tables.

The African Growth and Opportunity Act, referred to in subsec. (a)(2), is title I of Pub. L. 106–200, May 18, 2000, 114 Stat. 252, which is classified principally to chapter 23 (§3701 et seq.) of Title 19, Customs Duties. For complete classification of this Act to the Code, see Short Title note set out under section 3701 of Title 19 and Tables.

AMENDMENTS

2016—Subsec. (b). Pub. L. 114–125 substituted "U.S. Customs and Border Protection" for "the United States Customs Service" in pars. (1) and (2).

[1] *So in original. Probably should be section "203(1)".*

§213. Preservation of Customs funds

Notwithstanding any other provision of this chapter, no funds collected under paragraphs (1) through (8) of section 58c(a) of title 19 may be transferred for use by any other agency or office in the Department.

(Pub. L. 107–296, title IV, §413, Nov. 25, 2002, 116 Stat. 2180; Pub. L. 114–125, title VIII, §802(g)(1)(B)(iii)(III), Feb. 24, 2016, 130 Stat. 211.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2016—Pub. L. 114–125 struck out "available to the United States Customs Service or" after "no funds".

§214. Separate budget request for Customs

The President shall include in each budget transmitted to Congress under section 1105 of title 31 a separate budget request for U.S. Customs and Border Protection.

(Pub. L. 107–296, title IV, §414, Nov. 25, 2002, 116 Stat. 2180; Pub. L. 114–125, title VIII, §802(g)(1)(B)(iii)(IV), Feb. 24, 2016, 130 Stat. 211.)

EDITORIAL NOTES

AMENDMENTS

2016—Pub. L. 114–125 substituted "U.S. Customs and Border Protection" for "the United States Customs Service".

STATUTORY NOTES AND RELATED SUBSIDIARIES

LAND BORDER PROJECTS

Pub. L. 112–74, div. D, title II, Dec. 23, 2011, 125 Stat. 949, provided in part: "That for fiscal year 2012 and thereafter, the annual budget submission of U.S. Customs and Border Protection for 'Construction and Facilities Management' shall, in consultation with the General Services Administration, include a detailed 5-year plan for all Federal land border port of entry projects with a yearly update of total projected future funding needs delineated by land port of entry".

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 111–83, title II, Oct. 28, 2009, 123 Stat. 2148.

Pub. L. 110–329, div. D, title II, Sept. 30, 2008, 122 Stat. 3658.

§215. Definition

In this part, the term "customs revenue function" means the following:

(1) Assessing and collecting customs duties (including antidumping and countervailing duties and duties imposed under safeguard provisions), excise taxes, fees, and penalties due on imported merchandise, including classifying and valuing merchandise for purposes of such assessment.

(2) Processing and denial of entry of persons, baggage, cargo, and mail, with respect to the assessment and collection of import duties.

(3) Detecting and apprehending persons engaged in fraudulent practices designed to circumvent the customs laws of the United States.

(4) Enforcing section 1337 of title 19 and provisions relating to import quotas and the marking of imported merchandise, and providing Customs Recordations for copyrights, patents, and trademarks.

(5) Collecting accurate import data for compilation of international trade statistics.

(6) Enforcing reciprocal trade agreements.

(7) Functions performed by the following personnel, and associated support staff, of the United States Customs Service on the day before the effective date of this chapter, and of U.S. Customs and Border Protection on the day before the effective date of the U.S. Customs and Border Protection Authorization Act: Import Specialists, Entry Specialists, Drawback Specialists, National Import Specialist, Fines and Penalties Specialists, attorneys of the Office of Regulations and Rulings, Customs Auditors, International Trade Specialists, Financial Systems Specialists.

(8) Functions performed by the following offices, with respect to any function described in any of paragraphs (1) through (7), and associated support staff, of the United States Customs Service on the day before the effective date of this chapter, and of U.S. Customs and Border Protection on the day before the effective date of the U.S. Customs and Border Protection Authorization Act: the Office of Information and Technology, the Office of Laboratory Services, the Office of the Chief Counsel, the Office of Congressional Affairs, the Office of International Affairs, and the Office of Training and Development.

(Pub. L. 107–296, title IV, §415, Nov. 25, 2002, 116 Stat. 2180; Pub. L. 114–125, title VIII, §802(g)(1)(B)(iii)(V), Feb. 24, 2016, 130 Stat. 211.)

EDITORIAL NOTES

REFERENCES IN TEXT

This part, referred to in text, was in the original "this subtitle", meaning subtitle B (§§411–419) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2178, which enacted this part, amended section 5314 of Title 5, Government Organization and Employees, section 58c of Title 19, Customs Duties, and provisions set out as a note under section 2075 of Title 19. For complete classification of subtitle B to the Code, see Tables.

The effective date of this chapter, referred to in pars. (7) and (8), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

The effective date of the U.S. Customs and Border Protection Authorization Act, referred to in pars. (7) and (8), is the effective date of title VIII of Pub. L. 114–125, which is Feb. 24, 2016.

AMENDMENTS

2016—Pars. (7), (8). Pub. L. 114–125 inserted ", and of U.S. Customs and Border Protection on the day before the effective date of the U.S. Customs and Border Protection Authorization Act" before the colon.

§216. Protection against potential synthetic opioid exposure

(a) In general

The Commissioner of U.S. Customs and Border Protection shall issue a policy that specifies effective protocols and procedures for the safe handling of potential synthetic opioids, including fentanyl, by U.S. Customs and Border Protection officers, agents, other personnel, and canines, and to reduce the risk of injury or death resulting from accidental exposure and enhance post-exposure management.

(b) Training

(1) In general

Together with the issuance of the policy described in subsection (a), the Commissioner of U.S. Customs and Border Protection shall require mandatory and recurrent training on the following:

(A) The potential risk of opioid exposure and safe handling procedures for potential synthetic opioids, including precautionary measures such as the use of personal protective equipment during such handling.

(B) How to access and administer opioid receptor antagonists, including naloxone, post-exposure to potential synthetic opioids.

(C) How to use containment devices to prevent potential synthetic opioid exposure.

(2) Integration

The training described in paragraph (1) may be integrated into existing training under section 211(l) of this title for U.S. Customs and Border Protection officers, agents, and other personnel.

(c) Personal protective equipment, containment devices, and opioid receptor antagonists

Together with the issuance of the policy described in subsection (a), the Commissioner of U.S. Customs and Border Protection shall ensure the availability of personal protective equipment, opioid receptor antagonists, including naloxone, and containment devices, to all U.S. Customs and Border Protection officers, agents, other personnel, and canines at risk of accidental exposure to synthetic opioids.

(d) Oversight

To ensure effectiveness of the policy described in subsection (a)—

(1) the Commissioner of U.S. Customs and Border Protection shall regularly monitor the efficacy of the implementation of such policy and adjust protocols and procedures, as necessary; and

(2) the Inspector General of the Department shall audit compliance with the requirements of this section not less than once during the 3-year period after December 27, 2020.

(Pub. L. 107–296, title IV, §416, as added Pub. L. 116–260, div. U, title III, §302(a), Dec. 27, 2020, 134 Stat. 2291; amended Pub. L. 117–263, div. G, title LXXI, §7135(a), (b), Dec. 23, 2022, 136 Stat. 3650.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 216 of this title, Pub. L. 107–296, title IV, §416, Nov. 25, 2002, 116 Stat. 2181, related to GAO report to Congress, prior to repeal by Pub. L. 114–125, title VIII, §802(f), Feb. 24, 2016, 130 Stat. 210.

AMENDMENTS

2022—Subsec. (b)(1)(C). Pub. L. 117–263, §7135(a), added subpar. (C).

Subsec. (c). Pub. L. 117–263, §7135(b), inserted ", containment devices," after "equipment" in heading and substituted ", opioid receptor antagonists, including naloxone, and containment devices" for "and opioid receptor antagonists, including naloxone" in text.

STATUTORY NOTES AND RELATED SUBSIDIARIES

APPLICABILITY TO OTHER COMPONENTS

Pub. L. 117–263, div. G, title LXXI, §7135(c), Dec. 23, 2022, 136 Stat. 3650, provided that: "If the Secretary of Homeland Secretary determines that officers, agents, other personnel, or canines of a component of the Department of Homeland Security other than U.S. Customs and Border Protection are at risk of potential synthetic opioid exposure in the course of their duties, the head of such component shall carry out the responsibilities under section 416 of the Homeland Security Act of 2002 (6 U.S.C. 216) in the same manner and to the same degree as the Commissioner of U.S. Customs and Border Protection carries out such responsibilities."

§217. Allocation of resources by the Secretary

(a) In general

The Secretary shall ensure that adequate staffing is provided to assure that levels of customs revenue services provided on the day before the effective date of this chapter shall continue to be provided.

(b) Notification of Congress

The Secretary shall notify the Committee on Ways and Means of the House of Representatives and the Committee on Finance of the Senate at least 90 days prior to taking any action which would—

(1) result in any significant reduction in customs revenue services, including hours of operation, provided at any office within the Department or any port of entry;

(2) eliminate or relocate any office of the Department which provides customs revenue services; or

(3) eliminate any port of entry.

(c) Definition

In this section, the term "customs revenue services" means those customs revenue functions described in paragraphs (1) through (6) and paragraph (8) of section 215 of this title.

(Pub. L. 107–296, title IV, §417, Nov. 25, 2002, 116 Stat. 2181.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsec. (a), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

§218. Asia-Pacific Economic Cooperation Business Travel Cards

(a) In general

The Commissioner of U.S. Customs and Border Protection is authorized to issue an Asia-Pacific Economic Cooperation Business Travel Card (referred to in this section as an "ABT Card") to any individual described in subsection (b).

(b) Card issuance

An individual described in this subsection is an individual who—

(1) is a citizen of the United States;

(2) has been approved and is in good standing in an existing international trusted traveler program of the Department; and

(3) is—

(A) engaged in business in the Asia-Pacific region, as determined by the Commissioner of U.S. Customs and Border Protection; or

(B) a United States Government official actively engaged in Asia-Pacific Economic Cooperation business, as determined by the Commissioner of U.S. Customs and Border Protection.

(c) Integration with existing travel programs

The Commissioner of U.S. Customs and Border Protection shall integrate application procedures for, and issuance, renewal, and revocation of, ABT Cards with existing international trusted traveler programs of the Department.

(d) Cooperation with private entities and nongovernmental organizations

In carrying out this section, the Commissioner of U.S. Customs and Border Protection may consult with appropriate private sector entities and nongovernmental organizations, including academic institutions.

(e) Fee

(1) In general

The Commissioner of U.S. Customs and Border Protection shall—

(A) prescribe and collect a fee for the issuance and renewal of ABT Cards; and

(B) adjust such fee to the extent the Commissioner determines necessary to comply with paragraph (2).

(2) Limitation

The Commissioner of U.S. Customs and Border Protection shall ensure that the total amount of the fees collected under paragraph (1) during any fiscal year is sufficient to offset the direct and indirect costs associated with carrying out this section during such fiscal year, including the costs associated with operating and maintaining the ABT Card issuance and renewal processes.

(3) Account for collections

There is established in the Treasury of the United States an "Asia-Pacific Economic Cooperation Business Travel Card Account" into which the fees collected under paragraph (1) shall be deposited as offsetting receipts.

(4) Use of funds

Amounts deposited into the Asia Pacific [1] Economic Cooperation Business Travel Card Account established under paragraph (3) shall—

(A) be credited to the appropriate account of the [2] U.S. Customs and Border Protection for expenses incurred in carrying out this section; and

(B) remain available until expended.

(f) Notification

The Commissioner of U.S. Customs and Border Protection shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 60 days after the expenditures of funds to operate and provide ABT Card services beyond the amounts collected under subsection (e)(1).

(g) Trusted traveler program defined

In this section, the term "trusted traveler program" means a voluntary program of the Department that allows U.S. Customs and Border Protection to expedite clearance of pre-approved, low-risk travelers arriving in the United States.

(Pub. L. 107–296, title IV, §418, as added Pub. L. 115–79, §2(a), Nov. 2, 2017, 131 Stat. 1258.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 218, Pub. L. 107–296, title IV, §418, Nov. 25, 2002, 116 Stat. 2181, related to reports to Congress from the United States Customs Service and the Secretary of the Treasury, prior to repeal by Pub. L. 114–125, title VIII, §802(f), Feb. 24, 2016, 130 Stat. 210.

STATUTORY NOTES AND RELATED SUBSIDIARIES

TRANSFER OF FUNDS FROM APEC BUSINESS TRAVEL CARD ACCOUNT

Pub. L. 115–79, §3, Nov. 2, 2017, 131 Stat. 1259, provided that:

"(a) *In General*.—Notwithstanding the repeal of the Asia-Pacific Economic Cooperation Business Travel Cards Act of 2011 (Public Law 112–54; 8 U.S.C. 1185 note) pursuant to section 4(b)(1), amounts deposited

into the APEC Business Travel Card Account established pursuant to such Act as of the date of the enactment of this Act [Nov. 2, 2017] are hereby transferred to the Asia-Pacific Economic Cooperation Business Travel Card Account established pursuant to section 418(e) of the Homeland Security Act of 2002 [6 U.S.C. 218(e)] (as added by section 2(a) of this Act), and shall be available without regard to whether such amounts are expended in connection with expenses incurred with respect to an ABT Card issued at any time before or after such date of enactment.

"(b) *Availability*.—Amounts deposited in the Asia-Pacific Economic Cooperation Business Travel Card Account established pursuant to section 418(e) of the Homeland Security Act of 2002, in addition to the purposes for which such amounts are available pursuant to such subsection, shall also be available for expenditure in connection with expenses incurred with respect to ABT Cards issued at any time before the date of the enactment of such section.

"(c) *Termination*.—After the completion of the transfer described in subsection (a), the Asia-Pacific Economic Cooperation Business Travel Card Account established pursuant to the Asia-Pacific Economic Cooperation Business Travel Cards Act of 2011 shall be closed."

[1] So in original. Probably should be "Asia-Pacific".

[2] So in original. The word "the" probably should not appear.

§220. Methamphetamine and methamphetamine precursor chemicals

(a) Compliance with performance plan requirements

As part of the annual performance plan required in the budget submission of the United States Customs and Border Protection under section 1115 of title 31, the Commissioner shall establish performance indicators relating to the seizure of methamphetamine and methamphetamine precursor chemicals in order to evaluate the performance goals of the United States Customs and Border Protection with respect to the interdiction of illegal drugs entering the United States.

(b) Study and report relating to methamphetamine and methamphetamine precursor chemicals

(1) Analysis

The Commissioner shall, on an ongoing basis, analyze the movement of methamphetamine and methamphetamine precursor chemicals into the United States. In conducting the analysis, the Commissioner shall—

(A) consider the entry of methamphetamine and methamphetamine precursor chemicals through ports of entry, between ports of entry, through international mails, and through international courier services;

(B) examine the export procedures of each foreign country where the shipments of methamphetamine and methamphetamine precursor chemicals originate and determine if changes in the country's customs over time provisions would alleviate the export of methamphetamine and methamphetamine precursor chemicals; and

(C) identify emerging trends in smuggling techniques and strategies.

(2) Report

Not later than September 30, 2007, and each 2-year period thereafter, the Commissioner, in the consultation with the Attorney General, United States Immigration and Customs Enforcement, the United States Drug Enforcement Administration, and the United States Department of State, shall submit a report to the Committee on Finance of the Senate, the Committee on Foreign Relations of the Senate, the Committee on the Judiciary of the Senate, the Committee on Ways and Means of the House of Representatives, the Committee on International Relations of the House of Representatives, and the Committee on the Judiciary of the House of Representatives, that includes—

(A) a comprehensive summary of the analysis described in paragraph (1); and

(B) a description of how the Untied [1] States Customs and Border Protection utilized the analysis described in paragraph (1) to target shipments presenting a high risk for smuggling or circumvention of the Combat Methamphetamine Epidemic Act of 2005 (Public Law 109–177).

(3) Availability of analysis

The Commissioner shall ensure that the analysis described in paragraph (1) is made available in a timely manner to the Secretary of State to facilitate the Secretary in fulfilling the Secretary's reporting requirements in section 722 of the Combat Methamphetamine Epidemic Act of 2005.

(c) Definition

In this section, the term "methamphetamine precursor chemicals" means the chemicals ephedrine, pseudoephedrine, or phenylpropanolamine, including each of the salts, optical isomers, and salts of optical isomers of such chemicals.

(Pub. L. 109–347, title VII, §707, Oct. 13, 2006, 120 Stat. 1946.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Combat Methamphetamine Epidemic Act of 2005, referred to in subsec. (b)(2)(B), is Pub. L. 109–177, title VII, Mar. 9, 2006, 120 Stat. 256. Section 722 of the Act amended sections 2291h, 2291j, and 2291j–1 of Title 22, Foreign Relations and Intercourse, and enacted provisions set out as a note under section 2291h of Title 22. For complete classification of this Act to the Code, see Short Title note set out under section 801 of Title 21, Food and Drugs, and Tables.

CODIFICATION

Section was enacted as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on International Relations of House of Representatives changed to Committee on Foreign Affairs of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

DEFINITIONS

For definition of "Commissioner" as used in this section, see section 901 of this title.

[1] *So in original.*

§221. Requirements with respect to administering polygraph examinations to law enforcement personnel of U.S. Customs and Border Protection

(a) In general

The Secretary of Homeland Security shall ensure that—

(1) by not later than 2 years after January 4, 2011, all applicants for law enforcement positions with U.S. Customs and Border Protection (except as provided in subsection (b)) receive polygraph examinations before being hired for such a position; and

(2) by not later than 180 days after January 4, 2011, U.S. Customs and Border Protection initiates all periodic background reinvestigations for all law enforcement personnel of U.S. Customs and Border Protection that should receive periodic background reinvestigations pursuant to relevant policies of U.S. Customs and Border Protection in effect on the day before January 4, 2011.

(b) Waiver

The Commissioner of U.S. Customs and Border Protection may waive the polygraph examination requirement under subsection (a)(1) for any applicant who—

(1) is deemed suitable for employment;

(2) holds a current, active Top Secret/Sensitive Compartmented Information Clearance;

(3) has a current Single Scope Background Investigation;

(4) was not granted any waivers to obtain his or her clearance; and

(5) is a veteran (as defined in section 2108 of title 5).

(Pub. L. 111–376, §3, Jan. 4, 2011, 124 Stat. 4104; Pub. L. 114–279, §5, Dec. 16, 2016, 130 Stat. 1422.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Anti-Border Corruption Act of 2010, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2016—Pub. L. 114–279 designated existing provisions as subsec. (a), inserted heading, in par. (1) inserted "(except as provided in subsection (b))" after "Border Protection", and added subsec. (b).

STATUTORY NOTES AND RELATED SUBSIDIARIES

WAIVER OF CERTAIN POLYGRAPH EXAMINATION REQUIREMENTS

Pub. L. 114–328, div. A, title X, §1049, Dec. 23, 2016, 130 Stat. 2396, provided that: "The Secretary of Homeland Security, acting through the Commissioner of U.S. Customs and Border Protection, may waive the polygraph examination requirement under section 3 of the Anti-Border Corruption Act of 2010 (Public Law 111–376) [6 U.S.C. 221] for any applicant who—

"(1) the Commissioner determines is suitable for employment;

"(2) holds a current, active Top Secret clearance and is able to access sensitive compartmented information;

"(3) has a current single scope background investigation;

"(4) was not granted any waivers to obtain the clearance; and

"(5) is a veteran (as such term is defined in section 2108 or 2109a [probably should be "2108a"] of title 5, United States Code)."

FINDINGS

Pub. L. 111–376, §2, Jan. 4, 2011, 124 Stat. 4104, provided that: "Congress makes the following findings:

"(1) According to the Office of the Inspector General of the Department of Homeland Security, since 2003, 129 U.S. Customs and Border Protection officials have been arrested on corruption charges and, during 2009, 576 investigations were opened on allegations of improper conduct by U.S. Customs and Border Protection officials.

"(2) To foster integrity in the workplace, established policy of U.S. Customs and Border Protection calls for—

"(A) all job applicants for law enforcement positions at U.S. Customs and Border Protection to receive a polygraph examination and a background investigation before being offered employment; and

"(B) relevant employees to receive a periodic background reinvestigation every 5 years.

"(3) According to the Office of Internal Affairs of U.S. Customs and Border Protection—

"(A) in 2009, less than 15 percent of applicants for jobs with U.S. Customs and Border Protection received polygraph examinations;

"(B) as of March 2010, U.S. Customs and Border Protection had a backlog of approximately 10,000 periodic background reinvestigations of existing employees; and

"(C) without additional resources, by the end of fiscal year 2010, the backlog of periodic background reinvestigations will increase to approximately 19,000."

§222. Advanced Training Center Revolving Fund

For fiscal year 2012 and thereafter, U.S. Customs and Border Protection's Advanced Training Center is authorized to charge fees for any service and/or thing of value it provides to Federal Government or non-government entities or individuals, so long as the fees charged do not exceed the full costs associated with the service or thing of value provided: *Provided*, That notwithstanding section 3302(b) of title 31, fees collected by the Advanced Training Center are to be deposited into a separate account entitled "Advanced Training Center Revolving Fund", and be available, without further appropriations, for necessary expenses of the Advanced Training Center program, and are to remain available until expended.

(Pub. L. 112–74, div. D, title V, §557, Dec. 23, 2011, 125 Stat. 979.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2012, and also as part of the Consolidated Appropriations Act, 2012, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§223. Border security metrics

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(2) Consequence Delivery System

The term "Consequence Delivery System" means the series of consequences applied by U.S. Border Patrol in collaboration with other Federal agencies to persons unlawfully entering the United States, in order to prevent unlawful border crossing recidivism.

(3) Got away

The term "got away" means an unlawful border crosser who—

(A) is directly or indirectly observed making an unlawful entry into the United States;

(B) is not apprehended; and

(C) is not a turn back.

(4) Known maritime migrant flow

The term "known maritime migrant flow" means the sum of the number of undocumented migrants—

(A) interdicted in the waters over which the United States has jurisdiction;

(B) identified at sea either directly or indirectly, but not interdicted;

(C) if not described in subparagraph (A) or (B), who were otherwise reported, with a significant degree of certainty, as having entered, or attempted to enter, the United States through the maritime border.

(5) Major violator

The term "major violator" means a person or entity that has engaged in serious criminal activities at any land, air, or sea port of entry, including the following:

(A) Possession of illicit drugs.

(B) Smuggling of prohibited products.

(C) Human smuggling.

(D) Possession of illegal weapons.

(E) Use of fraudulent documents.

(F) Any other offense that is serious enough to result in an arrest.

(6) Secretary

The term "the Secretary" means the Secretary of Homeland Security.

(7) Situational awareness

The term "situational awareness" means knowledge and understanding of current unlawful cross-border activity, including the following:

(A) Threats and trends concerning illicit trafficking and unlawful crossings.

(B) The ability to forecast future shifts in such threats and trends.

(C) The ability to evaluate such threats and trends at a level sufficient to create actionable plans.

(D) The operational capability to conduct persistent and integrated surveillance of the international borders of the United States.

(8) Transit zone

The term "transit zone" means the sea corridors of the western Atlantic Ocean, the Gulf of Mexico, the Caribbean Sea, and the eastern Pacific Ocean through which undocumented migrants and illicit drugs transit, either directly or indirectly, to the United States.

(9) Turn back

The term "turn back" means an unlawful border crosser who, after making an unlawful entry into the United States, responds to United States enforcement efforts by returning promptly to the country from which such crosser entered.

(10) Unlawful border crossing effectiveness rate

The term "unlawful border crossing effectiveness rate" means the percentage that results from dividing the number of apprehensions and turn backs by the sum of the number of apprehensions, estimated undetected unlawful entries, turn backs, and got aways.

(11) Unlawful entry

The term "unlawful entry" means an unlawful border crosser who enters the United States and is not apprehended by a border security component of the Department of Homeland Security.

(b) Metrics for securing the border between ports of entry

(1) In general

Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security between ports of entry. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Estimates, using alternative methodologies where appropriate, including recidivism data, survey data, known-flow data, and technologically-measured data, of the following:

(i) The rate of apprehension of attempted unlawful border crossers.

(ii) The number of detected unlawful entries.

(iii) The number of estimated undetected unlawful entries.

(iv) Turn backs.

(v) Got aways.

(B) A measurement of situational awareness achieved in each U.S. Border Patrol sector.

(C) An unlawful border crossing effectiveness rate in each U.S. Border Patrol sector.

(D) A probability of detection rate, which compares the estimated total unlawful border crossing attempts not detected by U.S. Border Patrol to the unlawful border crossing effectiveness rate under subparagraph (C), as informed by subparagraph (A).

(E) The number of apprehensions in each U.S. Border Patrol sector.

(F) The number of apprehensions of unaccompanied alien children, and the nationality of

such children, in each U.S. Border Patrol sector.

(G) The number of apprehensions of family units, and the nationality of such family units, in each U.S. Border Patrol sector.

(H) An illicit drugs seizure rate for drugs seized by U.S. Border Patrol between ports of entry, which compares the ratio of the amount and type of illicit drugs seized between ports of entry in any fiscal year to the average of the amount and type of illicit drugs seized between ports of entry in the immediately preceding five fiscal years.

(I) Estimates of the impact of the Consequence Delivery System on the rate of recidivism of unlawful border crossers over multiple fiscal years.

(J) An examination of each consequence under the Consequence Delivery System referred to in subparagraph (I), including the following:

(i) Voluntary return.

(ii) Warrant of arrest or notice to appear.

(iii) Expedited removal.

(iv) Reinstatement of removal.

(v) Alien transfer exit program.

(vi) Criminal consequence program.

(vii) Standard prosecution.

(viii) Operation Against Smugglers Initiative on Safety and Security.

(2) Metrics consultation

To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department of Homeland Security; and

(B) where appropriate, with the heads of other agencies, including the Office of Refugee Resettlement of the Department of Health and Human Services and the Executive Office for Immigration Review of the Department of Justice.

(3) Manner of collection

The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner across all U.S. Border Patrol sectors, informed by situational awareness.

(c) Metrics for securing the border at ports of entry

(1) In general

Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security at ports of entry. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Estimates, using alternative methodologies where appropriate, including recidivism data, survey data, and randomized secondary screening data, of the following:

(i) Total inadmissible travelers who attempt to, or successfully, enter the United States at a port of entry.

(ii) The rate of refusals and interdictions for travelers who attempt to, or successfully, enter the United States at a port of entry.

(iii) The number of unlawful entries at a port of entry.

(B) The amount and type of illicit drugs seized by the Office of Field Operations of U.S. Customs and Border Protection at ports of entry during the previous fiscal year.

(C) An illicit drugs seizure rate for drugs seized by the Office of Field Operations, which compares the ratio of the amount and type of illicit drugs seized by the Office of Field Operations in any fiscal year to the average of the amount and type of illicit drugs seized by the Office of Field Operations in the immediately preceding five fiscal years.

(D) The number of infractions related to travelers and cargo committed by major violators who are interdicted by the Office of Field Operations at ports of entry, and the estimated number of such infractions committed by major violators who are not so interdicted.

(E) In consultation with the heads of the Office of National Drug Control Policy and the United States Southern Command, a cocaine seizure effectiveness rate, which is the percentage resulting from dividing the amount of cocaine seized by the Office of Field Operations by the total estimated cocaine flow rate at ports of entry along the United States land border with Mexico and Canada.

(F) A measurement of how border security operations affect crossing times, including the following:

(i) A wait time ratio that compares the average wait times to total commercial and private vehicular traffic volumes at each land port of entry.

(ii) An infrastructure capacity utilization rate that measures traffic volume against the physical and staffing capacity at each land port of entry.

(iii) A secondary examination rate that measures the frequency of secondary examinations at each land port of entry.

(iv) An enforcement rate that measures the effectiveness of such secondary examinations at detecting major violators.

(G) A seaport scanning rate that includes the following:

(i) The number of all cargo containers that are considered potentially "high-risk", as determined by the Executive Assistant Commissioner of the Office of Field Operations.

(ii) A comparison of the number of potentially high-risk cargo containers scanned by the Office of Field Operations at each sea port of entry during a fiscal year to the total number of high-risk cargo containers entering the United States at each such sea port of entry during the previous fiscal year.

(iii) The number of potentially high-risk cargo containers scanned upon arrival at a United States sea port of entry.

(iv) The number of potentially high-risk cargo containers scanned before arrival at a United States sea port of entry.

(2) Metrics consultation

To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department of Homeland Security; and

(B) where appropriate, work with heads of other appropriate agencies, including the Office of Refugee Resettlement of the Department of Health and Human Services and the Executive Office for Immigration Review of the Department of Justice.

(3) Manner of collection

The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner across all United States ports of entry, informed by situational awareness.

(d) Metrics for securing the maritime border

(1) In general

Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security in the maritime environment. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Situational awareness achieved in the maritime environment.

(B) A known maritime migrant flow rate.

(C) An illicit drugs removal rate for drugs removed inside and outside of a transit zone,

which compares the amount and type of illicit drugs removed, including drugs abandoned at sea, by the maritime security components of the Department of Homeland Security in any fiscal year to the average of the amount and type of illicit drugs removed by such maritime components for the immediately preceding five fiscal years.

(D) In consultation with the heads of the Office of National Drug Control Policy and the United States Southern Command, a cocaine removal effectiveness rate for cocaine removed inside a transit zone and outside a transit zone, which compares the amount of cocaine removed by the maritime security components of the Department of Homeland Security by the total documented cocaine flow rate, as contained in Federal drug databases.

(E) A response rate, which compares the ability of the maritime security components of the Department of Homeland Security to respond to and resolve known maritime threats, whether inside or outside a transit zone, by placing assets on-scene, to the total number of events with respect to which the Department has known threat information.

(F) An intergovernmental response rate, which compares the ability of the maritime security components of the Department of Homeland Security or other United States Government entities to respond to and resolve actionable maritime threats, whether inside or outside a transit zone, with the number of such threats detected.

(2) Metrics consultation

To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department of Homeland Security; and

(B) where appropriate, work with the heads of other agencies, including the Drug Enforcement Agency, the Department of Defense, and the Department of Justice.

(3) Manner of collection

The data used by the Secretary shall be collected and reported in a consistent and standardized manner by the maritime security components of the Department of Homeland Security, informed by situational awareness.

(e) Air and Marine security metrics in the land domain

(1) In general

Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of the aviation assets and operations of Air and Marine Operations of U.S. Customs and Border Protection. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) A flight hour effectiveness rate, which compares Air and Marine Operations flight hours requirements to the number of flight hours flown by Air and Marine Operations.

(B) A funded flight hour effectiveness rate, which compares the number of funded flight hours appropriated to Air and Marine Operations to the number of actual flight hours flown by Air and Marine Operations.

(C) A readiness rate, which compares the number of aviation missions flown by Air and Marine Operations to the number of aviation missions cancelled by Air and Marine Operations due to maintenance, operations, or other causes.

(D) The number of missions cancelled by Air and Marine Operations due to weather compared to the total planned missions.

(E) The number of individuals detected by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(F) The number of apprehensions assisted by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(G) The number and quantity of illicit drug seizures assisted by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(H) The number of times that actionable intelligence related to border security was obtained

through the use of unmanned aerial systems and manned aircraft.

(2) Metrics consultation

To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department of Homeland Security; and

(B) as appropriate, work with the heads of other departments and agencies, including the Department of Justice.

(3) Manner of collection

The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner by Air and Marine Operations, informed by situational awareness.

(f) Data transparency

The Secretary shall—

(1) in accordance with applicable privacy laws, make data related to apprehensions, inadmissible aliens, drug seizures, and other enforcement actions available to the public, law enforcement communities, and academic research communities; and

(2) provide the Office of Immigration Statistics of the Department of Homeland Security with unfettered access to the data referred to in paragraph (1).

(g) Evaluation by the Government Accountability Office and the Secretary

(1) Metrics report

(A) Mandatory disclosures

The Secretary shall submit to the appropriate congressional committees and the Comptroller General of the United States an annual report containing the metrics required under this section and the data and methodology used to develop such metrics.

(B) Permissible disclosures

The Secretary, for the purpose of validation and verification, may submit the annual report described in subparagraph (A) to—

(i) the Center for Borders, Trade, and Immigration Research of the Centers of Excellence network of the Department of Homeland Security;

(ii) the head of a national laboratory within the Department of Homeland Security laboratory network with prior expertise in border security; and

(iii) a Federally Funded Research and Development Center.

(2) GAO report

Not later than 270 days after receiving the first report under paragraph (1)(A) and biennially thereafter for the following ten years with respect to every other such report, the Comptroller General of the United States shall submit to the appropriate congressional committees a report that—

(A) analyzes the suitability and statistical validity of the data and methodology contained in each such report; and

(B) includes recommendations on—

(i) the feasibility of other suitable metrics that may be used to measure the effectiveness of border security; and

(ii) improvements that need to be made to the metrics being used to measure the effectiveness of border security.

(3) State of the Border report

Not later than 60 days after the end of each fiscal year through fiscal year 2026, the Secretary shall submit to the appropriate congressional committees a "State of the Border" report that—

(A) provides trends for each metric under this section for the last ten fiscal years, to the greatest extent possible;

(B) provides selected analysis into related aspects of illegal flow rates, including undocumented migrant flows and stock estimation techniques;

(C) provides selected analysis into related aspects of legal flow rates; and

(D) includes any other information that the Secretary determines appropriate.

(4) Metrics update

(A) In general

After submitting the tenth report to the Comptroller General under paragraph (1), the Secretary may reevaluate and update any of the metrics developed in accordance with this section to ensure that such metrics are suitable to measure the effectiveness of border security.

(B) Congressional notification

Not later than 30 days before updating the metrics pursuant to subparagraph (A), the Secretary shall notify the appropriate congressional committees of such updates.

(Pub. L. 114–328, div. A, title X, §1092, Dec. 23, 2016, 130 Stat. 2429.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2017, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§224. Other reporting requirements

(a) Unidentified remains

(1) Reporting requirement

Not later than 1 year after December 31, 2020, and annually thereafter, the Commissioner of U.S. Customs and Border Protection shall submit a report to the appropriate committees of Congress regarding all unidentified remains discovered, during the reporting period, on or near the border between the United States and Mexico, including—

(A) for each deceased person—

(i) the cause and manner of death, if known;

(ii) the sex, age (at time of death), and country of origin (if such information is determinable); and

(iii) the location of each unidentified remain;

(B) the total number of deceased people whose unidentified remains were discovered by U.S. Customs and Border Protection during the reporting period;

(C) to the extent such information is available to U.S. Customs and Border Protection, the total number of deceased people whose unidentified remains were discovered by Federal, State, local or Tribal law enforcement officers, military personnel, or medical examiners offices;

(D) the efforts of U.S. Customs and Border Protection to engage with nongovernmental organizations, institutions of higher education, medical examiners and coroners, and law enforcement agencies—

(i) to identify and map the locations at which migrant deaths occur; and

(ii) to count the number of deaths that occur at such locations; and

(E) a detailed description of U.S. Customs and Border Protection's Missing Migrant Program, including how the program helps mitigate migrant deaths while maintaining border security.

(2) Public disclosure

Not later than 30 days after each report required under paragraph (1) is submitted, the Commissioner of U.S. Customs and Border Protection shall publish on the website of the agency the information described in subparagraphs (A), (B), and (C) of paragraph (1) during each reporting period.

(b) Rescue beacons

Not later than 1 year after December 31, 2020, and annually thereafter, the Commissioner of U.S. Customs and Border Protection shall submit a report to the appropriate committees of Congress regarding the use of rescue beacons along the border between the United States and Mexico, including, for the reporting period—

(1) the number of rescue beacons in each border patrol sector;

(2) the specific location of each rescue beacon;

(3) the frequency with which each rescue beacon was activated by a person in distress;

(4) a description of the nature of the distress that resulted in each rescue beacon activation (if such information is determinable); and

(5) an assessment, in consultation with local stakeholders, including elected officials, nongovernmental organizations, and landowners, of necessary additional rescue beacons and recommendations for locations for deployment to reduce migrant deaths.

(c) GAO report

Not later than 6 months after the report required under subsection (a) is submitted to the appropriate committees of Congress, the Comptroller General of the United States shall submit a report to the same committees that describes—

(1) how U.S. Customs and Border Protection collects and records border-crossing death data;

(2) the differences (if any) in U.S. Customs and Border Protection border-crossing death data collection methodology across its sectors;

(3) how U.S. Customs and Border Protection's data and statistical analysis on trends in the numbers, locations, causes, and characteristics of border-crossing deaths compare to other sources of data on these deaths, including border county medical examiners and coroners and the Centers for Disease Control and Prevention;

(4) how U.S. Customs and Border Protection measures the effectiveness of its programs to mitigate migrant deaths; and

(5) the extent to which U.S. Customs and Border Protection engages Federal, State, local, and Tribal governments, foreign diplomatic and consular posts, and nongovernmental organizations—

(A) to accurately identify deceased individuals;

(B) to resolve cases involving unidentified remains;

(C) to resolve cases involving unidentified persons; and

(D) to share information on missing persons and unidentified remains, specifically with the National Missing and Unidentified Persons System (NamUs).

(Pub. L. 116–277, §5, Dec. 31, 2020, 134 Stat. 3370.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of Missing Persons and Unidentified Remains Act of 2019, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§225. Reports, evaluations, and research regarding drug interdiction at and between ports of entry

(a) Research on additional technologies to detect fentanyl

Not later than one year after December 23, 2022, the Secretary of Homeland Security, in consultation with the Attorney General, the Secretary of Health and Human Services, and the

Director of the Office of National Drug Control Policy, shall research additional technological solutions to—

(1) target and detect illicit fentanyl, fentanyl analogs, and precursor chemicals, including low-purity fentanyl, especially in counterfeit pressed tablets, and illicit pill press molds; and

(2) enhance detection of such counterfeit pressed tablets through nonintrusive, noninvasive, and other advanced screening technologies.

(b) Evaluation of current technologies and strategies in illicit drug interdiction and procurement decisions

(1) In general

The Secretary of Homeland Security, in consultation with the Attorney General, the Secretary of Health and Human Services, and the Director of the Office of National Drug Control Policy, shall establish a program to collect available data and develop metrics to measure how technologies and strategies used by the Department of Homeland Security, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and other relevant Federal agencies have helped detect trafficked illicit fentanyl, fentanyl analogs, and precursor chemicals or deter illicit fentanyl, fentanyl analogs, and precursor chemicals from being trafficked into the United States at and between land, air, and sea ports of entry.

(2) Considerations

The data and metrics program established pursuant to paragraph (1) may consider—

(A) the rate of detection of illicit fentanyl, fentanyl analogs, and precursor chemicals at land, air, and sea ports of entry;

(B) investigations and intelligence sharing into the origins of illicit fentanyl, fentanyl analogs, and precursor chemicals within the United States; and

(C) other data or metrics considered appropriate by the Secretary of Homeland Security.

(3) Updates

The Secretary of Homeland Security, as appropriate and in the coordination with the officials referred to in paragraph (1), may update the data and metrics program established pursuant to paragraph (1).

(4) Reports

(A) Secretary of Homeland Security

Not later than one year after December 23, 2022, and biennially thereafter, the Secretary of Homeland Security, in consultation with the Attorney General, the Secretary of Health and Human Services, and the Director of the Office of National Drug Control Policy shall, based on the data collected and metrics developed pursuant to the program established pursuant to paragraph (1), submit to the Committee on Homeland Security, the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate a report that—

(i) examines and analyzes current technologies, including pilot technologies, deployed at land, air, and sea ports of entry to assess how well such technologies detect, deter, and address illicit fentanyl, fentanyl analogs, and precursor chemicals; and

(ii) examines and analyzes current technologies, including pilot technologies, deployed between land ports of entry to assess how well and accurately such technologies detect, deter, interdict, and address illicit fentanyl, fentanyl analogs, and precursor chemicals; [1]

(B) Government Accountability Office

Not later than one year after the submission of each of the first three reports required under subparagraph (A), the Comptroller General of the United States shall submit to the Committee on Homeland Security, the Committee on Energy and Commerce, the Committee on Science,

Space, and Technology, and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate a report that evaluates and, as appropriate, makes recommendations to improve, the collection of data under the program established pursuant to paragraph (1) and metrics used in the subsequent reports required under such subparagraph.

(Pub. L. 117–263, div. G, title LXXI, §7136, Dec. 23, 2022, 136 Stat. 3650.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *So in original. The semicolon probably should be a period.*

§226. Ensuring timely updates to U.S. Customs and Border Protection field manuals

(a) In general

Not less frequently than triennially, the Commissioner of U.S. Customs and Border Protection shall review and update, as necessary, the current policies and manuals of the Office of Field Operations related to inspections at ports of entry to ensure the uniform implementation of inspection practices that will effectively respond to technological and methodological changes designed to disguise illegal activity, such as the smuggling of drugs and humans, along the border.

(b) Reporting requirement

Shortly after each update required under subsection (a), the Commissioner of U.S. Customs and Border Protection shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that summarizes the policy and manual changes implemented by such update.

(Pub. L. 118–43, §2, Mar. 18, 2024, 138 Stat. 453.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Eradicating Narcotic Drugs and Formulating Effective New Tools to Address National Yearly Losses of life Act, also known as the END FENTANYL Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PART C—MISCELLANEOUS PROVISIONS

§231. Transfer of certain agricultural inspection functions of the Department of Agriculture

(a) Transfer of agricultural import and entry inspection functions

There shall be transferred to the Secretary the functions of the Secretary of Agriculture relating to agricultural import and entry inspection activities under the laws specified in subsection (b).

(b) Covered animal and plant protection laws

The laws referred to in subsection (a) are the following:

(1) The Act commonly known as the Virus-Serum-Toxin Act (the eighth paragraph under the heading "Bureau of Animal Industry" in the Act of March 4, 1913; 21 U.S.C. 151 et seq.).

(2) Section 1 of the Act of August 31, 1922 (commonly known as the Honeybee Act; 7 U.S.C. 281).

(3) Title III of the Federal Seed Act (7 U.S.C. 1581 et seq.).

(4) The Plant Protection Act (7 U.S.C. 7701 et seq.).

(5) The Animal Health Protection Act (subtitle E of title X of Public Law 107–171; 7 U.S.C. 8301 et seq.).

(6) The Lacey Act Amendments of 1981 (16 U.S.C. 3371 et seq.).

(7) Section 11 of the Endangered Species Act of 1973 (16 U.S.C. 1540).

(c) Exclusion of quarantine activities

For purposes of this section, the term "functions" does not include any quarantine activities carried out under the laws specified in subsection (b).

(d) Effect of transfer

(1) Compliance with Department of Agriculture regulations

The authority transferred pursuant to subsection (a) shall be exercised by the Secretary in accordance with the regulations, policies, and procedures issued by the Secretary of Agriculture regarding the administration of the laws specified in subsection (b).

(2) Rulemaking coordination

The Secretary of Agriculture shall coordinate with the Secretary whenever the Secretary of Agriculture prescribes regulations, policies, or procedures for administering the functions transferred under subsection (a) under a law specified in subsection (b).

(3) Effective administration

The Secretary, in consultation with the Secretary of Agriculture, may issue such directives and guidelines as are necessary to ensure the effective use of personnel of the Department of Homeland Security to carry out the functions transferred pursuant to subsection (a).

(e) Transfer agreement

(1) Agreement required; revision

Before the end of the transition period, as defined in section 541 of this title, the Secretary of Agriculture and the Secretary shall enter into an agreement to effectuate the transfer of functions required by subsection (a) of this section. The Secretary of Agriculture and the Secretary may jointly revise the agreement as necessary thereafter.

(2) Required terms

The agreement required by this subsection shall specifically address the following:

(A) The supervision by the Secretary of Agriculture of the training of employees of the Secretary to carry out the functions transferred pursuant to subsection (a).

(B) The transfer of funds to the Secretary under subsection (f).

(3) Cooperation and reciprocity

The Secretary of Agriculture and the Secretary may include as part of the agreement the following:

(A) Authority for the Secretary to perform functions delegated to the Animal and Plant Health Inspection Service of the Department of Agriculture regarding the protection of domestic livestock and plants, but not transferred to the Secretary pursuant to subsection (a).

(B) Authority for the Secretary of Agriculture to use employees of the Department of Homeland Security to carry out authorities delegated to the Animal and Plant Health Inspection Service regarding the protection of domestic livestock and plants.

(f) Periodic transfer of funds to Department of Homeland Security

(1) Transfer of funds

Out of funds collected by fees authorized under sections 136 and 136a of title 21, the Secretary of Agriculture shall transfer, from time to time in accordance with the agreement under subsection (e), to the Secretary funds for activities carried out by the Secretary for which such fees were collected.

(2) Limitation

The proportion of fees collected pursuant to such sections that are transferred to the Secretary under this subsection may not exceed the proportion of the costs incurred by the Secretary to all costs incurred to carry out activities funded by such fees.

(g) Transfer of Department of Agriculture employees

Not later than the completion of the transition period defined under section 541 of this title, the Secretary of Agriculture shall transfer to the Secretary not more than 3,200 full-time equivalent positions of the Department of Agriculture.

(Pub. L. 107–296, title IV, §421, Nov. 25, 2002, 116 Stat. 2182.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Virus-Serum-Toxin Act, referred to in subsec. (b)(1), is the eighth paragraph under the heading "Bureau of Animal Industry" in act Mar. 4, 1913, ch. 145, 37 Stat. 832, 833, which is classified generally to chapter 5 (§151 et seq.) of Title 21, Food and Drugs. For complete classification of this Act to the Code, see Short Title note set out under section 151 of Title 21 and Tables.

The Federal Seed Act, referred to in subsec. (b)(3), is act Aug. 9, 1939, ch. 615, 53 Stat. 1275. Title III of the Act is classified generally to subchapter III (§1581 et seq.) of chapter 37 of Title 7, Agriculture. For complete classification of this Act to the Code, see section 1551 of Title 7 and Tables.

The Plant Protection Act, referred to in subsec. (b)(4), is title IV of Pub. L. 106–224, June 20, 2000, 114 Stat. 438, which is classified principally to chapter 104 (§7701 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 7701 of Title 7 and Tables.

The Animal Health Protection Act, referred to in subsec. (b)(5), is subtitle E (§§10401–10418) of title X of Pub. L. 107–171, May 13, 2002, 116 Stat. 494, which is classified principally to chapter 109 (§8301 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 8301 of Title 7 and Tables.

The Lacey Act Amendments of 1981, referred to in subsec. (b)(6), is Pub. L. 97–79, Nov. 16, 1981, 95 Stat. 1073, which enacted chapter 53 (§3371 et seq.) of Title 16, Conservation, amended section 1540 of Title 16 and section 42 of Title 18, Crimes and Criminal Procedure, repealed sections 667e and 851 to 856 of Title 16 and sections 43, 44, 3054, and 3112 of Title 18, and enacted provisions set out as notes under sections 1540 and 3371 of Title 16. For complete classification of this Act to the Code, see Short Title note set out under section 3371 of Title 16 and Tables.

CODIFICATION

Section is comprised of section 421 of Pub. L. 107–296. Subsec. (h) of section 421 of Pub. L. 107–296 amended sections 2279e and 2279f of Title 7, Agriculture.

§232. Functions of Administrator of General Services

(a) Operation, maintenance, and protection of Federal buildings and grounds

Nothing in this chapter may be construed to affect the functions or authorities of the Administrator of General Services with respect to the operation, maintenance, and protection of buildings and grounds owned or occupied by the Federal Government and under the jurisdiction, custody, or control of the Administrator. Except for the law enforcement and related security functions transferred under section 203(3) of this title, the Administrator shall retain all powers, functions, and

authorities vested in the Administrator under chapter 1, except section 121(e)(2)(A), and chapters 5 to 11 of title 40 and other provisions of law that are necessary for the operation, maintenance, and protection of such buildings and grounds.

(b) Collection of rents and fees; Federal Buildings Fund

(1) Statutory construction

Nothing in this chapter may be construed—

(A) to direct the transfer of, or affect, the authority of the Administrator of General Services to collect rents and fees, including fees collected for protective services; or

(B) to authorize the Secretary or any other official in the Department to obligate amounts in the Federal Buildings Fund established by section 592 of title 40.

(2) Use of transferred amounts

Any amounts transferred by the Administrator of General Services to the Secretary out of rents and fees collected by the Administrator shall be used by the Secretary solely for the protection of buildings or grounds owned or occupied by the Federal Government.

(Pub. L. 107–296, title IV, §422, Nov. 25, 2002, 116 Stat. 2184.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsecs. (a) and (b)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

"Chapter 1, except section 121(e)(2)(A), and chapters 5 to 11 of title 40" substituted in subsec. (a) for "chapter 10 of title 40" and "section 592 of title 40" substituted in subsec. (b)(1)(B) for "section 490(f) of title 40" on authority of Pub. L. 107–217, §5(c), Aug. 21, 2002, 116 Stat. 1303, the first section of which enacted Title 40, Public Buildings, Property, and Works.

§233. Functions of Transportation Security Administration

(a) Consultation with Federal Aviation Administration

The Secretary and other officials in the Department shall consult with the Administrator of the Federal Aviation Administration before taking any action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace. The Secretary shall establish a liaison office within the Department for the purpose of consulting with the Administrator of the Federal Aviation Administration.

(b) Report to Congress

Not later than 60 days after November 25, 2002, the Secretary of Transportation shall transmit to Congress a report containing a plan for complying with the requirements of section 44901(d) of title 49.

(c) Limitations on statutory construction

(1) Grant of authority

Nothing in this chapter may be construed to vest in the Secretary or any other official in the Department any authority over transportation security that is not vested in the Under Secretary of Transportation for Security, or in the Secretary of Transportation under chapter 449 of title 49 on the day before November 25, 2002.

(2) Obligation of AIP funds

Nothing in this chapter may be construed to authorize the Secretary or any other official in the Department to obligate amounts made available under section 48103 of title 49.

(Pub. L. 107–296, title IV, §423, Nov. 25, 2002, 116 Stat. 2185.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (c), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to Under Secretary of Transportation for Security deemed to refer to Administrator of the Transportation Security Administration, see section 1994 of Pub. L. 115–254, set out as a note under section 114 of Title 49, Transportation.

§234. Preservation of Transportation Security Administration as a distinct entity

Notwithstanding any other provision of this chapter, the Transportation Security Administration shall be maintained as a distinct entity within the Department.

(Pub. L. 107–296, title IV, §424, as added Pub. L. 114–125, title VIII, §802(g)(1)(B)(iv)(I), Feb. 24, 2016, 130 Stat. 212.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

PRIOR PROVISIONS

A prior section 234, Pub. L. 107–296, title IV, §424, Nov. 25, 2002, 116 Stat. 2185, provided for the preservation of the Transportation Security Administration as a distinct entity applicable until 2 years after Nov. 25, 2002, prior to repeal by Pub. L. 114–125, title VIII, §802(g)(1)(B)(iv)(I), Feb. 24, 2016, 130 Stat. 212.

§235. Coordination of information and information technology

(a) Definition of affected agency

In this section, the term "affected agency" means—

(1) the Department;

(2) the Department of Agriculture;

(3) the Department of Health and Human Services; and

(4) any other department or agency determined to be appropriate by the Secretary.

(b) Coordination

The Secretary, in coordination with the Secretary of Agriculture, the Secretary of Health and Human Services, and the head of each other department or agency determined to be appropriate by the Secretary, shall ensure that appropriate information (as determined by the Secretary) concerning

inspections of articles that are imported or entered into the United States, and are inspected or regulated by 1 or more affected agencies, is timely and efficiently exchanged between the affected agencies.

(c) Report and plan

Not later than 18 months after November 25, 2002, the Secretary, in consultation with the Secretary of Agriculture, the Secretary of Health and Human Services, and the head of each other department or agency determined to be appropriate by the Secretary, shall submit to Congress—

(1) a report on the progress made in implementing this section; and

(2) a plan to complete implementation of this section.

(Pub. L. 107–296, title IV, §427, Nov. 25, 2002, 116 Stat. 2187.)

§236. Visa issuance

(a) Definition

In this subsection,[1] the term "consular office" [2] has the meaning given that term under section 101(a)(9) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(9)).

(b) In general

Notwithstanding section 104(a) of the Immigration and Nationality Act (8 U.S.C. 1104(a)) or any other provision of law, and except as provided in subsection (c) of this section, the Secretary—

(1) shall be vested exclusively with all authorities to issue regulations with respect to, administer, and enforce the provisions of such Act [8 U.S.C. 1101 et seq.], and of all other immigration and nationality laws, relating to the functions of consular officers of the United States in connection with the granting or refusal of visas, and shall have the authority to refuse visas in accordance with law and to develop programs of homeland security training for consular officers (in addition to consular training provided by the Secretary of State), which authorities shall be exercised through the Secretary of State, except that the Secretary shall not have authority to alter or reverse the decision of a consular officer to refuse a visa to an alien; and

(2) shall have authority to confer or impose upon any officer or employee of the United States, with the consent of the head of the executive agency under whose jurisdiction such officer or employee is serving, any of the functions specified in paragraph (1).

(c) Authority of the Secretary of State

(1) In general

Notwithstanding subsection (b), the Secretary of State may direct a consular officer to refuse a visa to an alien if the Secretary of State deems such refusal necessary or advisable in the foreign policy or security interests of the United States.

(2) Construction regarding authority

Nothing in this section, consistent with the Secretary of Homeland Security's authority to refuse visas in accordance with law, shall be construed as affecting the authorities of the Secretary of State under the following provisions of law:

(A) Section 101(a)(15)(A) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(A)).

(B) Section 204(d)(2) of the Immigration and Nationality Act (8 U.S.C. 1154) (as it will take effect upon the entry into force of the Convention on Protection of Children and Cooperation in Respect to Inter-Country adoption).

(C) Section 212(a)(3)(B)(i)(IV)(bb) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(i)(IV)(bb)).

(D) Section 212(a)(3)(B)(i)(VI) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(i)(VI)).

(E) Section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi)(II)).

(F) Section 212(a)(3)(C) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(C)).
(G) Section 212(a)(10)(C) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(10)(C)).
(H) Section 212(f) of the Immigration and Nationality Act (8 U.S.C. 1182(f)).
(I) Section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a)).
(J) Section 237(a)(4)(C) of the Immigration and Nationality Act (8 U.S.C. 1227(a)(4)(C)).
(K) Section 401 of the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 [22 U.S.C. 6091].
(L) Section 613 of the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies Appropriations Act, 1999 [3] (as contained in section 101(b) of division A of Public Law 105–277) (Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999); 112 Stat. 2681; H.R. 4328 (originally H.R. 4276) as amended by section 617 of Public Law 106–553.
(M) Section 103(f) of the Chemical Weapon Convention Implementation Act of 1998 [22 U.S.C. 6713(f)] (112 Stat. 2681–865).
(N) Section 801 of H.R. 3427, the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001 [8 U.S.C. 1182e], as enacted by reference in Public Law 106–113.
(O) Section 568 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2002 (Public Law 107–115).
(P) Section 51 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2723).

(d) Consular officers and chiefs of missions

(1) In general

Nothing in this section may be construed to alter or affect—
(A) the employment status of consular officers as employees of the Department of State; or
(B) the authority of a chief of mission under section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927).

(2) Construction regarding delegation of authority

Nothing in this section shall be construed to affect any delegation of authority to the Secretary of State by the President pursuant to any proclamation issued under section 212(f) of the Immigration and Nationality Act (8 U.S.C. 1182(f)), consistent with the Secretary of Homeland Security's authority to refuse visas in accordance with law.

(e) Assignment of Homeland Security employees to diplomatic and consular posts

(1) In general

The Secretary is authorized to assign employees of the Department to each diplomatic and consular post at which visas are issued, unless the Secretary determines that such an assignment at a particular post would not promote homeland security.

(2) Functions

Employees assigned under paragraph (1) shall perform the following functions:
(A) Provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications.
(B) Review any such applications, either on the initiative of the employee of the Department or upon request by a consular officer or other person charged with adjudicating such applications.
(C) Conduct investigations with respect to consular matters under the jurisdiction of the Secretary.

(3) Evaluation of consular officers

The Secretary of State shall evaluate, in consultation with the Secretary, as deemed appropriate by the Secretary, the performance of consular officers with respect to the processing and adjudication of applications for visas in accordance with performance standards developed by the

Secretary for these procedures.

(4) Report

The Secretary shall, on an annual basis, submit a report to Congress that describes the basis for each determination under paragraph (1) that the assignment of an employee of the Department at a particular diplomatic post would not promote homeland security.

(5) Permanent assignment; participation in terrorist lookout committee

When appropriate, employees of the Department assigned to perform functions described in paragraph (2) may be assigned permanently to overseas diplomatic or consular posts with country-specific or regional responsibility. If the Secretary so directs, any such employee, when present at an overseas post, shall participate in the terrorist lookout committee established under section 304 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1733).

(6) Training and hiring

(A) In general

The Secretary shall ensure, to the extent possible, that any employees of the Department assigned to perform functions under paragraph (2) and, as appropriate, consular officers, shall be provided the necessary training to enable them to carry out such functions, including training in foreign languages, interview techniques, and fraud detection techniques, in conditions in the particular country where each employee is assigned, and in other appropriate areas of study.

(B) Use of Center

The Secretary is authorized to use the National Foreign Affairs Training Center, on a reimbursable basis, to obtain the training described in subparagraph (A).

(7) Report

Not later than 1 year after November 25, 2002, the Secretary and the Secretary of State shall submit to Congress—

(A) a report on the implementation of this subsection; and

(B) any legislative proposals necessary to further the objectives of this subsection.

(8) Effective date

This subsection shall take effect on the earlier of—

(A) the date on which the President publishes notice in the Federal Register that the President has submitted a report to Congress setting forth a memorandum of understanding between the Secretary and the Secretary of State governing the implementation of this section; or

(B) the date occurring 1 year after November 25, 2002.

(f) No creation of private right of action

Nothing in this section shall be construed to create or authorize a private right of action to challenge a decision of a consular officer or other United States official or employee to grant or deny a visa.

(g) Study regarding use of foreign nationals

(1) In general

The Secretary of Homeland Security shall conduct a study of the role of foreign nationals in the granting or refusal of visas and other documents authorizing entry of aliens into the United States. The study shall address the following:

(A) The proper role, if any, of foreign nationals in the process of rendering decisions on such grants and refusals.

(B) Any security concerns involving the employment of foreign nationals.

(C) Whether there are cost-effective alternatives to the use of foreign nationals.

(2) Report

Not later than 1 year after November 25, 2002, the Secretary shall submit a report containing

the findings of the study conducted under paragraph (1) to the Committee on the Judiciary, the Committee on International Relations, and the Committee on Government Reform of the House of Representatives, and the Committee on the Judiciary, the Committee on Foreign Relations, and the Committee on Government [4] Affairs of the Senate.

(h) Report

Not later than 120 days after November 25, 2002, the Director of the Office of Science and Technology Policy shall submit to Congress a report on how the provisions of this section will affect procedures for the issuance of student visas.

(i) Visa issuance program for Saudi Arabia

Notwithstanding any other provision of law, after November 25, 2002, all third party screening programs in Saudi Arabia shall be terminated. On-site personnel of the Department of Homeland Security shall review all visa applications prior to adjudication.

(Pub. L. 107–296, title IV, §428, Nov. 25, 2002, 116 Stat. 2187.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Immigration and Nationality Act, referred to in subsec. (b)(1), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

Section 613 of the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies Appropriations Act, 1999, referred to in subsec. (c)(2)(L), probably means section 101(b) [title VI, §616] of Pub. L. 105–277, div. A, Oct. 21, 1998, 112 Stat. 2681–50, 2681–114, which prohibits use of funds for issuance of visas to persons alleged to have ordered, carried out, or materially assisted in extrajudicial and political killings in Haiti and to certain others and is not classified to the Code.

Section 103(f) of the Chemical Weapon Convention Implementation Act of 1998, referred to in subsec. (c)(2)(M), probably means section 103(f) of the Chemical Weapons Convention Implementation Act of 1998, which is classified to section 6713(f) of Title 22, Foreign Relations and Intercourse.

Section 568 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2002, referred to in subsec. (c)(2)(O), is section 568 of title V of Pub. L. 107–115, Jan. 10, 2002, 115 Stat. 2166, which is not classified to the Code.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

References to National Foreign Affairs Training Center considered to refer to George P. Shultz National Foreign Affairs Training Center, see section 1(b) of Pub. L. 107–132, set out as a note under section 4021 of Title 22, Foreign Relations and Intercourse.

Committee on International Relations of House of Representatives changed to Committee on Foreign Affairs of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

[1] *So in original. Probably should be "section".*

[2] *So in original. Probably should be " 'consular officer' ".*

[3] *See References in Text note below.*

[4] *So in original. Probably should be "Governmental".*

§237. Information on visa denials required to be entered into electronic data system

(a) In general

Whenever a consular officer of the United States denies a visa to an applicant, the consular officer shall enter the fact and the basis of the denial and the name of the applicant into the interoperable electronic data system implemented under section 1722(a) of title 8.

(b) Prohibition

In the case of any alien with respect to whom a visa has been denied under subsection (a)—

(1) no subsequent visa may be issued to the alien unless the consular officer considering the alien's visa application has reviewed the information concerning the alien placed in the interoperable electronic data system, has indicated on the alien's application that the information has been reviewed, and has stated for the record why the visa is being issued or a waiver of visa ineligibility recommended in spite of that information; and

(2) the alien may not be admitted to the United States without a visa issued in accordance with the procedures described in paragraph (1).

(Pub. L. 107–296, title IV, §429, Nov. 25, 2002, 116 Stat. 2191.)

§238. Office for Domestic Preparedness

(a) Establishment

There is established in the Department an Office for Domestic Preparedness.

(b) Director

There shall be a Director of the Office for Domestic Preparedness, who shall be appointed by the President.

(c) Responsibilities

The Office for Domestic Preparedness shall have the primary responsibility within the executive branch of Government for the preparedness of the United States for acts of terrorism, including—

(1) coordinating preparedness efforts at the Federal level, and working with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support;

(2) coordinating or, as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government;

(3) directing and supervising terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers;

(4) incorporating the Strategy priorities into planning guidance on an agency level for the preparedness efforts of the Office for Domestic Preparedness;

(5) providing agency-specific training for agents and analysts within the Department, other agencies, and State and local agencies and international entities;

(6) as the lead executive branch agency for preparedness of the United States for acts of terrorism, cooperating closely with the Federal Emergency Management Agency, which shall have the primary responsibility within the executive branch to prepare for and mitigate the effects of nonterrorist-related disasters in the United States;

(7) assisting and supporting the Secretary, in coordination with other Directorates and entities outside the Department, in conducting appropriate risk analysis and risk management activities of State, local, and tribal governments consistent with the mission and functions of the Department;

(8) those elements of the Office of National Preparedness of the Federal Emergency Management Agency which relate to terrorism, which shall be consolidated within the Department in the Office for Domestic Preparedness established under this section; and

(9) helping to ensure the acquisition of interoperable communication technology by State and local governments and emergency response providers.

(d) Fiscal years 2003 and 2004

During fiscal year 2003 and fiscal year 2004, the Director of the Office for Domestic Preparedness established under this section shall manage and carry out those functions of the Office for Domestic Preparedness of the Department of Justice (transferred under this section) before September 11, 2001, under the same terms, conditions, policies, and authorities, and with the required level of personnel, assets, and budget before September 11, 2001.

(Pub. L. 107–296, title IV, §430, Nov. 25, 2002, 116 Stat. 2191; Pub. L. 108–458, title VII, §7303(h)(2), Dec. 17, 2004, 118 Stat. 3847; Pub. L. 112–166, §2(f)(1), Aug. 10, 2012, 126 Stat. 1284; Pub. L. 114–125, title VIII, §802(g)(1)(B)(iv)(II), Feb. 24, 2016, 130 Stat. 212.)

EDITORIAL NOTES

AMENDMENTS

2016—Subsec. (a). Pub. L. 114–125, §802(g)(1)(B)(iv)(II)(aa), amended subsec. (a) generally. Prior to amendment, text read as follows: "The Office for Domestic Preparedness shall be within the Directorate of Border and Transportation Security."

Subsec. (b). Pub. L. 114–125, §802(g)(1)(B)(iv)(II)(bb), struck out at end "The Director of the Office for Domestic Preparedness shall report directly to the Under Secretary for Border and Transportation Security."

Subsec. (c)(7). Pub. L. 114–125, §802(g)(1)(B)(iv)(II)(cc), substituted "functions of the Department" for "functions of the Directorate".

2012—Subsec. (b). Pub. L. 112–166 struck out ", by and with the advice and consent of the Senate" before period at end of first sentence.

2004—Subsec. (c)(9). Pub. L. 108–458 added par. (9).

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–166 effective 60 days after Aug. 10, 2012, and applicable to appointments made on and after that effective date, including any nomination pending in the Senate on that date, see section 6(a) of Pub. L. 112–166, set out as a note under section 113 of this title.

§239. Office of Cargo Security Policy

(a) Establishment

There is established within the Department an Office of Cargo Security Policy (referred to in this section as the "Office").

(b) Purpose

The Office shall—

(1) coordinate all Department policies relating to cargo security; and

(2) consult with stakeholders and coordinate with other Federal agencies in the establishment of

standards and regulations and to promote best practices.

(c) Director

(1) Appointment

The Office shall be headed by a Director, who shall—

(A) be appointed by the Secretary; and

(B) report to the Assistant Secretary for Policy.

(2) Responsibilities

The Director shall—

(A) advise the Assistant Secretary for Policy in the development of Department-wide policies regarding cargo security;

(B) coordinate all policies relating to cargo security among the agencies and offices within the Department relating to cargo security; and

(C) coordinate the cargo security policies of the Department with the policies of other executive agencies.

(Pub. L. 107–296, title IV, §431, as added Pub. L. 109–347, title III, §301(a), Oct. 13, 2006, 120 Stat. 1920.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 109–347, title III, §301(c), Oct. 13, 2006, 120 Stat. 1920, provided that: "Nothing in this section [enacting this section and section 1001 of this title] shall be construed to affect—

"(1) the authorities, functions, or capabilities of the Coast Guard to perform its missions; or

"(2) the requirement under section 888 of the Homeland Security Act (6 U.S.C. 468) that those authorities, functions, and capabilities be maintained intact."

§240. Border Enforcement Security Task Force

(a) Establishment

There is established within the Department a program to be known as the Border Enforcement Security Task Force (referred to in this section as "BEST").

(b) Purpose

The purpose of BEST is to establish units to enhance border security by addressing and reducing border security threats and violence by—

(1) facilitating collaboration among Federal, State, local, tribal, and foreign law enforcement agencies to execute coordinated activities in furtherance of border security, and homeland security; and

(2) enhancing information-sharing, including the dissemination of homeland security information among such agencies.

(c) Composition and establishment of units

(1) Composition

BEST units may be comprised of personnel from—

(A) U.S. Immigration and Customs Enforcement;

(B) U.S. Customs and Border Protection;

(C) the United States Coast Guard;

(D) other Department personnel, as appropriate [1]

(E) other Federal agencies, as appropriate;

(F) appropriate State law enforcement agencies;

(G) foreign law enforcement agencies, as appropriate;

(H) local law enforcement agencies from affected border cities and communities; and
(I) appropriate tribal law enforcement agencies.

(2) Establishment of units

The Secretary is authorized to establish BEST units in jurisdictions in which such units can contribute to BEST missions, as appropriate. Before establishing a BEST unit, the Secretary shall consider—

(A) whether the area in which the BEST unit would be established is significantly impacted by cross-border threats;

(B) the availability of Federal, State, local, tribal, and foreign law enforcement resources to participate in the BEST unit;

(C) the extent to which border security threats are having a significant harmful impact in the jurisdiction in which the BEST unit is to be established, and other jurisdictions in the country; and

(D) whether or not an Integrated Border Enforcement Team already exists in the area in which the BEST unit would be established.

(3) Duplication of efforts

In determining whether to establish a new BEST unit or to expand an existing BEST unit in a given jurisdiction, the Secretary shall ensure that the BEST unit under consideration does not duplicate the efforts of other existing interagency task forces or centers within that jurisdiction.

(d) Operation

After determining the jurisdictions in which to establish BEST units under subsection (c)(2), and in order to provide Federal assistance to such jurisdictions, the Secretary may—

(1) direct the assignment of Federal personnel to BEST, subject to the approval of the head of the department or agency that employs such personnel; and

(2) take other actions to assist Federal, State, local, and tribal entities to participate in BEST, including providing financial assistance, as appropriate, for operational, administrative, salary reimbursement, and technological costs associated with the participation of Federal, State, local, and tribal law enforcement agencies in BEST.

(e) Report

Not later than 180 days after the date on which BEST is established under this section, and annually thereafter for the following 5 years, the Secretary shall submit a report to Congress that describes the effectiveness of BEST in enhancing border security and reducing the drug trafficking, arms smuggling, illegal alien trafficking and smuggling, violence, and kidnapping along and across the international borders of the United States, as measured by crime statistics, including violent deaths, incidents of violence, and drug-related arrests.

(Pub. L. 107–296, title IV, §432, as added Pub. L. 112–205, §3(a), Dec. 7, 2012, 126 Stat. 1488; amended Pub. L. 117–159, div. A, title II, §12004(j), June 25, 2022, 136 Stat. 1332.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (d)(2). Pub. L. 117–159 inserted "salary reimbursement," after "administrative,".

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–159 to be construed to allow the establishment of a Federal system of registration of firearms, firearms owners, or firearms transactions or dispositions, see section 12004(k) of Pub. L. 117–159, set out as a note under section 922 of Title 18, Crimes and Criminal Procedure.

FINDINGS AND DECLARATION OF PURPOSES

Pub. L. 112–205, §2, Dec. 7, 2012, 126 Stat. 1487, provided that: "Congress finds the following:

"(1) The Department of Homeland Security's (DHS) overriding mission is to lead a unified national effort to protect the United States. United States Immigration and Customs Enforcement (ICE) is the largest investigative agency within DHS and is charged with enforcing a wide array of laws, including laws related to securing the border and combating criminal smuggling.

"(2) Mexico's northern border with the United States has experienced a dramatic surge in border crime and violence in recent years due to intense competition between Mexican drug cartels and criminal smuggling organizations that employ predatory tactics to realize their profits.

"(3) Law enforcement agencies at the United States northern border also face challenges from transnational smuggling organizations.

"(4) In response, DHS has partnered with Federal, State, local, tribal, and foreign law enforcement counterparts to create the Border Enforcement Security Task Force (BEST) initiative as a comprehensive approach to addressing border security threats. These multi-agency teams are designed to increase information-sharing and collaboration among the participating law enforcement agencies.

"(5) BEST teams incorporate personnel from ICE, United States Customs and Border Protection (CBP), the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATFE), the Federal Bureau of Investigation (FBI), the United States Coast Guard (USCG), and the U.S. Attorney's Office (USAO), along with other key Federal, State and local law enforcement agencies.

"(6) Foreign law enforcement agencies participating in BEST include Mexico's Secretaria de Seguridad Publica (SSP), the Canada Border Services Agency (CBSA), the Ontario Provincial Police (OPP), and the Royal Canadian Mounted Police (RCMP)."

[1] *So in original. Probably should be followed by a semicolon.*

§241. Prevention of international child abduction

(a) Program established

The Secretary, through the Commissioner of U.S. Customs and Border Protection (referred to in this section as "CBP"), in coordination with the Secretary of State, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish a program that—

(1) seeks to prevent a child (as defined in section 1204(b)(1) of title 18) from departing from the territory of the United States if a parent or legal guardian of such child presents a court order from a court of competent jurisdiction prohibiting the removal of such child from the United States to a CBP Officer in sufficient time to prevent such departure for the duration of such court order; and

(2) leverages other existing authorities and processes to address the wrongful removal and return of a child.

(b) Interagency coordination

(1) In general

The Secretary of State shall convene and chair an interagency working group to prevent international parental child abduction. The group shall be composed of presidentially appointed, Senate confirmed officials from—

(A) the Department of State;

(B) the Department of Homeland Security, including U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement; and

(C) the Department of Justice, including the Federal Bureau of Investigation.

(2) Department of Defense

The Secretary of Defense shall designate an official within the Department of Defense—

(A) to coordinate with the Department of State on international child abduction issues; and

(B) to oversee activities designed to prevent or resolve international child abduction cases relating to active duty military service members.

(Pub. L. 107–296, title IV, §433, as added Pub. L. 113–150, title III, §301(a), Aug. 8, 2014, 128 Stat.

1822.)

§242. Department of Homeland Security Blue Campaign

(a) Definition

In this section, the term "human trafficking" means an act or practice described in paragraph (9) or (10) [1] of section 7102 of title 22.

(b) Establishment

There is established within the Department a program, which shall be known as the "Blue Campaign". The Blue Campaign shall be headed by a Director, who shall be appointed by the Secretary.

(c) Purpose

The purpose of the Blue Campaign shall be to unify and coordinate Department efforts to address human trafficking.

(d) Responsibilities

The Secretary, working through the Director, shall, in accordance with subsection (e)—

(1) issue Department-wide guidance to appropriate Department personnel;

(2) develop training programs for such personnel;

(3) coordinate departmental efforts, including training for such personnel; and

(4) provide guidance and training on trauma-informed practices to ensure that human trafficking victims are afforded prompt access to victim support service providers, in addition to the assistance required under section 7105 of title 22, to address their immediate and long-term needs.

(e) Guidance and training

The Blue Campaign shall provide guidance and training to Department personnel and other Federal, State, tribal, and law enforcement personnel, as appropriate, regarding—

(1) programs to help identify instances of human trafficking;

(2) the types of information that should be collected and recorded in information technology systems utilized by the Department to help identify individuals suspected or convicted of human trafficking;

(3) systematic and routine information sharing within the Department and among Federal, State, tribal, and local law enforcement agencies regarding—

(A) individuals suspected or convicted of human trafficking; and

(B) patterns and practices of human trafficking;

(4) techniques to identify suspected victims of trafficking along the United States border and at airport security checkpoints;

(5) methods to be used by the Transportation Security Administration and personnel from other appropriate agencies to—

(A) train employees of the Transportation Security Administration to identify suspected victims of trafficking; and

(B) serve as a liaison and resource regarding human trafficking prevention to appropriate State, local, and private sector aviation workers and the traveling public;

(6) developing and utilizing, in consultation with the Blue Campaign Advisory Board established pursuant to subsection (g), resources such as indicator cards, fact sheets, pamphlets, posters, brochures, and radio and television campaigns to—

(A) educate partners and stakeholders; and

(B) increase public awareness of human trafficking;

(7) leveraging partnerships with State and local governmental, nongovernmental, and private

sector organizations to raise public awareness of human trafficking; and

(8) any other activities the Secretary determines necessary to carry out the Blue Campaign.

(f) Web-based training programs

To enhance training opportunities, the Director of the Blue Campaign shall develop web-based interactive training videos that utilize a learning management system to provide online training opportunities. During the 10-year period beginning on the date that is 90 days after December 27, 2021, such training opportunities shall be made available to the following individuals:

(1) Federal, State, local, Tribal, and territorial law enforcement officers.

(2) Non-Federal correction system personnel.

(3) Such other individuals as the Director determines appropriate.

(g) Blue Campaign Advisory Board

(1) In general

There is established in the Department a Blue Campaign Advisory Board, which shall be comprised of representatives assigned by the Secretary from—

(A) the Office for Civil Rights and Civil Liberties of the Department;

(B) the Privacy Office of the Department; and

(C) not fewer than four other separate components or offices of the Department.

(2) Charter

The Secretary is authorized to issue a charter for the Blue Campaign Advisory Board, and such charter shall specify the following:

(A) The Board's mission, goals, and scope of its activities.

(B) The duties of the Board's representatives.

(C) The frequency of the Board's meetings.

(3) Consultation

The Director shall consult the Blue Campaign Advisory Board and, as appropriate, experts from other components and offices of the Center for Countering Human Trafficking of the Department regarding the following:

(A) Recruitment tactics used by human traffickers to inform the development of training and materials by the Blue Campaign.

(B) The development of effective awareness tools for distribution to Federal and non-Federal officials to identify and prevent instances of human trafficking.

(C) Identification of additional persons or entities that may be uniquely positioned to recognize signs of human trafficking and the development of materials for such persons.

(h) Consultation

With regard to the development of programs under the Blue Campaign and the implementation of such programs, the Director is authorized to consult with State, local, Tribal, and territorial agencies, non-governmental organizations, private sector organizations, and experts.

(Pub. L. 107–296, title IV, §434, as added Pub. L. 115–125, §2(a), Feb. 14, 2018, 132 Stat. 315; amended Pub. L. 117–81, div. F, title LXIV, §6407, Dec. 27, 2021, 135 Stat. 2403.)

EDITORIAL NOTES

REFERENCES IN TEXT

Paragraphs (9) and (10) of section 7102 of title 22, referred to in subsec. (a), were redesignated pars. (11) and (12), respectively, of section 7102 of title 22 by Pub. L. 115–427, §2(1), Jan. 9, 2019, 132 Stat. 5503.

AMENDMENTS

2021—Subsec. (e)(6). Pub. L. 117–81, §6407(1), substituted "developing and utilizing, in consultation with the Blue Campaign Advisory Board established pursuant to subsection (g), resources" for "utilizing resources," in introductory provisions.

Subsecs. (f) to (h). Pub. L. 117–81, §6407(2), added subsecs. (f) to (h).

STATUTORY NOTES AND RELATED SUBSIDIARIES

TRANSFER OF OTHER FUNCTIONS RELATED TO HUMAN TRAFFICKING

Pub. L. 117–322, §6, Dec. 27, 2022, 136 Stat. 4436, provided that:

"(a) BLUE CAMPAIGN.—The functions and resources of the Blue Campaign located within the Office of Partnership and Engagement on the day before the date of the enactment of this Act [Dec. 27, 2022] are hereby transferred to CCHT [Center for Countering Human Trafficking].

"(b) OTHER TRANSFER.—

"(1) AUTHORIZATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security may transfer the functions and resources of any component, directorate, or other office of the Department of Homeland Security related to combating human trafficking to the CCHT.

"(2) NOTIFICATION.—Not later than 30 days before executing any transfer authorized under paragraph (1), the Secretary of Homeland Security shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of such planned transfer."

INFORMATION TECHNOLOGY SYSTEMS

Pub. L. 115–125, §3, Feb. 14, 2018, 132 Stat. 316, provided that: "Not later than one year after the date of the enactment of this Act [Feb. 14, 2018], the Secretary of Homeland Security shall ensure, in accordance with the Department of Homeland Security-wide guidance required under section 434(d) of the Homeland Security Act of 2002 [6 U.S.C. 242(d)], as added by section 2 of this Act, the integration of information technology systems utilized within the Department to record and track information regarding individuals suspected or convicted of human trafficking (as such term is defined in such section)."

[1] *See References in Text note below.*

§242a. Department of Homeland Security Center for Countering Human Trafficking

(a) Establishment

(1) In general

The Secretary of Homeland Security shall operate, within U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the Center for Countering Human Trafficking (referred to in this Act as "CCHT").

(2) Purpose

The purpose of CCHT shall be to serve at the forefront of the Department of Homeland Security's unified global efforts to counter human trafficking through law enforcement operations and victim protection, prevention, and awareness programs.

(3) Administration

Homeland Security Investigations shall—

(A) maintain a concept of operations that identifies CCHT participants, funding, core functions, and personnel; and

(B) update such concept of operations, as needed, to accommodate its mission and the threats to such mission.

(4) Personnel

(A) Director

The Secretary of Homeland Security shall appoint a CCHT Director, who shall—

(i) be a member of the Senior Executive Service; and

(ii) serve as the Department of Homeland Security's representative on human trafficking.

(B) Minimum core personnel requirements

Subject to appropriations, the Secretary of Homeland Security shall ensure that CCHT is staffed with at least 45 employees in order to maintain continuity of effort, subject matter expertise, and necessary support to the Department of Homeland Security, including—

(i) employees who are responsible for the Continued Presence Program and other victim protection duties;

(ii) employees who are responsible for training, including curriculum development, and public awareness and education;

(iii) employees who are responsible for stakeholder engagement, Federal interagency coordination, multilateral partnerships, and policy;

(iv) employees who are responsible for public relations, human resources, evaluation, data analysis and reporting, and information technology;

(v) special agents and criminal analysts necessary to accomplish its mission of combating human trafficking and the importation of goods produced with forced labor; and

(vi) managers.

(b) Operations Unit

The CCHT Director shall operate, within CCHT, an Operations Unit, which shall, at a minimum—

(1) support criminal investigations of human trafficking (including sex trafficking and forced labor)—

(A) by developing, tracking, and coordinating leads; and

(B) by providing subject matter expertise;

(2) augment the enforcement of the prohibition on the importation of goods produced with forced labor through civil and criminal authorities;

(3) coordinate a Department-wide effort to conduct procurement audits and enforcement actions, including suspension and debarment, in order to mitigate the risk of human trafficking throughout Department acquisitions and contracts; and

(4) support all CCHT enforcement efforts with intelligence by conducting lead development, lead validation, case support, strategic analysis, and data analytics.

(c) Protection and Awareness Programs Unit

The CCHT Director shall operate, within CCHT, a Protection and Awareness Programs Unit, which shall—

(1) incorporate a victim-centered approach throughout Department of Homeland Security policies, training, and practices;

(2) operate a comprehensive Continued Presence program;

(3) conduct, review, and assist with Department of Homeland Security human trafficking training, screening, and identification tools and efforts;

(4) operate the Blue Campaign's nationwide public awareness effort and any other awareness efforts needed to encourage victim identification and reporting to law enforcement and to prevent human trafficking; and

(5) coordinate external engagement, including training and events, regarding human trafficking with critical partners, including survivors, nongovernmental organizations, corporations, multilateral entities, law enforcement agencies, and other interested parties.

(Pub. L. 117–322, §3, Dec. 27, 2022, 136 Stat. 4433.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (a)(1), is Pub. L. 117–322, Dec. 27, 2022, 136 Stat. 4433, known as the Countering Human Trafficking Act of 2021, which enacted this section and section 242b of this title and

provisions set out as notes under this section and section 242 of this title. For complete classification of this Act to the Code, see section 1 of Pub. L. 117–322, set out as a Short Title of 2022 Amendment note under section 101 of this title and Tables.

CODIFICATION

Section was enacted as part of the Countering Human Trafficking Act of 2021, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

FORCED LABOR REQUIREMENTS: DEPARTMENT OF HOMELAND SECURITY

Pub. L. 117–347, title IV, §406(b), Jan. 5, 2023, 136 Stat. 6209, provided that:

"(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act [Jan. 5, 2023], the Secretary of Homeland Security shall establish a team of not less than 10 agents within the Center for Countering Human Trafficking of the Department of Homeland Security to be assigned to exclusively investigate labor trafficking.

"(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out paragraph (1) $2,000,000 for each of fiscal years 2022 to 2027, to remain available until expended."

SENSE OF CONGRESS

Pub. L. 117–322, §2, Dec. 27, 2022, 136 Stat. 4433, provided that: "It is the sense of Congress that—

"(1) the victim-centered approach must become universally understood, adopted, and practiced;

"(2) criminal justice efforts must increase the focus on, and adeptness at, investigating and prosecuting forced labor cases;

"(3) corporations must eradicate forced labor from their supply chains;

"(4) the Department of Homeland Security must lead by example—

"(A) by ensuring that its government supply chain of contracts and procurement are not tainted by forced labor; and

"(B) by leveraging all of its authorities against the importation of goods produced with forced labor; and

"(5) human trafficking training, awareness, identification, and screening efforts—

"(A) are a necessary first step for prevention, protection, and enforcement; and

"(B) should be evidence-based to be most effective."

§242b. Reports

(a) Information sharing to facilitate reports and analysis

Each subagency of the Department of Homeland Security shall share with CCHT—

(1) any information needed by CCHT to develop the strategy and proposal required under section 4(a);[1] and

(2) any additional data analysis to help CCHT better understand the issues surrounding human trafficking.

(b) Report to Congress

Not later than 1 year after December 27, 2022, the CCHT Director shall submit a report to Congress that identifies any legislation that is needed to facilitate the Department of Homeland Security's mission to end human trafficking.

(c) Annual report on potential human trafficking victims

Not later than 1 year after December 27, 2022, and annually thereafter, the Secretary of Homeland Security shall submit a report to Congress that includes—

(1) the numbers of screened and identified potential victims of trafficking (as defined in section 7102(17) of title 22) at or near the international border between the United States and Mexico, including a summary of the age ranges of such victims and their countries of origin; and

(2) an update on the Department of Homeland Security's efforts to establish protocols and methods for personnel to report human trafficking, pursuant to the Department of Homeland

Security Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation, published in January 2020.

(Pub. L. 117–322, §5, Dec. 27, 2022, 136 Stat. 4435.)

EDITORIAL NOTES

REFERENCES IN TEXT

CCHT, referred to in text, means the Center for Countering Human Trafficking, see section 242a(a)(1) of this title.

Section 4(a), referred to in subsec. (a)(1), means section 4(a) of Pub. L. 117–322, Dec. 27, 2022, 136 Stat. 4435, which is not classified to the Code.

CODIFICATION

Section was enacted as part of the Countering Human Trafficking Act of 2021, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *See References in Text note below.*

§243. Maritime operations coordination plan

(a) In general

Not later than 180 days after October 5, 2018, and biennially thereafter, the Secretary shall—

(1) update the Maritime Operations Coordination Plan, published by the Department on July 7, 2011, to strengthen coordination, planning, information sharing, and intelligence integration for maritime operations of components and offices of the Department with responsibility for maritime security missions; and

(2) submit each update to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives.

(b) Contents

Each update shall address the following:

(1) Coordinating the planning, integration of maritime operations, and development of joint maritime domain awareness efforts of any component or office of the Department with responsibility for maritime security missions.

(2) Maintaining effective information sharing and, as appropriate, intelligence integration, with Federal, State, and local officials and the private sector, regarding threats to maritime security.

(3) Cooperating and coordinating with Federal departments and agencies, and State and local agencies, in the maritime environment, in support of maritime security missions.

(4) Highlighting the work completed within the context of other national and Department maritime security strategic guidance and how that work fits with the Maritime Operations Coordination Plan.

(Pub. L. 107–296, title IV, §435, as added Pub. L. 115–254, div. J, §1807(a), Oct. 5, 2018, 132 Stat. 3536.)

§244. Maritime security capabilities assessments

Not later than 180 days after October 5, 2018, and annually thereafter, the Secretary shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives, an

assessment of the number and type of maritime assets and the number of personnel required to increase the Department's maritime response rate pursuant to section 223 of this title.

(Pub. L. 107–296, title IV, §436, as added Pub. L. 115–254, div. J, §1811(a), Oct. 5, 2018, 132 Stat. 3538.)

§245. Operational data sharing capability

(a) In general

Not later than 18 months after December 23, 2022, the Secretary shall, consistent with the ongoing Integrated Multi-Domain Enterprise joint effort by the Department of Homeland Security and the Department of Defense, establish a secure, centralized capability to allow real-time, or near real-time, data and information sharing between Customs and Border Protection and the Coast Guard for purposes of maritime boundary domain awareness and enforcement activities along the maritime boundaries of the United States, including the maritime boundaries in the northern and southern continental United States and Alaska.

(b) Priority

In establishing the capability under subsection (a), the Secretary shall prioritize enforcement areas experiencing the highest levels of enforcement activity.

(c) Requirements

The capability established under subsection (a) shall be sufficient for the secure sharing of data, information, and surveillance necessary for operational missions, including data from governmental assets, irrespective of whether an asset located in or around mission operation areas belongs to the Coast Guard, Customs and Border Protection, or any other partner agency.

(d) Elements

The Commissioner of Customs and Border Protection and the Commandant shall jointly—

(1) assess and delineate the types of data and quality of data sharing needed to meet the respective operational missions of Customs and Border Protection and the Coast Guard, including video surveillance, seismic sensors, infrared detection, space-based remote sensing, and any other data or information necessary;

(2) develop appropriate requirements and processes for the credentialing of personnel of Customs and Border Protection and personnel of the Coast Guard to access and use the capability established under subsection (a); and

(3) establish a cost-sharing agreement for the long-term operation and maintenance of the capability and the assets that provide data to the capability.

(e) Report

Not later than 2 years after December 23, 2022, the Secretary shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives a report on the establishment of the capability under this section.

(f) Rule of construction

Nothing in this section may be construed to authorize the Coast Guard, Customs and Border Protection, or any other partner agency to acquire, share, or transfer personal information relating to an individual in violation of any Federal or State law or regulation.

(Pub. L. 117–263, div. K, title CXII, §11264, Dec. 23, 2022, 136 Stat. 4062.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 117–263, div. K, §11003, Dec. 23, 2022, 136 Stat. 4003, provided that:

"(a) IN GENERAL.—Nothing in this division [div. K (§§11001–11808) of Pub. L. 117–263, see Tables for classification] may be construed—

"(1) to satisfy any requirement for government-to-government consultation with Tribal governments; or

"(2) to affect or modify any treaty or other right of any Tribal government.

"(b) TRIBAL GOVERNMENT DEFINED.—In this section, the term 'Tribal government' means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, individually identified (including parenthetically) in the list published most recently as of the date of the enactment of this Act [Dec. 23, 2022] pursuant to section 104 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131)."

DEFINITIONS

For definitions of "Secretary" and "Commandant" as referred to in this section, see section 11002 of div. K of Pub. L. 117–263, set out as a note under section 106 of Title 14, Coast Guard.

PART D—IMMIGRATION ENFORCEMENT FUNCTIONS

§251. Transfer of functions

In accordance with subchapter XII (relating to transition provisions), there shall be transferred from the Commissioner of Immigration and Naturalization to the Secretary all functions performed under the following programs, and all personnel, assets, and liabilities pertaining to such programs, immediately before such transfer occurs:

(1) The Border Patrol program.

(2) The detention and removal program.

(3) The intelligence program.

(4) The investigations program.

(5) The inspections program.

(Pub. L. 107–296, title IV, §441, Nov. 25, 2002, 116 Stat. 2192; Pub. L. 114–125, title VIII, §802(g)(1)(B)(v)(I), Feb. 24, 2016, 130 Stat. 212.)

EDITORIAL NOTES

AMENDMENTS

2016—Pub. L. 114–125 substituted "Transfer of functions" for "Transfer of functions to Under Secretary for Border and Transportation Security" in section catchline and "Secretary" for "Under Secretary for Border and Transportation Security" in introductory provisions.

§252. U.S. Immigration and Customs Enforcement

(a) Establishment

(1) In general

There shall be in the Department of Homeland Security a bureau to be known as the "Bureau of Border Security".

(2) Assistant Secretary

The head of U.S. Immigration and Customs Enforcement shall be the Assistant Secretary of U.S. Immigration and Customs Enforcement, who—

(A) shall report directly to the Under Secretary for Border and Transportation Security; and

(B) shall have a minimum of 5 years professional experience in law enforcement, and a minimum of 5 years of management experience.

(3) Functions

The Assistant Secretary of U.S. Immigration and Customs Enforcement—

(A) shall establish the policies for performing such functions as are—

(i) transferred to the Under Secretary for Border and Transportation Security by section 251 of this title and delegated to the Assistant Secretary by the Under Secretary for Border and Transportation Security; or

(ii) otherwise vested in the Assistant Secretary by law;

(B) shall oversee the administration of such policies; and

(C) shall advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of U.S. Immigration and Customs Enforcement affecting U.S. Citizenship and Immigration Services established under part E of this subchapter, including potentially conflicting policies or operations.

(4) Program to collect information relating to foreign students

The Assistant Secretary of U.S. Immigration and Customs Enforcement shall be responsible for administering the program to collect information relating to nonimmigrant foreign students and other exchange program participants described in section 1372 of title 8, including the Student and Exchange Visitor Information System established under that section, and shall use such information to carry out the enforcement functions of the agency.

(5) Managerial rotation program

(A) In general

Not later than 1 year after the date on which the transfer of functions specified under section 251 of this title takes effect, the Assistant Secretary of U.S. Immigration and Customs Enforcement shall design and implement a managerial rotation program under which employees of such agency holding positions involving supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, as a GS–14 or above, shall—

(i) gain some experience in all the major functions performed by such agency; and

(ii) work in at least one local office of such agency.

(B) Report

Not later than 2 years after the date on which the transfer of functions specified under section 251 of this title takes effect, the Secretary shall submit a report to the Congress on the implementation of such program.

(b) Chief of Policy and Strategy

(1) In general

There shall be a position of Chief of Policy and Strategy for U.S. Immigration and Customs Enforcement.

(2) Functions

In consultation with U.S. Immigration and Customs Enforcement personnel in local offices, the Chief of Policy and Strategy shall be responsible for—

(A) making policy recommendations and performing policy research and analysis on immigration enforcement issues; and

(B) coordinating immigration policy issues with the Chief of Policy and Strategy for U.S.

Citizenship and Immigration Services (established under part E of this subchapter), as appropriate.

(c) Legal advisor

There shall be a principal legal advisor to the Assistant Secretary of U.S. Immigration and Customs Enforcement. The legal advisor shall provide specialized legal advice to the Assistant Secretary of U.S. Immigration and Customs Enforcement and shall represent the agency in all exclusion, deportation, and removal proceedings before the Executive Office for Immigration Review.

(Pub. L. 107–296, title IV, §442, Nov. 25, 2002, 116 Stat. 2193; Pub. L. 118–96, §3(b)(2), Oct. 1, 2024, 138 Stat. 1571.)

AMENDMENT OF SECTION

For termination of amendment by section 6 of Pub. L. 118–96, see Termination Date of 2024 Amendment note below.

EDITORIAL NOTES

REFERENCES IN TEXT

Part E of this subchapter, referred to in subsecs. (a)(3)(C) and (b)(2)(B), was in the original "subtitle E", meaning subtitle E (§§451–462) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2195, which enacted part E (§271 et seq.) of this subchapter, amended sections 1356 and 1573 of Title 8, Aliens and Nationality, and enacted provisions set out as a note under section 271 of this title. For complete classification of subtitle E to the Code, see Tables.

AMENDMENTS

2024—Pub. L. 118–96, §§3(b)(2)(C), 6, temporarily substituted "U.S. Immigration and Customs Enforcement" for "the Bureau of Border Security" wherever appearing. See Termination Date of 2024 Amendment note below.

Pub. L. 118–96, §§3(b)(2)(A), 6, temporarily amended section catchline generally, substituting "U.S. Immigration and Customs Enforcement" for "Establishment of Bureau of Border Security". See Termination Date of 2024 Amendment note below.

Subsec. (a). Pub. L. 118–96, §§3(b)(2)(D)(i), 6, temporarily struck out "of Bureau" after "Establishment" in heading. See Termination Date of 2024 Amendment note below.

Subsec. (a)(3)(C). Pub. L. 118–96, §§3(b)(2)(D)(ii), 6, which directed the temporary substitution of "affecting U.S." for "affecting the Bureau of", was executed by making the temporary substitution for "that may affect the Bureau of" to reflect the probable intent of Congress. See Termination Date of 2024 Amendment note below.

Subsec. (a)(4). Pub. L. 118–96, §§3(b)(2)(D), 6, temporarily substituted "the agency." for "the Bureau." See Termination Date of 2024 Amendment note below.

Subsec. (a)(5)(A). Pub. L. 118–96, §§3(b)(2)(B), 6, temporarily substituted "agency" for "bureau" wherever appearing. See Termination Date of 2024 Amendment note below.

Subsec. (b)(2). Pub. L. 118–96, §§3(b)(2)(E)(i), 6, temporarily substituted "U.S. Immigration and Customs Enforcement" for "Bureau of Border Security" in introductory provisions. See Termination Date of 2024 Amendment note below.

Subsec. (b)(2)(B). Pub. L. 118–96, §§3(b)(2)(E)(ii), 6, temporarily substituted "U.S." for "the Bureau of". See Termination Date of 2024 Amendment note below.

Subsec. (c). Pub. L. 118–96, §§3(b)(2)(B), 6, temporarily substituted "agency" for "bureau". See Termination Date of 2024 Amendment note below.

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION DATE OF 2024 AMENDMENT

Pub. L. 118–96, §6, Oct. 1, 2024, 138 Stat. 1572, provided that: "This Act [enacting section 258 of this title, amending this section and section 253 of this title and enacting provisions set out as a note under section 258 of this title] and the amendments made by this Act shall cease to have force or effect beginning on October 1,

2030."

CHANGE OF NAME

Bureau of Border Security, referred to in section catchline and text, changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§253. Professional responsibility and quality review

The Secretary shall be responsible for—

(1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving any employee of U.S. Immigration and Customs Enforcement that are not subject to investigation by the Inspector General for the Department;

(2) inspecting the operations of U.S. Immigration and Customs Enforcement and providing assessments of the quality of the operations of such agency as a whole and each of its components; and

(3) providing an analysis of the management of U.S. Immigration and Customs Enforcement.

(Pub. L. 107–296, title IV, §443, Nov. 25, 2002, 116 Stat. 2194; Pub. L. 114–125, title VIII, §802(g)(1)(B)(v)(II), Feb. 24, 2016, 130 Stat. 212; Pub. L. 118–96, §3(b)(3), Oct. 1, 2024, 138 Stat. 1571.)

AMENDMENT OF SECTION

For termination of amendment by section 6 of Pub. L. 118–96, see Termination Date of 2024 Amendment note below.

EDITORIAL NOTES

AMENDMENTS

2024—Par. (2). Pub. L. 118–96, §§3(b)(3), 6, temporarily substituted "such agency" for "such bureau". See Termination Date of 2024 Amendment note below.

2016—Pub. L. 114–125 substituted "Secretary" for "Under Secretary for Border and Transportation Security" in introductory provisions and "U.S. Immigration and Customs Enforcement" for "the Bureau of Border Security" in pars. (1) to (3).

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION DATE OF 2024 AMENDMENT

Amendment by Pub. L. 118–96 to cease to have force or effect beginning on Oct. 1, 2030, see section 6 of Pub. L. 118–96, set out as a note under section 252 of this title.

§254. Employee discipline

Notwithstanding any other provision of law, the Secretary may impose disciplinary action on any employee of U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection who willfully deceives Congress or agency leadership on any matter.

(Pub. L. 107–296, title IV, §444, Nov. 25, 2002, 116 Stat. 2194; Pub. L. 114–125, title VIII, §802(g)(1)(B)(v)(III), Feb. 24, 2016, 130 Stat. 212.)

EDITORIAL NOTES

AMENDMENTS

2016—Pub. L. 114–125 amended section generally. Prior to amendment, text read as follows: "The Under

Secretary for Border and Transportation Security may, notwithstanding any other provision of law, impose disciplinary action, including termination of employment, pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation, on any employee of the Bureau of Border Security who willfully deceives the Congress or agency leadership on any matter."

§255. Report on improving enforcement functions

(a) In general

The Secretary, not later than 1 year after being sworn into office, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report with a plan detailing how the Bureau of Border Security, after the transfer of functions specified under section 251 of this title takes effect, will enforce comprehensively, effectively, and fairly all the enforcement provisions of the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) relating to such functions.

(b) Consultation

In carrying out subsection (a), the Secretary of Homeland Security shall consult with the Attorney General, the Secretary of State, the Director of the Federal Bureau of Investigation, the Secretary of the Treasury, the Secretary of Labor, the Commissioner of Social Security, the Director of the Executive Office for Immigration Review, and the heads of State and local law enforcement agencies to determine how to most effectively conduct enforcement operations.

(Pub. L. 107–296, title IV, §445, Nov. 25, 2002, 116 Stat. 2194.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Immigration and Nationality Act, referred to in subsec. (a), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (a), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§256. Sense of Congress regarding construction of fencing near San Diego, California

It is the sense of the Congress that completing the 14-mile border fence project required to be carried out under section 102(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) should be a priority for the Secretary.

(Pub. L. 107–296, title IV, §446, Nov. 25, 2002, 116 Stat. 2195.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 102(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, referred to in text, is section 102(b) of title I of div. C of Pub. L. 104–208, which is set out as a note under section 1103 of Title 8, Aliens and Nationality.

§257. Report

(a) In general

The Secretary of Homeland Security shall submit an annual report to the congressional committees set forth in subsection (b) that includes a description of—

(1) the cross-border tunnels along the border between Mexico and the United States discovered during the preceding fiscal year; and

(2) the needs of the Department of Homeland Security to effectively prevent, investigate and prosecute border tunnel construction along the border between Mexico and the United States.

(b) Congressional committees

The congressional committees set forth in this subsection are—

(1) the Committee on Homeland Security and Governmental Affairs of the Senate;

(2) the Committee on the Judiciary of the Senate;

(3) the Committee on Appropriations of the Senate;

(4) the Committee on Homeland Security of the House of Representatives;

(5) the Committee on the Judiciary of the House of Representatives; and

(6) the Committee on Appropriations of the House of Representatives.

(Pub. L. 112–127, §8, June 5, 2012, 126 Stat. 371.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Border Tunnel Prevention Act of 2012, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DHS ILLICIT CROSS-BORDER TUNNEL DEFENSE

Pub. L. 117–263, div. G, title LXXI, §7134, Dec. 23, 2022, 136 Stat. 3649, provided that:

"(a) COUNTER ILLICIT CROSS-BORDER TUNNEL OPERATIONS STRATEGIC PLAN.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2022], the Commissioner of U.S. Customs and Border Protection, in coordination with the Under Secretary for Science and Technology, and, as appropriate, other officials of the Department of Homeland Security, shall develop a counter illicit cross-border tunnel operations strategic plan (in this section referred to as the 'strategic plan') to address the following:

"(A) Risk-based criteria to be used to prioritize the identification, breach, assessment, and remediation of illicit cross-border tunnels.

"(B) Promote the use of innovative technologies to identify, breach, assess, and remediate illicit cross-border tunnels in a manner that, among other considerations, reduces the impact of such activities on surrounding communities.

"(C) Processes to share relevant illicit cross-border tunnel location, operations, and technical information.

"(D) Indicators of specific types of illicit cross-border tunnels found in each U.S. Border Patrol sector identified through operations to be periodically disseminated to U.S. Border Patrol sector chiefs to educate field personnel.

"(E) A counter illicit cross-border tunnel operations resource needs assessment that includes consideration of the following:

"(i) Technology needs.

"(ii) Staffing needs, including the following:

"(I) A position description for counter illicit cross-border tunnel operations personnel.

"(II) Any specialized skills required of such personnel.

"(III) The number of such full time personnel, disaggregated by U.S. Border Patrol sector.

"(2) REPORT TO CONGRESS ON STRATEGIC PLAN.—Not later than one year after the development of the strategic plan, the Commissioner of U.S. Customs and Border Protection shall submit to

the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the implementation of the strategic plan.

"(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commissioner of U.S. Customs and Border Protection $1,000,000 for each of fiscal years 2023 and 2024 to carry out—

"(1) the development of the strategic plan; and

"(2) remediation operations of illicit cross-border tunnels in accordance with the strategic plan to the maximum extent practicable."

§258. Homeland Security Investigations Victim Assistance Program

(a) Definitions

In this section:

(1) Forensic interview specialist

The term "forensic interview specialist" is an interview professional who has specialized experience and training in conducting trauma-informed forensic interviews with victims of crime.

(2) Victim

The term "victim" has the meaning given such term in section 20141(e)(2) of title 34.

(3) Victim assistance specialist

The term "victim assistance specialist" is a victim assistance professional who—

(A) has experience working with victims of crime in a service capacity;

(B) has been trained on the exposure of various forms of trauma and other stressors experienced in working with victims; and

(C) may have experience working with local government and community-based organizations, including victim advocacy centers, child advocacy centers, child welfare agencies, faith-based organizations, and other social service programs.

(b) In general

There is established, in Homeland Security Investigations of U.S. Immigration and Customs Enforcement, the Victim Assistance Program.

(c) Functions

The Victim Assistance Program shall—

(1) provide oversight, guidance, training, travel, equipment, and coordination to Homeland Security Investigations victim assistance personnel throughout the United States;

(2) recruit not fewer than—

(A) 1 forensic interview specialist and 1 victim assistance specialist for each Homeland Security Investigations Special Agent in Charge office;

(B) 1 victim assistance specialist for—

(i) every Homeland Security Investigations office participating in a human trafficking task force; and

(ii) every Homeland Security Investigations office participating in a child sexual exploitation task force;

(3) support Homeland Security Investigations regional attaché offices, to the extent necessary;

(4) provide training regarding victims' rights, victim-related policies, roles of forensic interviewers and victim assistance specialists, and an approach that is—

(A) victim-centered;

(B) trauma-informed; and

(C) linguistically appropriate, to the extent feasible; and

(5) purchase emergency items that are needed to assist identified victims in Homeland Security

Investigations criminal investigations, including food, clothing, hygiene products, transportation, and temporary shelter that is not otherwise provided by a nongovernmental organization.

(Pub. L. 107–296, title IV, §447, as added Pub. L. 118–96, §3(a), Oct. 1, 2024, 138 Stat. 1570.)

TERMINATION OF SECTION

For termination of section by section 6 of Pub. L. 118–96, see Termination Date note below.

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION DATE

Section to cease to be effective Oct. 1, 2030, see section 6 of Pub. L. 118–96, set out as a Termination Date of 2024 Amendment note under section 252 of this title.

INVESTIGATORS MAINTAIN PURPOSEFUL AWARENESS TO COMBAT TRAFFICKING TRAUMA PROGRAM

Pub. L. 118–96, §2, Oct. 1, 2024, 138 Stat. 1569, provided that:

"(a) ESTABLISHMENT.—There is established, in Homeland Security Investigations of U.S. Immigration and Customs Enforcement, the Investigators Maintain Purposeful Awareness to Combat Trafficking Trauma Program (referred to in this Act [see Short Title of 2024 Amendment note set out under section 101 of this title] as the 'IMPACTT Program').

"(b) FUNCTIONS.—The IMPACTT Program shall—

"(1) provide outreach and training to Homeland Security Investigations employees who have been exposed to various forms of trauma in working with victims of human trafficking, including—

"(A) self-awareness training for the relevant employees on recognizing the signs of burnout, compassion fatigue, critical incident stress, traumatic stress, posttraumatic stress, secondary traumatic stress, and vicarious trauma;

"(B) training material that—

"(i) provides mechanisms for self-care and resilience and notification of resources that are available through U.S. Immigration and Customs Enforcement, such as the Employee Assistance Program, the Peer Support Program, the Chaplain Program, and other relevant accredited programs that are available; and

"(ii) provides examples of potential resources that are available outside of U.S. Immigration and Customs Enforcement, which may include, faith-based and community-based resources; and

"(C) provide [sic] additional training to first line supervisors of relevant employees on recognizing the signs referred to in subparagraph (A) and the appropriate responses to employees exhibiting such signs;

"(2) include training modules that are carried out by—

"(A) licensed and accredited clinicians who—

"(i) have been trained on the exposure of various forms of trauma and other stressors experienced in working with victims; and

"(ii) may have experience working with faith-based organizations, community-based organizations, counseling programs, or other social service programs; and

"(B) additional subject matter experts who are available; and

"(3) be overseen and coordinated by the Department of Homeland Security Center for Countering Human Trafficking to ensure that—

"(A) appropriate program materials are distributed;

"(B) training is offered to all relevant employees; and

"(C) any needed travel and equipment is provided."

PART E—CITIZENSHIP AND IMMIGRATION SERVICES

§271. Establishment of Bureau of Citizenship and Immigration Services

(a) Establishment of Bureau

(1) In general

There shall be in the Department a bureau to be known as the "Bureau of Citizenship and Immigration Services".

(2) Director

The head of the Bureau of Citizenship and Immigration Services shall be the Director of the Bureau of Citizenship and Immigration Services, who—

(A) shall report directly to the Deputy Secretary;

(B) shall have a minimum of 5 years of management experience; and

(C) shall be paid at the same level as the Assistant Secretary of the Bureau of Border Security.

(3) Functions

The Director of the Bureau of Citizenship and Immigration Services—

(A) shall establish the policies for performing such functions as are transferred to the Director by this section or this chapter or otherwise vested in the Director by law;

(B) shall oversee the administration of such policies;

(C) shall advise the Deputy Secretary with respect to any policy or operation of the Bureau of Citizenship and Immigration Services that may affect the Bureau of Border Security of the Department, including potentially conflicting policies or operations;

(D) shall establish national immigration services policies and priorities;

(E) shall meet regularly with the Ombudsman described in section 272 of this title to correct serious service problems identified by the Ombudsman; and

(F) shall establish procedures requiring a formal response to any recommendations submitted in the Ombudsman's annual report to Congress within 3 months after its submission to Congress.

(4) Managerial rotation program

(A) In general

Not later than 1 year after the effective date specified in section 455,[1] the Director of the Bureau of Citizenship and Immigration Services shall design and implement a managerial rotation program under which employees of such bureau holding positions involving supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, as a GS–14 or above, shall—

(i) gain some experience in all the major functions performed by such bureau; and

(ii) work in at least one field office and one service center of such bureau.

(B) Report

Not later than 2 years after the effective date specified in section 455,[1] the Secretary shall submit a report to Congress on the implementation of such program.

(5) Pilot initiatives for backlog elimination

The Director of the Bureau of Citizenship and Immigration Services is authorized to implement innovative pilot initiatives to eliminate any remaining backlog in the processing of immigration benefit applications, and to prevent any backlog in the processing of such applications from recurring, in accordance with section 1573(a) of title 8. Such initiatives may include measures such as increasing personnel, transferring personnel to focus on areas with the largest potential for backlog, and streamlining paperwork.

(b) Transfer of functions from Commissioner

In accordance with subchapter XII (relating to transition provisions), there are transferred from the Commissioner of Immigration and Naturalization to the Director of the Bureau of Citizenship and

Immigration Services the following functions, and all personnel, infrastructure, and funding provided to the Commissioner in support of such functions immediately before the effective date specified in section 455: [1]

(1) Adjudications of immigrant visa petitions.
(2) Adjudications of naturalization petitions.
(3) Adjudications of asylum and refugee applications.
(4) Adjudications performed at service centers.
(5) All other adjudications performed by the Immigration and Naturalization Service immediately before the effective date specified in section 455.[1]

(c) Chief of Policy and Strategy

(1) In general

There shall be a position of Chief of Policy and Strategy for the Bureau of Citizenship and Immigration Services.

(2) Functions

In consultation with Bureau of Citizenship and Immigration Services personnel in field offices, the Chief of Policy and Strategy shall be responsible for—

(A) making policy recommendations and performing policy research and analysis on immigration services issues; and

(B) coordinating immigration policy issues with the Chief of Policy and Strategy for the Bureau of Border Security of the Department.

(d) Legal advisor

(1) In general

There shall be a principal legal advisor to the Director of the Bureau of Citizenship and Immigration Services.

(2) Functions

The legal advisor shall be responsible for—

(A) providing specialized legal advice, opinions, determinations, regulations, and any other assistance to the Director of the Bureau of Citizenship and Immigration Services with respect to legal matters affecting the Bureau of Citizenship and Immigration Services; and

(B) representing the Bureau of Citizenship and Immigration Services in visa petition appeal proceedings before the Executive Office for Immigration Review.

(e) Budget Officer

(1) In general

There shall be a Budget Officer for the Bureau of Citizenship and Immigration Services.

(2) Functions

(A) [2] In general

The Budget Officer shall be responsible for—

(i) formulating and executing the budget of the Bureau of Citizenship and Immigration Services;

(ii) financial management of the Bureau of Citizenship and Immigration Services; and

(iii) collecting all payments, fines, and other debts for the Bureau of Citizenship and Immigration Services.

(f) Chief of Office of Citizenship

(1) In general

There shall be a position of Chief of the Office of Citizenship for the Bureau of Citizenship and Immigration Services.

(2) Functions

The Chief of the Office of Citizenship for the Bureau of Citizenship and Immigration Services shall be responsible for promoting instruction and training on citizenship responsibilities for aliens interested in becoming naturalized citizens of the United States, including the development of educational materials.

(Pub. L. 107–296, title IV, §451, Nov. 25, 2002, 116 Stat. 2195; Pub. L. 110–382, §2(a), Oct. 9, 2008, 122 Stat. 4087.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (a)(3)(A), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

For the effective date specified in section 455, referred to in subsecs. (a)(4) and (b), see Effective Date note below.

AMENDMENTS

2008—Subsec. (g). Pub. L. 110–382, §§2(a), 4, temporarily added subsec. (g) which established an Office of the FBI Liaison in the Department of Homeland Security, defined its functions, and authorized appropriations. See Termination Date of 2008 Amendment note below.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsecs. (a)(2)(C), (3)(C), and (c)(2)(B), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

TERMINATION DATE OF 2008 AMENDMENT

Pub. L. 110–382, §4, Oct. 9, 2008, 122 Stat. 4089, provided that: "This Act [amending this section and section 1439 of Title 8, Aliens and Nationality, and enacting provisions set out as notes under this section and section 1101 of Title 8] and the amendments made by this Act are repealed on the date that is 5 years after the date of the enactment of this Act [Oct. 9, 2008]."

EFFECTIVE DATE

Pub. L. 107–296, title IV, §455, Nov. 25, 2002, 116 Stat. 2200, provided that: "Notwithstanding section 4 [enacting provisions set out as a note under section 101 of this title], sections 451 through 456 [enacting this section and sections 272 to 275 of this title], and the amendments made by such sections, shall take effect on the date on which the transfer of functions specified under section 441 [enacting section 251 of this title] takes effect." [For date on which transfer of functions specified under section 441 takes effect, see section 251 of this title and Department of Homeland Security Reorganization Plan, Nov. 25, 2002, set out as a note under section 542 of this title.]

RULEMAKING

Pub. L. 110–382, §2(b), Oct. 9, 2008, 122 Stat. 4087, which required the Secretary of Homeland Security, in consultation with the Attorney General, to promulgate rules to carry out the amendment made by section 2(a) of Pub. L. 110–382 no later than 180 days after Oct. 9, 2008, was repealed by Pub. L. 110–382, §4, Oct. 9, 2008, 122 Stat. 4089, effective 5 years after Oct. 9, 2008.

[1] *See References in Text note below.*

[2] *So in original. There is no subpar. (B).*

§272. Citizenship and Immigration Services Ombudsman

(a) In general

Within the Department, there shall be a position of Citizenship and Immigration Services Ombudsman (in this section referred to as the "Ombudsman"). The Ombudsman shall report directly to the Deputy Secretary. The Ombudsman shall have a background in customer service as well as immigration law.

(b) Functions

It shall be the function of the Ombudsman—

(1) to assist individuals and employers in resolving problems with the Bureau of Citizenship and Immigration Services;

(2) to identify areas in which individuals and employers have problems in dealing with the Bureau of Citizenship and Immigration Services; and

(3) to the extent possible, to propose changes in the administrative practices of the Bureau of Citizenship and Immigration Services to mitigate problems identified under paragraph (2).

(c) Annual reports

(1) Objectives

Not later than June 30 of each calendar year, the Ombudsman shall report to the Committee on the Judiciary of the House of Representatives and the Senate on the objectives of the Office of the Ombudsman for the fiscal year beginning in such calendar year. Any such report shall contain full and substantive analysis, in addition to statistical information, and—

(A) shall identify the recommendations the Office of the Ombudsman has made on improving services and responsiveness of the Bureau of Citizenship and Immigration Services;

(B) shall contain a summary of the most pervasive and serious problems encountered by individuals and employers, including a description of the nature of such problems;

(C) shall contain an inventory of the items described in subparagraphs (A) and (B) for which action has been taken and the result of such action;

(D) shall contain an inventory of the items described in subparagraphs (A) and (B) for which action remains to be completed and the period during which each item has remained on such inventory;

(E) shall contain an inventory of the items described in subparagraphs (A) and (B) for which no action has been taken, the period during which each item has remained on such inventory, the reasons for the inaction, and shall identify any official of the Bureau of Citizenship and Immigration Services who is responsible for such inaction;

(F) shall contain recommendations for such administrative action as may be appropriate to resolve problems encountered by individuals and employers, including problems created by excessive backlogs in the adjudication and processing of immigration benefit petitions and applications; and

(G) shall include such other information as the Ombudsman may deem advisable.

(2) Report to be submitted directly

Each report required under this subsection shall be provided directly to the committees described in paragraph (1) without any prior comment or amendment from the Secretary, Deputy Secretary, Director of the Bureau of Citizenship and Immigration Services, or any other officer or employee of the Department or the Office of Management and Budget.

(d) Other responsibilities

The Ombudsman—

(1) shall monitor the coverage and geographic allocation of local offices of the Ombudsman;

(2) shall develop guidance to be distributed to all officers and employees of the Bureau of Citizenship and Immigration Services outlining the criteria for referral of inquiries to local offices of the Ombudsman;

(3) shall ensure that the local telephone number for each local office of the Ombudsman is published and available to individuals and employers served by the office; and

(4) shall meet regularly with the Director of the Bureau of Citizenship and Immigration Services to identify serious service problems and to present recommendations for such administrative action as may be appropriate to resolve problems encountered by individuals and employers.

(e) Personnel actions

(1) In general

The Ombudsman shall have the responsibility and authority—

(A) to appoint local ombudsmen and make available at least 1 such ombudsman for each State; and

(B) to evaluate and take personnel actions (including dismissal) with respect to any employee of any local office of the Ombudsman.

(2) Consultation

The Ombudsman may consult with the appropriate supervisory personnel of the Bureau of Citizenship and Immigration Services in carrying out the Ombudsman's responsibilities under this subsection.

(f) Responsibilities of Bureau of Citizenship and Immigration Services

The Director of the Bureau of Citizenship and Immigration Services shall establish procedures requiring a formal response to all recommendations submitted to such director by the Ombudsman within 3 months after submission to such director.

(g) Operation of local offices

(1) In general

Each local ombudsman—

(A) shall report to the Ombudsman or the delegate thereof;

(B) may consult with the appropriate supervisory personnel of the Bureau of Citizenship and Immigration Services regarding the daily operation of the local office of such ombudsman;

(C) shall, at the initial meeting with any individual or employer seeking the assistance of such local office, notify such individual or employer that the local offices of the Ombudsman operate independently of any other component of the Department and report directly to Congress through the Ombudsman; and

(D) at the local ombudsman's discretion, may determine not to disclose to the Bureau of Citizenship and Immigration Services contact with, or information provided by, such individual or employer.

(2) Maintenance of independent communications

Each local office of the Ombudsman shall maintain a phone, facsimile, and other means of electronic communication access, and a post office address, that is separate from those maintained by the Bureau of Citizenship and Immigration Services, or any component of the Bureau of Citizenship and Immigration Services.

(Pub. L. 107–296, title IV, §452, Nov. 25, 2002, 116 Stat. 2197.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective on the date on which the transfer of functions specified under section 251 of this title takes effect, see section 455 of Pub. L. 107–296, set out as a note under section 271 of this title.

§273. Professional responsibility and quality review

(a) In general

The Director of the Bureau of Citizenship and Immigration Services shall be responsible for—

(1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving any employee of the Bureau of Citizenship and Immigration Services that are not subject to investigation by the Inspector General for the Department;

(2) inspecting the operations of the Bureau of Citizenship and Immigration Services and providing assessments of the quality of the operations of such bureau as a whole and each of its components; and

(3) providing an analysis of the management of the Bureau of Citizenship and Immigration Services.

(b) Special considerations

In providing assessments in accordance with subsection (a)(2) with respect to a decision of the Bureau of Citizenship and Immigration Services, or any of its components, consideration shall be given to—

(1) the accuracy of the findings of fact and conclusions of law used in rendering the decision;

(2) any fraud or misrepresentation associated with the decision; and

(3) the efficiency with which the decision was rendered.

(Pub. L. 107–296, title IV, §453, Nov. 25, 2002, 116 Stat. 2199.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective on the date on which the transfer of functions specified under section 251 of this title takes effect, see section 455 of Pub. L. 107–296, set out as a note under section 271 of this title.

§274. Employee discipline

The Director of the Bureau of Citizenship and Immigration Services may, notwithstanding any other provision of law, impose disciplinary action, including termination of employment, pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation, on any employee of the Bureau of Citizenship and Immigration Services who willfully deceives Congress or agency leadership on any matter.

(Pub. L. 107–296, title IV, §454, Nov. 25, 2002, 116 Stat. 2200.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective on the date on which the transfer of functions specified under section 251 of this title takes effect, see section 455 of Pub. L. 107–296, set out as a note under section 271 of this title.

§275. Transition

(a) References

With respect to any function transferred by this part to, and exercised on or after the effective date specified in section 455 [1] by, the Director of the Bureau of Citizenship and Immigration Services, any reference in any other Federal law, Executive order, rule, regulation, or delegation of authority, or any document of or pertaining to a component of government from which such function is transferred—

(1) to the head of such component is deemed to refer to the Director of the Bureau of Citizenship and Immigration Services; or

(2) to such component is deemed to refer to the Bureau of Citizenship and Immigration Services.

(b) Other transition issues

(1) Exercise of authorities

Except as otherwise provided by law, a Federal official to whom a function is transferred by this part may, for purposes of performing the function, exercise all authorities under any other provision of law that were available with respect to the performance of that function to the official responsible for the performance of the function immediately before the effective date specified in section 455.[1]

(2) Transfer and allocation of appropriations and personnel

The personnel of the Department of Justice employed in connection with the functions transferred by this part (and functions that the Secretary determines are properly related to the functions of the Bureau of Citizenship and Immigration Services), and the assets, liabilities, contracts, property, records, and unexpended balance of appropriations, authorizations, allocations, and other funds employed, held, used, arising from, available to, or to be made available to, the Immigration and Naturalization Service in connection with the functions transferred by this part, subject to section 1531 of title 31, shall be transferred to the Director of the Bureau of Citizenship and Immigration Services for allocation to the appropriate component of the Department. Unexpended funds transferred pursuant to this paragraph shall be used only for the purposes for which the funds were originally authorized and appropriated. The Secretary shall have the right to adjust or realign transfers of funds and personnel effected pursuant to this part for a period of 2 years after the effective date specified in section 455.[1]

(Pub. L. 107–296, title IV, §456, Nov. 25, 2002, 116 Stat. 2200.)

EDITORIAL NOTES

REFERENCES IN TEXT

This part, referred to in text, was in the original "this subtitle", meaning subtitle E (§§451–462) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2195, which enacted this part, amended sections 1356 and 1573 of Title 8, Aliens and Nationality, and enacted provisions set out as a note under section 271 of this title. For complete classification of subtitle E to the Code, see Tables.

For the effective date specified in section 455, referred to in text, see section 455 of Pub. L. 107–296, set out as an Effective Date note under section 271 of this title.

CODIFICATION

In subsec. (b)(2), "section 1531 of title 31" substituted for "section 202 of the Budget and Accounting Procedures Act of 1950" on authority of Pub. L. 97–258, §4(b), Sept. 13, 1982, 96 Stat. 1067, the first section of which enacted Title 31, Money and Finance.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective on the date on which the transfer of functions specified under section 251 of this title takes effect, see section 455 of Pub. L. 107–296, set out as a note under section 271 of this title.

[1] *See References in Text note below.*

§276. Report on improving immigration services

(a) In general

The Secretary, not later than 1 year after the effective date of this chapter, shall submit to the

Committees on the Judiciary and Appropriations of the House of Representatives and of the Senate a report with a plan detailing how the Bureau of Citizenship and Immigration Services, after the transfer of functions specified in this part takes effect, will complete efficiently, fairly, and within a reasonable time, the adjudications described in paragraphs (1) through (5) of section 271(b) of this title.

(b) Contents

For each type of adjudication to be undertaken by the Director of the Bureau of Citizenship and Immigration Services, the report shall include the following:

(1) Any potential savings of resources that may be implemented without affecting the quality of the adjudication.

(2) The goal for processing time with respect to the application.

(3) Any statutory modifications with respect to the adjudication that the Secretary considers advisable.

(c) Consultation

In carrying out subsection (a), the Secretary shall consult with the Secretary of State, the Secretary of Labor, the Assistant Secretary of the Bureau of Border Security of the Department, and the Director of the Executive Office for Immigration Review to determine how to streamline and improve the process for applying for and making adjudications described in section 271(b) of this title and related processes.

(Pub. L. 107–296, title IV, §459, Nov. 25, 2002, 116 Stat. 2201.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsec. (a), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (c), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§277. Report on responding to fluctuating needs

Not later than 30 days after November 25, 2002, the Attorney General shall submit to Congress a report on changes in law, including changes in authorizations of appropriations and in appropriations, that are needed to permit the Immigration and Naturalization Service, and, after the transfer of functions specified in this part takes effect, the Bureau of Citizenship and Immigration Services of the Department, to ensure a prompt and timely response to emergent, unforeseen, or impending changes in the number of applications for immigration benefits, and otherwise to ensure the accommodation of changing immigration service needs.

(Pub. L. 107–296, title IV, §460, Nov. 25, 2002, 116 Stat. 2201.)

§278. Application of Internet-based technologies

(a) Establishment of tracking system

The Secretary, not later than 1 year after the effective date of this chapter, in consultation with the Technology Advisory Committee established under subsection (c), shall establish an Internet-based

system, that will permit a person, employer, immigrant, or nonimmigrant who has filings with the Secretary for any benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.), access to online information about the processing status of the filing involved.

(b) Feasibility study for online filing and improved processing

(1) Online filing

The Secretary, in consultation with the Technology Advisory Committee established under subsection (c), shall conduct a feasibility study on the online filing of the filings described in subsection (a). The study shall include a review of computerization and technology of the Immigration and Naturalization Service relating to the immigration services and processing of filings related to immigrant services. The study shall also include an estimate of the timeframe and cost and shall consider other factors in implementing such a filing system, including the feasibility of fee payment online.

(2) Report

A report on the study under this subsection shall be submitted to the Committees on the Judiciary of the House of Representatives and the Senate not later than 1 year after the effective date of this chapter.

(c) Technology Advisory Committee

(1) Establishment

The Secretary shall establish, not later than 60 days after the effective date of this chapter, an advisory committee (in this section referred to as the "Technology Advisory Committee") to assist the Secretary in—

(A) establishing the tracking system under subsection (a); and

(B) conducting the study under subsection (b).

The Technology Advisory Committee shall be established after consultation with the Committees on the Judiciary of the House of Representatives and the Senate.

(2) Composition

The Technology Advisory Committee shall be composed of representatives from high technology companies capable of establishing and implementing the system in an expeditious manner, and representatives of persons who may use the tracking system described in subsection (a) and the online filing system described in subsection (b)(1).

(Pub. L. 107–296, title IV, §461, Nov. 25, 2002, 116 Stat. 2202.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsecs. (a), (b)(2), and (c)(1), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

The Immigration and Nationality Act, referred to in subsec. (a), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION OF ADVISORY COMMITTEES

Advisory committees established after Jan. 5, 1973, to terminate not later than the expiration of the 2-year period beginning on date of their establishment, unless, in the case of a committee established by the President or an officer of the Federal Government, such committee is renewed by appropriate action prior to expiration of such 2-year period, or in the case of a committee established by Congress, its duration is otherwise provided for by law. See section 1013 of Title 5, Government Organization and Employees.

§279. Children's affairs

(a) Transfer of functions

There are transferred to the Director of the Office of Refugee Resettlement of the Department of Health and Human Services functions under the immigration laws of the United States with respect to the care of unaccompanied alien children that were vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or any officer, employee, or component of the Immigration and Naturalization Service) immediately before the effective date specified in subsection (d).

(b) Functions

(1) In general

Pursuant to the transfer made by subsection (a), the Director of the Office of Refugee Resettlement shall be responsible for—

(A) coordinating and implementing the care and placement of unaccompanied alien children who are in Federal custody by reason of their immigration status, including developing a plan to be submitted to Congress on how to ensure that qualified and independent legal counsel is timely appointed to represent the interests of each such child, consistent with the law regarding appointment of counsel that is in effect on November 25, 2002;

(B) ensuring that the interests of the child are considered in decisions and actions relating to the care and custody of an unaccompanied alien child;

(C) making placement determinations for all unaccompanied alien children who are in Federal custody by reason of their immigration status;

(D) implementing the placement determinations;

(E) implementing policies with respect to the care and placement of unaccompanied alien children;

(F) identifying a sufficient number of qualified individuals, entities, and facilities to house unaccompanied alien children;

(G) overseeing the infrastructure and personnel of facilities in which unaccompanied alien children reside;

(H) reuniting unaccompanied alien children with a parent abroad in appropriate cases;

(I) compiling, updating, and publishing at least annually a state-by-state list of professionals or other entities qualified to provide guardian and attorney representation services for unaccompanied alien children;

(J) maintaining statistical information and other data on unaccompanied alien children for whose care and placement the Director is responsible, which shall include—

(i) biographical information, such as a child's name, gender, date of birth, country of birth, and country of habitual residence;

(ii) the date on which the child came into Federal custody by reason of his or her immigration status;

(iii) information relating to the child's placement, removal, or release from each facility in which the child has resided;

(iv) in any case in which the child is placed in detention or released, an explanation relating to the detention or release; and

(v) the disposition of any actions in which the child is the subject;

(K) collecting and compiling statistical information from the Department of Justice, the Department of Homeland Security, and the Department of State on each department's actions relating to unaccompanied alien children; and

(L) conducting investigations and inspections of facilities and other entities in which unaccompanied alien children reside, including regular follow-up visits to such facilities, placements, and other entities, to assess the continued suitability of such placements.

(2) Coordination with other entities; no release on own recognizance

In making determinations described in paragraph (1)(C), the Director of the Office of Refugee Resettlement—

(A) shall consult with appropriate juvenile justice professionals, the Director of the Bureau of Citizenship and Immigration Services, and the Assistant Secretary of the Bureau of Border Security to ensure that such determinations ensure that unaccompanied alien children described in such subparagraph—

(i) are likely to appear for all hearings or proceedings in which they are involved;

(ii) are protected from smugglers, traffickers, or others who might seek to victimize or otherwise engage them in criminal, harmful, or exploitive activity; and

(iii) are placed in a setting in which they are not likely to pose a danger to themselves or others; and

(B) shall not release such children upon their own recognizance.

(3) Duties with respect to foster care

In carrying out the duties described in paragraph (1), the Director of the Office of Refugee Resettlement is encouraged to use the refugee children foster care system established pursuant to section 412(d) of the Immigration and Nationality Act (8 U.S.C. 1522(d)) for the placement of unaccompanied alien children.

(4) Rule of construction

Nothing in paragraph (2)(B) may be construed to require that a bond be posted for an unaccompanied alien child who is released to a qualified sponsor.

(c) Rule of construction

Nothing in this section may be construed to transfer the responsibility for adjudicating benefit determinations under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) from the authority of any official of the Department of Justice, the Department of Homeland Security, or the Department of State.

(d) Effective date

Notwithstanding section 4,[1] this section shall take effect on the date on which the transfer of functions specified under section 251 of this title takes effect.

(e) References

With respect to any function transferred by this section, any reference in any other Federal law, Executive order, rule, regulation, or delegation of authority, or any document of or pertaining to a component of government from which such function is transferred—

(1) to the head of such component is deemed to refer to the Director of the Office of Refugee Resettlement; or

(2) to such component is deemed to refer to the Office of Refugee Resettlement of the Department of Health and Human Services.

(f) Other transition issues

(1) Exercise of authorities

Except as otherwise provided by law, a Federal official to whom a function is transferred by this section may, for purposes of performing the function, exercise all authorities under any other provision of law that were available with respect to the performance of that function to the official responsible for the performance of the function immediately before the effective date specified in subsection (d).

(2) Savings provisions

Subsections (a), (b), and (c) of section 552 of this title shall apply to a transfer of functions under this section in the same manner as such provisions apply to a transfer of functions under this

chapter to the Department of Homeland Security.

(3) Transfer and allocation of appropriations and personnel

The personnel of the Department of Justice employed in connection with the functions transferred by this section, and the assets, liabilities, contracts, property, records, and unexpended balance of appropriations, authorizations, allocations, and other funds employed, held, used, arising from, available to, or to be made available to, the Immigration and Naturalization Service in connection with the functions transferred by this section, subject to section 1531 of title 31, shall be transferred to the Director of the Office of Refugee Resettlement for allocation to the appropriate component of the Department of Health and Human Services. Unexpended funds transferred pursuant to this paragraph shall be used only for the purposes for which the funds were originally authorized and appropriated.

(g) Definitions

As used in this section—

(1) the term "placement" means the placement of an unaccompanied alien child in either a detention facility or an alternative to such a facility; and

(2) the term "unaccompanied alien child" means a child who—

(A) has no lawful immigration status in the United States;

(B) has not attained 18 years of age; and

(C) with respect to whom—

(i) there is no parent or legal guardian in the United States; or

(ii) no parent or legal guardian in the United States is available to provide care and physical custody.

(Pub. L. 107–296, title IV, §462, Nov. 25, 2002, 116 Stat. 2202; Pub. L. 110–457, title II, §235(f), Dec. 23, 2008, 122 Stat. 5081.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Immigration and Nationality Act, referred to in subsec. (c), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

Section 4, referred to in subsec. (d), is section 4 of Pub. L. 107–296, which is set out as an Effective Date note under section 101 of this title.

This chapter, referred to in subsec. (f)(2), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

In subsec. (f)(3), "section 1531 of title 31" substituted for "section 202 of the Budget and Accounting Procedures Act of 1950" on authority of Pub. L. 97–258, §4(b), Sept. 13, 1982, 96 Stat. 1067, the first section of which enacted Title 31, Money and Finance.

AMENDMENTS

2008—Subsec. (b)(1)(L). Pub. L. 110–457, §235(f)(1), substituted ", including regular follow-up visits to such facilities, placements, and other entities, to assess the continued suitability of such placements." for period at end.

Subsec. (b)(3). Pub. L. 110–457, §235(f)(2)(A), substituted "paragraph (1)," for "paragraph (1)(G),".

Subsec. (b)(4). Pub. L. 110–457, §235(f)(2)(B), added par. (4).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (b)(2)(A), changed to Bureau of Immigration and Customs

Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

NOTIFICATION OF USE OF UNLICENSED INFLUX FACILITY

Pub. L. 119–75, div. B, title II, §232, Feb. 3, 2026, 140 Stat. 290, provided that: "In addition to the existing Congressional notification for formal site assessments of potential influx facilities, the Secretary [of Health and Human Services] shall notify the Committees on Appropriations of the House of Representatives and the Senate at least 15 days before operationalizing an unlicensed facility, and shall (1) specify whether the facility is hard-sided or soft-sided, and (2) provide analysis that indicates that, in the absence of the influx facility, the likely outcome is that unaccompanied alien children will remain in the custody of the Department of Homeland Security for longer than 72 hours or that unaccompanied alien children will be otherwise placed in danger. Within 60 days of bringing such a facility online, and monthly thereafter, the Secretary shall provide to the Committees on Appropriations of the House of Representatives and the Senate a report detailing the total number of children in care at the facility, the average length of stay and average length of care of children at the facility, and, for any child that has been at the facility for more than 60 days, their length of stay and reason for delay in release."

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 118–47, div. D, title II, §232, Mar. 23, 2024, 138 Stat. 679.
Pub. L. 117–328, div. H, title II, §232, Dec. 29, 2022, 136 Stat. 4886.
Pub. L. 117–103, div. H, title II, §232, Mar. 15, 2022, 136 Stat. 473.
Pub. L. 116–260, div. H, title II, §233, Dec. 27, 2020, 134 Stat. 1596.
Pub. L. 116–94, div. A, title II, §233, Dec. 20, 2019, 133 Stat. 2585.

REPORT ON CHILDREN SEPARATED FROM PARENTS OR LEGAL GUARDIANS

Pub. L. 119–75, div. B, title II, §234, Feb. 3, 2026, 140 Stat. 291, provided that: "Not later than 14 days after the date of enactment of this Act [Feb. 3, 2026], and monthly thereafter, the Secretary [of Health and Human Services] shall submit to the Committees on Appropriations of the House of Representatives and the Senate, and make publicly available online, a report with respect to children who were separated from their parents or legal guardians by the Department of Homeland Security (DHS) (regardless of whether or not such separation was pursuant to an option selected by the children, parents, or guardians), subsequently classified as unaccompanied alien children, and transferred to the care and custody of ORR [Office of Refugee Resettlement] during the previous month. Each report shall contain the following information:

"(1) the number and ages of children so separated subsequent to apprehension at or between ports of entry, to be reported by sector where separation occurred; and

"(2) the documented cause of separation, as reported by DHS when each child was referred."

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 118–47, div. D, title II, §234, Mar. 23, 2024, 138 Stat. 680.
Pub. L. 117–328, div. H, title II, §234, Dec. 29, 2022, 136 Stat. 4886.
Pub. L. 117–103, div. H, title II, §234, Mar. 15, 2022, 136 Stat. 473.
Pub. L. 116–260, div. H, title II, §235, Dec. 27, 2020, 134 Stat. 1597.
Pub. L. 116–94, div. A, title II, §235, Dec. 20, 2019, 133 Stat. 2585.

[1] *See References in Text note below.*

PART F—GENERAL IMMIGRATION PROVISIONS

§291. Abolishment of INS

(a) In general

Upon completion of all transfers from the Immigration and Naturalization Service as provided for by this chapter, the Immigration and Naturalization Service of the Department of Justice is abolished.

(b) Prohibition

The authority provided by section 542 of this title may be used to reorganize functions or organizational units within the Bureau of Border Security or the Bureau of Citizenship and Immigration Services, but may not be used to recombine the two bureaus into a single agency or otherwise to combine, join, or consolidate functions or organizational units of the two bureaus with each other.

(Pub. L. 107–296, title IV, §471, Nov. 25, 2002, 116 Stat. 2205.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (a), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (b), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§292. Voluntary separation incentive payments

(a) Definitions

For purposes of this section—

(1) the term "employee" means an employee (as defined by section 2105 of title 5) who—

(A) has completed at least 3 years of current continuous service with 1 or more covered entities; and

(B) is serving under an appointment without time limitation,

but does not include any person under subparagraphs (A)–(G) of section 663(a)(2) of Public Law 104–208 (5 U.S.C. 5597 note);

(2) the term "covered entity" means—

(A) the Immigration and Naturalization Service;

(B) the Bureau of Border Security of the Department of Homeland Security; and

(C) the Bureau of Citizenship and Immigration Services of the Department of Homeland Security; and

(3) the term "transfer date" means the date on which the transfer of functions specified under section 251 of this title takes effect.

(b) Strategic restructuring plan

Before the Attorney General or the Secretary obligates any resources for voluntary separation incentive payments under this section, such official shall submit to the appropriate committees of Congress a strategic restructuring plan, which shall include—

(1) an organizational chart depicting the covered entities after their restructuring pursuant to this chapter;

(2) a summary description of how the authority under this section will be used to help carry out that restructuring; and

(3) the information specified in section 663(b)(2) of Public Law 104–208 (5 U.S.C. 5597 note).

As used in the preceding sentence, the "appropriate committees of Congress" are the Committees

on Appropriations, Government Reform, and the Judiciary of the House of Representatives, and the Committees on Appropriations, Governmental Affairs, and the Judiciary of the Senate.

(c) Authority

The Attorney General and the Secretary may, to the extent necessary to help carry out their respective strategic restructuring plan described in subsection (b), make voluntary separation incentive payments to employees. Any such payment—

(1) shall be paid to the employee, in a lump sum, after the employee has separated from service;

(2) shall be paid from appropriations or funds available for the payment of basic pay of the employee;

(3) shall be equal to the lesser of—

(A) the amount the employee would be entitled to receive under section 5595(c) of title 5; or

(B) an amount not to exceed $25,000, as determined by the Attorney General or the Secretary;

(4) may not be made except in the case of any qualifying employee who voluntarily separates (whether by retirement or resignation) before the end of—

(A) the 3-month period beginning on the date on which such payment is offered or made available to such employee; or

(B) the 3-year period beginning on November 25, 2002,

whichever occurs first;

(5) shall not be a basis for payment, and shall not be included in the computation, of any other type of Government benefit; and

(6) shall not be taken into account in determining the amount of any severance pay to which the employee may be entitled under section 5595 of title 5, based on any other separation.

(d) Additional agency contributions to the retirement fund

(1) In general

In addition to any payments which it is otherwise required to make, the Department of Justice and the Department of Homeland Security shall, for each fiscal year with respect to which it makes any voluntary separation incentive payments under this section, remit to the Office of Personnel Management for deposit in the Treasury of the United States to the credit of the Civil Service Retirement and Disability Fund the amount required under paragraph (2).

(2) Amount required

The amount required under this paragraph shall, for any fiscal year, be the amount under subparagraph (A) or (B), whichever is greater.

(A) First method

The amount under this subparagraph shall, for any fiscal year, be equal to the minimum amount necessary to offset the additional costs to the retirement systems under title 5 (payable out of the Civil Service Retirement and Disability Fund) resulting from the voluntary separation of the employees described in paragraph (3), as determined under regulations of the Office of Personnel Management.

(B) Second method

The amount under this subparagraph shall, for any fiscal year, be equal to 45 percent of the sum total of the final basic pay of the employees described in paragraph (3).

(3) Computations to be based on separations occurring in the fiscal year involved

The employees described in this paragraph are those employees who receive a voluntary separation incentive payment under this section based on their separating from service during the fiscal year with respect to which the payment under this subsection relates.

(4) Final basic pay defined

In this subsection, the term "final basic pay" means, with respect to an employee, the total amount of basic pay which would be payable for a year of service by such employee, computed using the employee's final rate of basic pay, and, if last serving on other than a full-time basis, with appropriate adjustment therefor.

(e) Effect of subsequent employment with the Government

An individual who receives a voluntary separation incentive payment under this section and who, within 5 years after the date of the separation on which the payment is based, accepts any compensated employment with the Government or works for any agency of the Government through a personal services contract, shall be required to pay, prior to the individual's first day of employment, the entire amount of the incentive payment. Such payment shall be made to the covered entity from which the individual separated or, if made on or after the transfer date, to the Deputy Secretary or the Under Secretary for Border and Transportation Security (for transfer to the appropriate component of the Department of Homeland Security, if necessary).

(f) Effect on employment levels

(1) Intended effect

Voluntary separations under this section are not intended to necessarily reduce the total number of full-time equivalent positions in any covered entity.

(2) Use of voluntary separations

A covered entity may redeploy or use the full-time equivalent positions vacated by voluntary separations under this section to make other positions available to more critical locations or more critical occupations.

(Pub. L. 107–296, title IV, §472, Nov. 25, 2002, 116 Stat. 2205.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 663 of Public Law 104–208, referred to in subsecs. (a)(1) and (b)(3), probably means Pub. L. 104–208, div. A, title I, §101(f) [title VI, §663], Sept. 30, 1996, 110 Stat. 3009–314, 3009–383, which is classified as a note under section 5597 of Title 5, Government Organization and Employees.

This chapter, referred to in subsec. (b)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (a)(2)(B), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§293. Authority to conduct a demonstration project relating to disciplinary action

(a) In general

The Attorney General and the Secretary may each, during a period ending not later than 5 years after November 25, 2002, conduct a demonstration project for the purpose of determining whether one or more changes in the policies or procedures relating to methods for disciplining employees would result in improved personnel management.

(b) Scope

A demonstration project under this section—

(1) may not cover any employees apart from those employed in or under a covered entity; and

(2) shall not be limited by any provision of chapter 43, 75, or 77 of title 5.

(c) Procedures

Under the demonstration project—

(1) the use of alternative means of dispute resolution (as defined in section 571 of title 5) shall be encouraged, whenever appropriate; and

(2) each covered entity under the jurisdiction of the official conducting the project shall be required to provide for the expeditious, fair, and independent review of any action to which section 4303 or subchapter II of chapter 75 of such title 5 would otherwise apply (except an action described in section 7512(5) of such title 5).

(d) Actions involving discrimination

Notwithstanding any other provision of this section, if, in the case of any matter described in section 7702(a)(1)(B) of title 5, there is no judicially reviewable action under the demonstration project within 120 days after the filing of an appeal or other formal request for review (referred to in subsection (c)(2)), an employee shall be entitled to file a civil action to the same extent and in the same manner as provided in section 7702(e)(1) of such title 5 (in the matter following subparagraph (C) thereof).

(e) Certain employees

Employees shall not be included within any project under this section if such employees are—

(1) neither managers nor supervisors; and

(2) within a unit with respect to which a labor organization is accorded exclusive recognition under chapter 71 of title 5.

Notwithstanding the preceding sentence, an aggrieved employee within a unit (referred to in paragraph (2)) may elect to participate in a complaint procedure developed under the demonstration project in lieu of any negotiated grievance procedure and any statutory procedure (as such term is used in section 7121 of such title 5).

(f) Reports

The Government Accountability Office shall prepare and submit to the Committees on Government Reform and the Judiciary of the House of Representatives and the Committees on Governmental Affairs and the Judiciary of the Senate periodic reports on any demonstration project conducted under this section, such reports to be submitted after the second and fourth years of its operation. Upon request, the Attorney General or the Secretary shall furnish such information as the Government Accountability Office may require to carry out this subsection.

(g) Definition

In this section, the term "covered entity" has the meaning given such term in section 292(a)(2) of this title.

(Pub. L. 107–296, title IV, §473, Nov. 25, 2002, 116 Stat. 2208; Pub. L. 108–271, §8(b), July 7,

2004, 118 Stat. 814.)

EDITORIAL NOTES

AMENDMENTS

2004—Subsec. (f). Pub. L. 108–271 substituted "Government Accountability Office" for "General Accounting Office" in two places.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§294. Sense of Congress

It is the sense of Congress that—

(1) the missions of the Bureau of Border Security and the Bureau of Citizenship and Immigration Services are equally important and, accordingly, they each should be adequately funded; and

(2) the functions transferred under this part should not, after such transfers take effect, operate at levels below those in effect prior to November 25, 2002.

(Pub. L. 107–296, title IV, §474, Nov. 25, 2002, 116 Stat. 2209.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in par. (1), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§295. Director of Shared Services

(a) In general

Within the Office of Deputy Secretary, there shall be a Director of Shared Services.

(b) Functions

The Director of Shared Services shall be responsible for the coordination of resources for the Bureau of Border Security and the Bureau of Citizenship and Immigration Services, including—

(1) information resources management, including computer databases and information technology;

(2) records and file management; and

(3) forms management.

(Pub. L. 107–296, title IV, §475, Nov. 25, 2002, 116 Stat. 2209.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsec. (b), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§296. Separation of funding

(a) In general

There shall be established separate accounts in the Treasury of the United States for appropriated funds and other deposits available for the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(b) Separate budgets

To ensure that the Bureau of Citizenship and Immigration Services and the Bureau of Border Security are funded to the extent necessary to fully carry out their respective functions, the Director of the Office of Management and Budget shall separate the budget requests for each such entity.

(c) Fees

Fees imposed for a particular service, application, or benefit shall be deposited into the account established under subsection (a) that is for the bureau with jurisdiction over the function to which the fee relates.

(d) Fees not transferable

No fee may be transferred between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security for purposes not authorized by section 1356 of title 8.

(Pub. L. 107–296, title IV, §476, Nov. 25, 2002, 116 Stat. 2209.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in subsecs. (a), (b), and (d), changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§297. Reports and implementation plans

(a) Division of funds

The Secretary, not later than 120 days after the effective date of this chapter, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report on the proposed division and transfer of funds, including unexpended funds, appropriations, and fees, between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(b) Division of personnel

The Secretary, not later than 120 days after the effective date of this chapter, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report on the proposed division of personnel between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(c) Implementation plan

(1) In general

The Secretary, not later than 120 days after the effective date of this chapter, and every 6 months thereafter until the termination of fiscal year 2005, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate an implementation plan to carry out this chapter.

(2) Contents

The implementation plan should include details concerning the separation of the Bureau of Citizenship and Immigration Services and the Bureau of Border Security, including the following:

(A) Organizational structure, including the field structure.

(B) Chain of command.

(C) Procedures for interaction among such bureaus.

(D) Fraud detection and investigation.

(E) The processing and handling of removal proceedings, including expedited removal and applications for relief from removal.

(F) Recommendations for conforming amendments to the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(G) Establishment of a transition team.

(H) Methods to phase in the costs of separating the administrative support systems of the Immigration and Naturalization Service in order to provide for separate administrative support systems for the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(d) Comptroller General studies and reports

(1) Status reports on transition

Not later than 18 months after the date on which the transfer of functions specified under section 251 of this title takes effect, and every 6 months thereafter, until full implementation of this part has been completed, the Comptroller General of the United States shall submit to the Committees on Appropriations and on the Judiciary of the House of Representatives and the Senate a report containing the following:

(A) A determination of whether the transfers of functions made by parts D and E of this subchapter have been completed, and if a transfer of functions has not taken place, identifying the reasons why the transfer has not taken place.

(B) If the transfers of functions made by parts D and E of this subchapter have been completed, an identification of any issues that have arisen due to the completed transfers.

(C) An identification of any issues that may arise due to any future transfer of functions.

(2) Report on management

Not later than 4 years after the date on which the transfer of functions specified under section 251 of this title takes effect, the Comptroller General of the United States shall submit to the Committees on Appropriations and on the Judiciary of the House of Representatives and the Senate a report, following a study, containing the following:

(A) Determinations of whether the transfer of functions from the Immigration and Naturalization Service to the Bureau of Citizenship and Immigration Services and the Bureau of Border Security have improved, with respect to each function transferred, the following:

(i) Operations.

(ii) Management, including accountability and communication.

(iii) Financial administration.

(iv) Recordkeeping, including information management and technology.

(B) A statement of the reasons for the determinations under subparagraph (A).

(C) Any recommendations for further improvements to the Bureau of Citizenship and

Immigration Services and the Bureau of Border Security.

(3) Report on fees

Not later than 1 year after November 25, 2002, the Comptroller General of the United States shall submit to the Committees on the Judiciary of the House of Representatives and of the Senate a report examining whether the Bureau of Citizenship and Immigration Services is likely to derive sufficient funds from fees to carry out its functions in the absence of appropriated funds.

(Pub. L. 107–296, title IV, §477, Nov. 25, 2002, 116 Stat. 2209.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsecs. (a), (b), and (c)(1), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

This chapter, referred to in subsec. (c)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The Immigration and Nationality Act, referred to in subsec. (c)(2)(F), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

Parts D and E of this subchapter, referred to in subsec. (d)(1)(A), (B), was in the original "subtitles D and E", meaning subtitles D (§§441–446) and E (§§451–462) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2192, 2195, which enacted parts D and E of this subchapter, amended sections 1356 and 1573 of Title 8, Aliens and Nationality, and enacted provisions set out as a note under section 271 of this title. For complete classification of subtitles D and E to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Bureau of Border Security, referred to in text, changed to Bureau of Immigration and Customs Enforcement by Reorganization Plan Modification for the Department of Homeland Security, eff. Mar. 1, 2003, H. Doc. No. 108–32, 108th Congress, 1st Session, set out as a note under section 542 of this title.

§298. Immigration functions

(a) Annual report

(1) In general

One year after November 25, 2002, and each year thereafter, the Secretary shall submit a report to the President, to the Committees on the Judiciary and Government Reform of the House of Representatives, and to the Committees on the Judiciary and Government Affairs of the Senate, on the impact the transfers made by this part has had on immigration functions.

(2) Matter included

The report shall address the following with respect to the period covered by the report:

(A) The aggregate number of all immigration applications and petitions received, and processed, by the Department.

(B) Region-by-region statistics on the aggregate number of immigration applications and petitions filed by an alien (or filed on behalf of an alien) and denied, disaggregated by category of denial and application or petition type.

(C) The quantity of backlogged immigration applications and petitions that have been processed, the aggregate number awaiting processing, and a detailed plan for eliminating the backlog.

(D) The average processing period for immigration applications and petitions, disaggregated by application or petition type.

(E) The number and types of immigration-related grievances filed with any official of the Department of Justice, and if those grievances were resolved.

(F) Plans to address grievances and improve immigration services.

(G) Whether immigration-related fees were used consistent with legal requirements regarding such use.

(H) Whether immigration-related questions conveyed by customers to the Department (whether conveyed in person, by telephone, or by means of the Internet) were answered effectively and efficiently.

(b) Sense of Congress regarding immigration services

It is the sense of Congress that—

(1) the quality and efficiency of immigration services rendered by the Federal Government should be improved after the transfers made by this part take effect; and

(2) the Secretary should undertake efforts to guarantee that concerns regarding the quality and efficiency of immigration services are addressed after such effective date.

(Pub. L. 107–296, title IV, §478, Nov. 25, 2002, 116 Stat. 2211.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

PART G—U.S. CUSTOMS AND BORDER PROTECTION PUBLIC PRIVATE PARTNERSHIPS

§301. Fee agreements for certain services at ports of entry

(a) In general

Notwithstanding section 58c(e) of title 19 and section 1451 of title 19, the Commissioner of U.S. Customs and Border Protection, upon the request of any entity, may enter into a fee agreement with such entity under which—

(1) U.S. Customs and Border Protection shall provide services described in subsection (b) at a United States port of entry or any other facility at which U.S. Customs and Border Protection provides or will provide such services;

(2) such entity shall remit to U.S. Customs and Border Protection a fee imposed under subsection (h) in an amount equal to the full costs that are incurred or will be incurred in providing such services; and

(3) if space is provided by such entity, each facility at which U.S. Customs and Border

Protection services are performed shall be maintained and equipped by such entity, without cost to the Federal Government, in accordance with U.S. Customs and Border Protection specifications.

(b) Services described

The services described in this subsection are any activities of any employee or Office of Field Operations contractor of U.S. Customs and Border Protection (except employees of the U.S. Border Patrol, as established under section 211(e) of this title) pertaining to, or in support of, customs, agricultural processing, border security, or immigration inspection-related matters at a port of entry or any other facility at which U.S. Customs and Border Protection provides or will provide services.

(c) Modification of prior agreements

The Commissioner of U.S. Customs and Border Protection, at the request of an entity who has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on December 16, 2016, may modify such agreement to implement any provisions of this section.

(d) Limitations

(1) Impacts of services

The Commissioner of U.S. Customs and Border Protection—

(A) may enter into fee agreements under this section only for services that—

(i) will increase or enhance the operational capacity of U.S. Customs and Border Protection based on available staffing and workload; and

(ii) will not shift the cost of services funded in any appropriations Act, or provided from any account in the Treasury of the United States derived by the collection of fees, to entities under this chapter; and

(B) may not enter into a fee agreement under this section if such agreement would unduly and permanently impact services funded in any appropriations Act, or provided from any account in the Treasury of the United States, derived by the collection of fees.

(2) Number

There shall be no limit to the number of fee agreements that the Commissioner of U.S. Customs and Border Protection may enter into under this section.

(e) Air ports of entry

(1) Fee agreement

Except as otherwise provided in this subsection, a fee agreement for U.S. Customs and Border Protection services at an air port of entry may only provide for the payment of overtime costs of U.S. Customs and Border Protection officers and salaries and expenses of U.S. Customs and Border Protection employees to support U.S. Customs and Border Protection officers in performing services described in subsection (b).

(2) Small airports

Notwithstanding paragraph (1), U.S. Customs and Border Protection may receive reimbursement in addition to overtime costs if the fee agreement is for services at an air port of entry that has fewer than 100,000 arriving international passengers annually.

(3) Covered services

In addition to costs described in paragraph (1), a fee agreement for U.S. Customs and Border Protection services at an air port of entry referred to in paragraph (2) may provide for the reimbursement of—

(A) salaries and expenses of not more than five full-time equivalent U.S. Customs and Border Protection Officers beyond the number of such officers assigned to the port of entry on the date on which the fee agreement was signed;

(B) salaries and expenses of employees of U.S. Customs and Border Protection, other than

the officers referred to in subparagraph (A), to support U.S. Customs and Border Protection officers in performing law enforcement functions; and

(C) other costs incurred by U.S. Customs and Border Protection relating to services described in subparagraph (B), such as temporary placement or permanent relocation of employees, including incentive pay for relocation, as appropriate.

(f) Port of entry size

The Commissioner of U.S. Customs and Border Protection shall ensure that each fee agreement proposal is given equal consideration regardless of the size of the port of entry.

(g) Denied application

(1) In general

If the Commissioner of U.S. Customs and Border Protection denies a proposal for a fee agreement under this section, the Commissioner shall provide the entity submitting such proposal with the reason for the denial unless—

(A) the reason for the denial is law enforcement sensitive; or

(B) withholding the reason for the denial is in the national security interests of the United States.

(2) Judicial review

Decisions of the Commissioner of U.S. Customs and Border Protection under paragraph (1) are in the discretion of the Commissioner and are not subject to judicial review.

(h) Fee

(1) In general

The amount of the fee to be charged under an agreement authorized under subsection (a) shall be paid by each entity requesting U.S. Customs and Border Protection services, and shall be for the full cost of providing such services, including the salaries and expenses of employees and contractors of U.S. Customs and Border Protection, to provide such services and other costs incurred by U.S. Customs and Border Protection relating to such services, such as temporary placement or permanent relocation of such employees and contractors.

(2) Timing

The Commissioner of U.S. Customs and Border Protection may require that the fee referred to in paragraph (1) be paid by each entity that has entered into a fee agreement under subsection (a) with U.S. Customs and Border Protection in advance of the performance of U.S. Customs and Border Protection services.

(3) Oversight of fees

The Commissioner of U.S. Customs and Border Protection shall develop a process to oversee the services for which fees are charged pursuant to an agreement under subsection (a), including—

(A) a determination and report on the full costs of providing such services, and a process for increasing such fees, as necessary;

(B) the establishment of a periodic remittance schedule to replenish appropriations, accounts, or funds, as necessary; and

(C) the identification of costs paid by such fees.

(i) Deposit of funds

(1) Account

Funds collected pursuant to any agreement entered into pursuant to subsection (a)—

(A) shall be deposited as offsetting collections;

(B) shall remain available until expended without fiscal year limitation; and

(C) shall be credited to the applicable appropriation, account, or fund for the amount paid out of such appropriation, account, or fund for any expenses incurred or to be incurred by U.S. Customs and Border Protection in providing U.S. Customs and Border Protection services

under any such agreement and any other costs incurred or to be incurred by U.S. Customs and Border Protection relating to such services.

(2) Return of unused funds

The Commissioner of U.S. Customs and Border Protection shall return any unused funds collected and deposited into the account described in paragraph (1) if a fee agreement entered into pursuant to subsection (a) is terminated for any reason or the terms of such fee agreement change by mutual agreement to cause a reduction of U.S. Customs and Border Protections [1] services. No interest shall be owed upon the return of any such unused funds.

(j) Termination

(1) In general

The Commissioner of U.S. Customs and Border Protection shall terminate the services provided pursuant to a fee agreement entered into under subsection (a) with an entity that, after receiving notice from the Commissioner that a fee under subsection (h) is due, fails to pay such fee in a timely manner. If such services are terminated, all costs incurred by U.S. Customs and Border Protection that have not been paid shall become immediately due and payable. Interest on unpaid fees shall accrue based on the rate and amount established under sections 6621 and 6622 of title 26.

(2) Penalty

Any entity that, after notice and demand for payment of any fee under subsection (h), fails to pay such fee in a timely manner shall be liable for a penalty or liquidated damage equal to two times the amount of such fee. Any such amount collected under this paragraph shall be deposited into the appropriate account specified under subsection (i) and shall be available as described in such subsection.

(3) Termination by the entity

Any entity who has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on December 16, 2016, or under the provisions of this section, may request that such agreement be amended to provide for termination upon advance notice, length, and terms that are negotiated between such entity and U.S. Customs and Border Protection.

(k) Annual report

The Commissioner of U.S. Customs and Border Protection shall—

(1) submit an annual report identifying the activities undertaken and the agreements entered into pursuant to this section to—

(A) the Committee on Appropriations of the Senate;
(B) the Committee on Finance of the Senate;
(C) the Committee on Homeland Security and Governmental Affairs of the Senate;
(D) the Committee on the Judiciary of the Senate;
(E) the Committee on Appropriations of the House of Representatives;
(F) the Committee on Homeland Security of the House of Representatives;
(G) the Committee on the Judiciary of the House of Representatives; and
(H) the Committee on Ways and Means of the House of Representatives; and

(2) not later than 15 days before entering into a fee agreement, notify the members of Congress that represent the State or Congressional District in which the affected port of entry or facility is located of such agreement.

(l) Rule of construction

Nothing in this section may be construed as imposing on U.S. Customs and Border Protection any responsibilities, duties, or authorities relating to real property.

(Pub. L. 107–296, title IV, §481, as added Pub. L. 114–279, §2(a), Dec. 16, 2016, 130 Stat. 1413.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (d)(1)(A)(ii), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

[1] So in original. Probably should be "Protection".

§301a. Port of entry donation authority

(a) Personal property donation authority

(1) In general

The Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, may enter into an agreement with any entity to accept a donation of personal property, money, or nonpersonal services for the uses described in paragraph (3) only with respect to the following locations at which U.S. Customs and Border Protection performs or will be performing inspection services:

(A) A new or existing sea or air port of entry.

(B) An existing Federal Government-owned or -leased land port of entry.

(C) A new Federal Government-owned or -leased land port of entry if—

(i) the fair market value of the donation is $75,000,000 or less; and

(ii) the fair market value of donations with respect to the land port of entry total $75,000,000 or less over the preceding five years.

(2) Limitation on monetary donations

Any monetary donation accepted pursuant to this subsection may not be used to pay the salaries of U.S. Customs and Border Protection employees performing inspection services.

(3) Uses

Donations accepted pursuant to this subsection may be used for activities of the Office of Field Operations set forth in subparagraphs (A) through (F) of section 211(g)(3) of this title, which are related to a new or existing sea or air port of entry or a new or existing Federal Government-owned or -leased land port of entry described in paragraph (1), including expenses related to—

(A) furniture, fixtures, equipment, or technology, including the installation or deployment of such items; and

(B) the operation and maintenance of such furniture, fixtures, equipment, or technology.

(b) Real property donation authority

(1) In general

Subject to paragraph (3), the Commissioner of U.S. Customs and Border Protection, and the Administrator of General Services, as applicable, may enter into an agreement with any entity to accept a donation of real property or money for uses described in paragraph (2) only with respect to the following locations at which U.S. Customs and Border Protection performs or will be performing inspection services:

(A) A new or existing sea or air port of entry.

(B) An existing Federal Government-owned land port of entry.

(C) A new Federal Government-owned land port of entry if—

(i) the fair market value of the donation is $75,000,000 or less; and

(ii) the fair market value of donations with respect to the land port of entry total $75,000,000 or less over the preceding five years.

(2) Use

Donations accepted pursuant to this subsection may be used for activities of the Office of Field Operations set forth in section 211(g) of this title, which are related to the construction, alteration, operation, or maintenance of a new or existing sea or air port of entry or a new or existing a [1] Federal Government-owned land port of entry described in paragraph (1), including expenses related to—

(A) land acquisition, design, construction, repair, or alteration; and

(B) operation and maintenance of such port of entry facility.

(3) Limitation on real property donations

A donation of real property under this subsection at an existing land port of entry owned by the General Services Administration may only be accepted by the Administrator of General Services.

(4) Sunset

(A) In general

The authority to enter into an agreement under this subsection shall terminate on December 31, 2026.

(B) Rule of construction

The termination date referred to in subparagraph (A) shall not apply to a proposal accepted for consideration by U.S. Customs and Border Protection or the General Services Administration pursuant to this section or a prior pilot program prior to such termination date.

(c) General provisions

(1) Duration

An agreement entered into under subsection (a) or (b) (and, in the case of such subsection (b), in accordance with paragraph (4) of such subsection) may last as long as required to meet the terms of such agreement.

(2) Criteria

In carrying out an agreement entered into under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, shall establish criteria regarding—

(A) the selection and evaluation of donors;

(B) the identification of roles and responsibilities between U.S. Customs and Border Protection, the General Services Administration, and donors;

(C) the identification, allocation, and management of explicit and implicit risks of partnering between the Federal Government and donors;

(D) decision-making and dispute resolution processes; and

(E) processes for U.S. Customs and Border Protection, and the General Services Administration, as applicable, to terminate agreements if selected donors are not meeting the terms of any such agreement, including the security standards established by U.S. Customs and Border Protection.

(3) Evaluation procedures

(A) In general

The Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, as applicable, shall—

(i) establish criteria for evaluating a proposal to enter into an agreement under subsection (a) or (b); and

(ii) make such criteria publicly available.

(B) Considerations

Criteria established pursuant to subparagraph (A) shall consider—

(i) the impact of a proposal referred to in such subparagraph on the land, sea, or air port of entry at issue and other ports of entry or similar facilities or other infrastructure near the location of the proposed donation;

(ii) such proposal's potential to increase trade and travel efficiency through added capacity;

(iii) such proposal's potential to enhance the security of the port of entry at issue;

(iv) the impact of the proposal on reducing wait times at that port of entry or facility and other ports of entry on the same border;

(v) for a donation under subsection (b)—

(I) whether such donation satisfies the requirements of such proposal, or whether additional real property would be required; and

(II) how such donation was acquired, including if eminent domain was used;

(vi) the funding available to complete the intended use of such donation;

(vii) the costs of maintaining and operating such donation;

(viii) the impact of such proposal on U.S. Customs and Border Protection staffing requirements; and

(ix) other factors that the Commissioner or Administrator determines to be relevant.

(C) Determination and notification

(i) Incomplete proposals

(I) In general

Not later than 60 days after receiving the proposals for a donation agreement from an entity, the Commissioner of U.S. Customs and Border Protection shall notify such entity as to whether such proposal is complete or incomplete.

(II) Resubmission

If the Commissioner of U.S. Customs and Border Protection determines that a proposal is incomplete, the Commissioner shall—

(aa) notify the appropriate entity and provide such entity with a description of all information or material that is needed to complete review of the proposal; and

(bb) allow the entity to resubmit the proposal with additional information and material described in item (aa) to complete the proposal.

(ii) Complete proposals

Not later than 180 days after receiving a completed proposal to enter into an agreement under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection, with the concurrence of the Administrator of General Services, as applicable, shall—

(I) determine whether to approve or deny such proposal; and

(II) notify the entity that submitted such proposal of such determination.

(4) Supplemental funding

Except as required under section 3307 of title 40, real property donations to the Administrator of General Services made pursuant to subsection [1] (a) and [1] (b) at a GSA-owned land port of entry may be used in addition to any other funding for such purpose, including appropriated funds, property, or services.

(5) Return of donations

The Commissioner of U.S. Customs and Border Protection, or the Administrator of General Services, as applicable, may return any donation made pursuant to subsection (a) or (b). No interest shall be owed to the donor with respect to any donation provided under such subsections that is returned pursuant to this subsection.

(6) Prohibition on certain funding

(A) In general

Except as provided in subsections (a) and (b) regarding the acceptance of donations, the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services, as applicable, may not, with respect to an agreement entered into under either of such subsections, obligate or expend amounts in excess of amounts that have been appropriated pursuant to any appropriations Act for purposes specified in either of such subsections or otherwise made available for any of such purposes.

(B) Certification requirement

Before accepting any donations pursuant to an agreement under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection shall certify to the congressional committees set forth in paragraph (7) that [2]

(i) the donation will not be used for the construction of a detention facility or a border fence or wall; and

(ii) the donor will be notified in the Donations Acceptance Agreement that the donor shall be financially responsible for all costs and operating expenses related to the operation, maintenance, and repair of the donated real property until such time as U.S. Customs and Border Protection provides the donor written notice otherwise.

(7) Annual reports

The Commissioner of U.S. Customs and Border Protection, in collaboration with the Administrator of General Services, as applicable, shall submit an annual report identifying the activities undertaken and agreements entered into pursuant to subsections (a) and (b) to—

(A) the Committee on Appropriations of the Senate;
(B) the Committee on Environment and Public Works of the Senate;
(C) the Committee on Finance of the Senate;
(D) the Committee on Homeland Security and Governmental Affairs of the Senate;
(E) the Committee on the Judiciary of the Senate;
(F) the Committee on Appropriations of the House of Representatives;
(G) the Committee on Homeland Security of the House of Representatives;
(H) the Committee on the Judiciary of the House of Representatives;
(I) the Committee on Transportation and Infrastructure of the House of Representatives; and
(J) the Committee on Ways and Means of the House of Representatives.

(d) GAO report

The Comptroller General of the United States shall submit an [3] biennial report to the congressional committees referred to in subsection (c)(7) that evaluates—

(1) fee agreements entered into pursuant to section 301 of this title;
(2) donation agreements entered into pursuant to subsections (a) and (b); and
(3) the fees and donations received by U.S. Customs and Border Protection pursuant to such agreements.

(e) Judicial review

Decisions of the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services under this section regarding the acceptance of real or personal property are in the discretion of the Commissioner and the Administrator and are not subject to judicial review.

(f) Rule of construction

Except as otherwise provided in this section, nothing in this section may be construed as affecting in any manner the responsibilities, duties, or authorities of U.S. Customs and Border Protection or the General Services Administration.

(Pub. L. 107–296, title IV, §482, as added Pub. L. 114–279, §2(a), Dec. 16, 2016, 130 Stat. 1417; amended Pub. L. 116–260, div. O, title III, §301, Dec. 27, 2020, 134 Stat. 2149; Pub. L. 117–81, div. F, title LXIV, §6410, Dec. 27, 2021, 135 Stat. 2408.)

EDITORIAL NOTES

AMENDMENTS

2021—Subsec. (a)(1)(B), (C). Pub. L. 117–81, §6410(1)(A)(i), (ii)(I), inserted "or -leased" before "land".

Subsec. (a)(1)(C)(i). Pub. L. 117–81, §6410(1)(A)(ii)(II), substituted "$75,000,000" for "$50,000,000".

Subsec. (a)(1)(C)(ii). Pub. L. 117–81, §6410(1)(A)(ii)(III), amended cl. (ii) generally. Prior to amendment, text read as follows: "the fair market value, including any personal and real property donations in total, of such port of entry when completed, is $50,000,000 or less.".

Subsec. (a)(3). Pub. L. 117–81, §6410(1)(B), inserted "or -leased" before "land" in introductory provisions.

Subsec. (b)(1). Pub. L. 117–81, §6410(2)(A), which directed substitution of "Administrator of General Services" for "Administrator of the General Services Administration" in the matter preceding par. (1), was executed in par. (1) to reflect the probable intent of Congress.

Subsec. (b)(1)(C)(i). Pub. L. 117–81, §6410(2)(B)(i), substituted "$75,000,000" for "$50,000,000".

Subsec. (b)(1)(C)(ii). Pub. L. 117–81, §6410(2)(b)(ii), amended cl. (ii) genrally. Prior to amendment, text read as follows: "the fair market value, including any personal and real property donations in total, of such port of entry when completed, is $50,000,000 or less.".

Subsec. (b)(4)(A). Pub. L. 117–81, §6410(2)(C)(i), substituted "terminate on December 31, 2026." for "terminate on the date that is December 16, 2021.".

Subsec. (b)(4)(B). Pub. L. 117–81, §6410(2)(C)(ii), substituted "a proposal accepted for consideration by U.S. Customs and Border Protection or the General Services Administration pursuant to this section or a prior pilot program prior to such termination date" for "carrying out the terms of an agreement under this subsection if such agreement is entered into before such termination date".

Subsec. (c)(6)(B). Pub. L. 117–81, §6410(3), substituted cls. (i) and (ii) for "the donation will not be used for the construction of a detention facility or a border fence or wall."

Subsec. (d). Pub. L. 117–81, §6401(4), substituted "biennial" for "annual" in introductory provisions.

Subsec. (e). Pub. L. 117–81, §6410(d), substituted "Administrator of General Services" for "Administrator of the General Services Administration".

2020—Subsec. (b)(4)(A). Pub. L. 116–260, which directed substitution of "December 16, 2021" for "4 years after December 16, 2016", was executed by making the substitution for original text reading "4 years after the date of the enactment of this section", which had been translated as "4 years after December 16, 2016", to reflect the probable intent of Congress.

[1] So in original.

[2] So in original. Probably should be followed by a dash.

[3] So in original. Probably should be "a".

§301b. Current and proposed agreements

Nothing in this part or in section 4 of the Cross-Border Trade Enhancement Act of 2016 may be construed as affecting—

(1) any agreement entered into pursuant to section 560 of division D of the Consolidated and Further Continuing Appropriations Act, 2013 (Public Law 113–6) or section 559 of title V of division F of the Consolidated Appropriations Act, 2014 (6 U.S.C. 211 note; Public Law 113–76), as in existence on the day before December 16, 2016, and any such agreement shall continue to have full force and effect on and after such date; or

(2) a proposal accepted for consideration by U.S. Customs and Border Protection pursuant to such section 559, as in existence on the day before December 16, 2016.

(Pub. L. 107–296, title IV, §483, as added Pub. L. 114–279, §2(a), Dec. 16, 2016, 130 Stat. 1421.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 4 of the Cross-Border Trade Enhancement Act of 2016, referred to in text, is section 4 of Pub. L. 114–279, Dec. 16, 2016, 130 Stat. 1422, which repealed section 560 of division D of Pub. L. 113–6 and section 559 of title V of division F of Pub. L. 113–76. Section 560 of Pub. L. 113–6, was not classified to the Code. Section 559 of Pub. L. 113–76 was classified as a note under section 211 of this title.

§301c. Definitions

In this part:

(1) Donor

The term "donor" means any entity that is proposing to make a donation under this chapter.

(2) Entity

The term "entity" means any—

(A) person;

(B) partnership, corporation, trust, estate, cooperative, association, or any other organized group of persons;

(C) Federal, State or local government (including any subdivision, agency or instrumentality thereof); or

(D) any other private or governmental entity.

(Pub. L. 107–296, title IV, §484, as added Pub. L. 114–279, §2(a), Dec. 16, 2016, 130 Stat. 1421.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in par. (1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

SUBCHAPTER V—NATIONAL EMERGENCY MANAGEMENT

EDITORIAL NOTES

CODIFICATION

Pub. L. 109–295, title VI, §611(1), Oct. 4, 2006, 120 Stat. 1395, substituted "NATIONAL EMERGENCY MANAGEMENT" for "EMERGENCY PREPAREDNESS AND RESPONSE" in subchapter heading.

§311. Definitions

In this subchapter—

(1) the term "Administrator" means the Administrator of the Agency;

(2) the term "Agency" means the Federal Emergency Management Agency;

(3) the term "catastrophic incident" means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area;

(4) the terms "credentialed" and "credentialing" mean having provided, or providing, respectively, documentation that identifies personnel and authenticates and verifies the qualifications of such personnel by ensuring that such personnel possess a minimum common

level of training, experience, physical and medical fitness, and capability appropriate for a particular position in accordance with standards created under section 320 of this title;

(5) the term "Federal coordinating officer" means a Federal coordinating officer as described in section 5143 of title 42;

(6) the term "interoperable" has the meaning given the term "interoperable communications" under section 194(g)(1) of this title;

(7) the term "National Incident Management System" means a system to enable effective, efficient, and collaborative incident management;

(8) the term "National Response Plan" means the National Response Plan or any successor plan prepared under section 314(a)(6) [1] of this title;

(9) the term "Regional Administrator" means a Regional Administrator appointed under section 317 of this title;

(10) the term "Regional Office" means a Regional Office established under section 317 of this title;

(11) the term "resources" means personnel and major items of equipment, supplies, and facilities available or potentially available for responding to a natural disaster, act of terrorism, or other man-made disaster;

(12) the term "surge capacity" means the ability to rapidly and substantially increase the provision of search and rescue capabilities, food, water, medicine, shelter and housing, medical care, evacuation capacity, staffing (including disaster assistance employees), and other resources necessary to save lives and protect property during a catastrophic incident;

(13) the term "tribal government" means the government of any entity described in section 101(13)(B) of this title; and

(14) the terms "typed" and "typing" mean having evaluated, or evaluating, respectively, a resource in accordance with standards created under section 320 of this title.

(Pub. L. 107–296, title V, §501, as added Pub. L. 109–295, title VI, §611(10), Oct. 4, 2006, 120 Stat. 1395; amended Pub. L. 110–53, title IV, §401(a), title V, §502(c)(1), Aug. 3, 2007, 121 Stat. 301, 311; Pub. L. 114–328, div. A, title XIX, §1913(b)(2), Dec. 23, 2016, 130 Stat. 2687.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 314(a)(6) of this title, referred to in par. (8), was in the original "section 502(a)(6)" and was translated as meaning section 502 of Pub. L. 107–296 prior to its redesignation as section 504 by Pub. L. 109–295, §611(8), and not section 506 which was redesignated section 502 by Pub. L. 109–295, §611(9), and is classified to section 312 of this title, to reflect the probable intent of Congress.

PRIOR PROVISIONS

A prior section 311, Pub. L. 107–296, title V, §501, Nov. 25, 2002, 116 Stat. 2212, provided for an Under Secretary for Emergency Preparedness and Response, prior to repeal by Pub. L. 109–295, title VI, §611(2), Oct. 4, 2006, 120 Stat. 1395.

AMENDMENTS

2016—Par. (13). Pub. L. 114–328 substituted "101(13)(B)" for "101(11)(B)".

2007—Pars. (4) to (12). Pub. L. 110–53, §401(a)(1)–(4), added pars. (4) and (11) and redesignated former pars. (4) to (10) as (5) to (10) and (12), respectively. Former par. (11) redesignated (13).

Par. (13). Pub. L. 110–53, §502(c)(1), substituted "101(11)(B)" for "101(10)(B)".

Pub. L. 110–53, §401(a)(1), redesignated par. (11) as (13).

Par. (14). Pub. L. 110–53, §401(a)(5)–(7), added par. (14).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L.

109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

INTERIM ACTIONS

Pub. L. 109–295, title VI, §612(f)(1), Oct. 4, 2006, 120 Stat. 1411, provided that: "During the period beginning on the date of enactment of this Act [Oct. 4, 2006] and ending on March 31, 2007, the Secretary [of Homeland Security], the Under Secretary for Preparedness, and the Director of the Federal Emergency Management Agency shall take such actions as are necessary to provide for the orderly implementation of any amendment under this subtitle [subtitle A (§§611–614) of title VI of Pub. L. 109–295, see Tables for classification] that takes effect on March 31, 2007."

[1] *See References in Text note below.*

§312. Definition

In this subchapter, the term "Nuclear Incident Response Team" means a resource that includes—

(1) those entities of the Department of Energy that perform nuclear or radiological emergency support functions (including accident response, search response, advisory, and technical operations functions), radiation exposure functions at the medical assistance facility known as the Radiation Emergency Assistance Center/Training Site (REAC/TS), radiological assistance functions, and related functions; and

(2) those entities of the Environmental Protection Agency that perform such support functions (including radiological emergency response functions) and related functions.

(Pub. L. 107–296, title V, §502, formerly §506, Nov. 25, 2002, 116 Stat. 2214; renumbered §502, Pub. L. 109–295, title VI, §611(9), Oct. 4, 2006, 120 Stat. 1395.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 316 of this title prior to renumbering by Pub. L. 109–295.

PRIOR PROVISIONS

A prior section 502 of Pub. L. 107–296 was renumbered section 504 and is classified to section 314 of this title.

§313. Federal Emergency Management Agency

(a) In general

There is in the Department the Federal Emergency Management Agency, headed by an Administrator.

(b) Mission

(1) Primary mission

The primary mission of the Agency is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation.

(2) Specific activities

In support of the primary mission of the Agency, the Administrator shall—

(A) lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters,

including catastrophic incidents;

(B) partner with State, local, and tribal governments and emergency response providers, with other Federal agencies, with the private sector, and with nongovernmental organizations to build a national system of emergency management that can effectively and efficiently utilize the full measure of the Nation's resources to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;

(C) develop a Federal response capability that, when necessary and appropriate, can act effectively and rapidly to deliver assistance essential to saving lives or protecting or preserving property or public health and safety in a natural disaster, act of terrorism, or other man-made disaster;

(D) integrate the Agency's emergency preparedness, protection, response, recovery, and mitigation responsibilities to confront effectively the challenges of a natural disaster, act of terrorism, or other man-made disaster;

(E) develop and maintain robust Regional Offices that will work with State, local, and tribal governments, emergency response providers, and other appropriate entities to identify and address regional priorities;

(F) under the leadership of the Secretary, coordinate with the Commandant of the Coast Guard, the Director of Customs and Border Protection, the Director of Immigration and Customs Enforcement, the National Operations Center, and other agencies and offices in the Department to take full advantage of the substantial range of resources in the Department;

(G) provide funding, training, exercises, technical assistance, planning, and other assistance to build tribal, local, State, regional, and national capabilities (including communications capabilities), necessary to respond to a natural disaster, act of terrorism, or other man-made disaster;

(H) develop and coordinate the implementation of a risk-based, all-hazards strategy for preparedness that builds those common capabilities necessary to respond to natural disasters, acts of terrorism, and other man-made disasters while also building the unique capabilities necessary to respond to specific types of incidents that pose the greatest risk to our Nation; and

(I) identify, integrate, and implement the needs of children, including children within under-served communities, into activities to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other disasters, including catastrophic incidents, including by appointing a technical expert, who may consult with relevant outside organizations and experts, as necessary, to coordinate such integration, as necessary.

(c) Administrator

(1) In general

The Administrator shall be appointed by the President, by and with the advice and consent of the Senate.

(2) Qualifications

The Administrator shall be appointed from among individuals who have—

(A) a demonstrated ability in and knowledge of emergency management and homeland security; and

(B) not less than 5 years of executive leadership and management experience in the public or private sector.

(3) Reporting

The Administrator shall report to the Secretary, without being required to report through any other official of the Department.

(4) Principal advisor on emergency management

(A) In general

The Administrator is the principal advisor to the President, the Homeland Security Council,

and the Secretary for all matters relating to emergency management in the United States.

(B) Advice and recommendations

(i) In general

In presenting advice with respect to any matter to the President, the Homeland Security Council, or the Secretary, the Administrator shall, as the Administrator considers appropriate, inform the President, the Homeland Security Council, or the Secretary, as the case may be, of the range of emergency preparedness, protection, response, recovery, and mitigation options with respect to that matter.

(ii) Advice on request

The Administrator, as the principal advisor on emergency management, shall provide advice to the President, the Homeland Security Council, or the Secretary on a particular matter when the President, the Homeland Security Council, or the Secretary requests such advice.

(iii) Recommendations to Congress

After informing the Secretary, the Administrator may make such recommendations to Congress relating to emergency management as the Administrator considers appropriate.

(5) Cabinet status

(A) In general

The President may designate the Administrator to serve as a member of the Cabinet in the event of natural disasters, acts of terrorism, or other man-made disasters.

(B) Retention of authority

Nothing in this paragraph shall be construed as affecting the authority of the Secretary under this chapter.

(Pub. L. 107–296, title V, §503, as added Pub. L. 109–295, title VI, §611(11), Oct. 4, 2006, 120 Stat. 1396; amended Pub. L. 117–130, §3, June 6, 2022, 136 Stat. 1229.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (c)(5)(B), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

PRIOR PROVISIONS

A prior section 313, Pub. L. 107–296, title V, §503, Nov. 25, 2002, 116 Stat. 2213; Pub. L. 108–276, §3(c)(3), July 21, 2004, 118 Stat. 853; Pub. L. 109–417, title III, §301(c)(2), Dec. 19, 2006, 120 Stat. 2854, related to the transfer of certain functions to the Secretary of Homeland Security, prior to repeal by Pub. L. 109–295, title VI, §611(3), Oct. 4, 2006, 120 Stat. 1395.

AMENDMENTS

2022—Subsec. (b)(2)(I). Pub. L. 117–130 added subpar. (I).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Pub. L. 109–295, title VI, §612(c), Oct. 4, 2006, 120 Stat. 1410, provided that: "Any reference to the Director of the Federal Emergency Management Agency, in any law, rule, regulation, certificate, directive, instruction, or other official paper shall be considered to refer and apply to the Administrator of the Federal Emergency Management Agency."

Pub. L. 109–295, title VI, §612(f)(2), Oct. 4, 2006, 120 Stat. 1411, provided that: "Any reference to the

Administrator of the Federal Emergency Management Agency in this title [see Tables for classification] or an amendment by this title shall be considered to refer and apply to the Director of the Federal Emergency Management Agency until March 31, 2007."

EFFECTIVE DATE

Section effective Mar. 31, 2007, see section 614(b)(1) of Pub. L. 109–295, set out as a note under section 701 of this title.

§314. Authority and responsibilities

(a) In general

The Administrator shall provide Federal leadership necessary to prepare for, protect against, respond to, recover from, or mitigate against a natural disaster, act of terrorism, or other man-made disaster, including—

(1) helping to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies;

(2) with respect to the Nuclear Incident Response Team (regardless of whether it is operating as an organizational unit of the Department pursuant to this subchapter)—

(A) establishing standards and certifying when those standards have been met;

(B) conducting joint and other exercises and training and evaluating performance; and

(C) providing funds to the Department of Energy and the Environmental Protection Agency, as appropriate, for homeland security planning, exercises and training, and equipment;

(3) providing the Federal Government's response to terrorist attacks and major disasters, including—

(A) managing such response;

(B) directing the Domestic Emergency Support Team and (when operating as an organizational unit of the Department pursuant to this subchapter) the Nuclear Incident Response Team;

(C) overseeing the Metropolitan Medical Response System; and

(D) coordinating other Federal response resources, including requiring deployment of the Strategic National Stockpile, in the event of a terrorist attack or major disaster;

(4) aiding the recovery from terrorist attacks and major disasters;

(5) building a comprehensive national incident management system with Federal, State, and local government personnel, agencies, and authorities, to respond to such attacks and disasters;

(6) consolidating existing Federal Government emergency response plans into a single, coordinated national response plan;

(7) helping ensure the acquisition of operable and interoperable communications capabilities by Federal, State, local, and tribal governments and emergency response providers;

(8) assisting the President in carrying out the functions under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) and carrying out all functions and authorities given to the Administrator under that Act;

(9) carrying out the mission of the Agency to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a risk-based, comprehensive emergency management system of—

(A) mitigation, by taking sustained actions to reduce or eliminate long-term risks to people and property from hazards and their effects;

(B) preparedness, by planning, training, and building the emergency management profession to prepare effectively for, mitigate against, respond to, and recover from any hazard;

(C) response, by conducting emergency operations to save lives and property through positioning emergency equipment, personnel, and supplies, through evacuating potential victims, through providing food, water, shelter, and medical care to those in need, and through

restoring critical public services; and

(D) recovery, by rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards;

(10) increasing efficiencies, by coordinating efforts relating to preparedness, protection, response, recovery, and mitigation;

(11) helping to ensure the effectiveness of emergency response providers in responding to a natural disaster, act of terrorism, or other man-made disaster;

(12) supervising grant programs administered by the Agency;

(13) administering and ensuring the implementation of the National Response Plan, including coordinating and ensuring the readiness of each emergency support function under the National Response Plan;

(14) coordinating with the National Advisory Council established under section 318 of this title;

(15) preparing and implementing the plans and programs of the Federal Government for—

(A) continuity of operations;

(B) continuity of government; and

(C) continuity of plans;

(16) minimizing, to the extent practicable, overlapping planning and reporting requirements applicable to State, local, and tribal governments and the private sector;

(17) maintaining and operating within the Agency the National Response Coordination Center or its successor;

(18) developing a national emergency management system that is capable of preparing for, protecting against, responding to, recovering from, and mitigating against catastrophic incidents;

(19) assisting the President in carrying out the functions under the national preparedness goal and the national preparedness system and carrying out all functions and authorities of the Administrator under the national preparedness System;

(20) carrying out all authorities of the Federal Emergency Management Agency and the Directorate of Preparedness of the Department as transferred under section 315 of this title; and

(21) otherwise carrying out the mission of the Agency as described in section 313(b) of this title.

(b) All-hazards approach

In carrying out the responsibilities under this section, the Administrator shall coordinate the implementation of a risk-based, all-hazards strategy that builds those common capabilities necessary to prepare for, protect against, respond to, recover from, or mitigate against natural disasters, acts of terrorism, and other man-made disasters, while also building the unique capabilities necessary to prepare for, protect against, respond to, recover from, or mitigate against the risks of specific types of incidents that pose the greatest risk to the Nation.

(Pub. L. 107–296, title V, §504, formerly §502, Nov. 25, 2002, 116 Stat. 2212; Pub. L. 108–276, §3(b)(1), July 21, 2004, 118 Stat. 852; Pub. L. 108–458, title VII, §7303(h)(1), Dec. 17, 2004, 118 Stat. 3846; renumbered §504 and amended Pub. L. 109–295, title VI, §611(8), (12), Oct. 4, 2006, 120 Stat. 1395, 1398; Pub. L. 109–417, title III, §301(c)(1), Dec. 19, 2006, 120 Stat. 2854.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a)(8), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

CODIFICATION

Section was formerly classified to section 312 of this title prior to renumbering by Pub. L. 109–295.

PRIOR PROVISIONS

A prior section 504 of Pub. L. 107–296 was renumbered section 517 and is classified to section 321f of this title.

AMENDMENTS

2006—Pub. L. 109–295, §611(12)(A), (B), inserted "Authority and" before "responsibilities" in section catchline, designated existing provisions as subsec. (a), inserted subsec. heading, and substituted "The Administrator shall provide Federal leadership necessary to prepare for, protect against, respond to, recover from, or mitigate against a natural disaster, act of terrorism, or other man-made disaster, including—" for "The Secretary, acting through the Under Secretary for Emergency Preparedness and Response, shall include—" in introductory provisions.

Subsec. (a)(3)(B). Pub. L. 109–417, which directed that section 502(3)(B) of Pub. L. 107–296 be amended by striking ", the National Disaster Medical System,", was executed by striking those words after "Domestic Emergency Support Team" in subsec. (a)(3)(B) of this section, to reflect the probable intent of Congress and the redesignation of section 502(3)(B) as 504(a)(3)(B) by Pub. L. 109–295, §611(8), (12)(B). See credits and Amendment note above.

Subsec. (a)(7) to (21). Pub. L. 109–295, §611(12)(C), (D), added pars. (7) to (21) and struck out former par. (7) which read as follows: "helping to ensure that emergency response providers acquire interoperable communications technology."

Subsec. (b). Pub. L. 109–295, §611(12)(D), added subsec. (b).

2004—Par. (3)(B). Pub. L. 108–276, §3(b)(1)(A), struck out "the Strategic National Stockpile," after "Domestic Emergency Support Team,".

Par. (3)(D). Pub. L. 108–276, §3(b)(1)(B), inserted ", including requiring deployment of the Strategic National Stockpile," after "resources".

Par. (7). Pub. L. 108–458 struck out "developing comprehensive programs for developing interoperative communications technology, and" before "helping" and substituted "acquire interoperable communications technology" for "acquire such technology".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2006 AMENDMENT

Pub. L. 109–417, title III, §301(f), Dec. 19, 2006, 120 Stat. 2855, provided that: "The amendments made by subsections (b) and (c) [amending this section and former section 313 of this title and enacting provisions set out as a note under section 300hh–11 of Title 42, The Public Health and Welfare] shall take effect on January 1, 2007."

Amendment by section 611(12) of Pub. L. 109–295 effective Mar. 31, 2007, see section 614(b)(2) of Pub. L. 109–295, set out as an Effective Date note under section 701 of this title.

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13347. INDIVIDUALS WITH DISABILITIES IN EMERGENCY PREPAREDNESS

Ex. Ord. No. 13347, July 22, 2004, 69 F.R. 44573, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to strengthen emergency preparedness with respect to individuals with disabilities, it is hereby ordered as follows:

SECTION 1. *Policy*. To ensure that the Federal Government appropriately supports safety and security for individuals with disabilities in situations involving disasters, including earthquakes, tornadoes, fires, floods, hurricanes, and acts of terrorism, it shall be the policy of the United States that executive departments and agencies of the Federal Government (agencies):

(a) consider, in their emergency preparedness planning, the unique needs of agency employees with disabilities and individuals with disabilities whom the agency serves;

(b) encourage, including through the provision of technical assistance, as appropriate, consideration of the unique needs of employees and individuals with disabilities served by State, local, and tribal governments and private organizations and individuals in emergency preparedness planning; and

(c) facilitate cooperation among Federal, State, local, and tribal governments and private organizations and individuals in the implementation of emergency preparedness plans as they relate to individuals with disabilities.

SEC. 2. *Establishment of Council*. (a) There is hereby established, within the Department of Homeland Security for administrative purposes, the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (the "Council"). The Council shall consist exclusively of the following members or their designees:

(i) the heads of executive departments, the Administrator of the Environmental Protection Agency, the Administrator of General Services, the Director of the Office of Personnel Management, and the Commissioner of Social Security; and

(ii) any other agency head as the Secretary of Homeland Security may, with the concurrence of the agency head, designate.

(b) The Secretary of Homeland Security shall chair the Council, convene and preside at its meetings, determine its agenda, direct its work, and, as appropriate to particular subject matters, establish and direct subgroups of the Council, which shall consist exclusively of Council members.

(c) A member of the Council may designate, to perform the Council functions of the member, an employee of the member's department or agency who is either an officer of the United States appointed by the President, or a full-time employee serving in a position with pay equal to or greater than the minimum rate payable for GS–15 of the General Schedule.

SEC. 3. *Functions of Council*. (a) The Council shall:

(i) coordinate implementation by agencies of the policy set forth in section 1 of this order;

(ii) whenever the Council obtains in the performance of its functions information or advice from any individual who is not a full-time or permanent part-time Federal employee, obtain such information and advice only in a manner that seeks individual advice and does not involve collective judgment or consensus advice or deliberation; and

(iii) at the request of any agency head (or the agency head's designee under section 2(c) of this order) who is a member of the Council, unless the Secretary of Homeland Security declines the request, promptly review and provide advice, for the purpose of furthering the policy set forth in section 1, on a proposed action by that agency.

(b) The Council shall submit to the President each year beginning 1 year after the date of this order, through the Assistant to the President for Homeland Security, a report that describes:

(i) the achievements of the Council in implementing the policy set forth in section 1;

(ii) the best practices among Federal, State, local, and tribal governments and private organizations and individuals for emergency preparedness planning with respect to individuals with disabilities; and

(iii) recommendations of the Council for advancing the policy set forth in section 1.

SEC. 4. *General*. (a) To the extent permitted by law:

(i) agencies shall assist and provide information to the Council for the performance of its functions under this order; and

(ii) the Department of Homeland Security shall provide funding and administrative support for the Council.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers or employees, or any other person.

GEORGE W. BUSH.

§314a. FEMA programs

Notwithstanding any other provision of Federal law, as of April 1, 2007, the Director of the Federal Emergency Management Agency shall be responsible for the radiological emergency preparedness program and the chemical stockpile emergency preparedness program.

(Pub. L. 109–347, title VI, §612, Oct. 13, 2006, 120 Stat. 1943.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Security and Accountability For Every Port Act of 2006, also known as

the SAFE Port Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

References to the Director of the Federal Emergency Management Agency considered to refer and apply to the Administrator of the Federal Emergency Management Agency, see section 612(c) of Pub. L. 109–295, set out as a note under section 313 of this title.

§315. Functions transferred

(a) In general

Except as provided in subsection (b), there are transferred to the Agency the following:

(1) All functions of the Federal Emergency Management Agency, including existing responsibilities for emergency alert systems and continuity of operations and continuity of government plans and programs as constituted on June 1, 2006, including all of its personnel, assets, components, authorities, grant programs, and liabilities, and including the functions of the Under Secretary for Federal Emergency Management relating thereto.

(2) The Directorate of Preparedness, as constituted on June 1, 2006, including all of its functions, personnel, assets, components, authorities, grant programs, and liabilities, and including the functions of the Under Secretary for Preparedness relating thereto.

(b) Exceptions

The following within the Preparedness Directorate shall not be transferred:

(1) The Office of Infrastructure Protection.

(2) The National Communications System.

(3) The National Cybersecurity Division.

(4) The functions, personnel, assets, components, authorities, and liabilities of each component described under paragraphs (1) through (3).

(Pub. L. 107–296, title V, §505, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1400; amended Pub. L. 115–387, §2(f)(4), Dec. 21, 2018, 132 Stat. 5168.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 505 of Pub. L. 107–296 was renumbered section 518 and is classified to section 321g of this title.

AMENDMENTS

2018—Subsec. (b)(4), (5). Pub. L. 115–387 redesignated par. (5) as (4), substituted "(1) through (3)" for "(1) through (4)", and struck out former par. (4) which read as follows: "The Office of the Chief Medical Officer."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective Mar. 31, 2007, see section 614(b)(3) of Pub. L. 109–295, set out as a note under section 701 of this title.

TRANSFER OF FUNCTIONS

For transfer of functions, personnel, assets, and liabilities of the Federal Emergency Management Agency, including the functions of the Director of the Federal Emergency Management Agency relating thereto, to the

Secretary of Homeland Security, and for treatment of related references, see former section 313(1) and sections 551(d), 552(d), and 557 of this title and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of this title.

§316. Preserving the Federal Emergency Management Agency

(a) Distinct entity

The Agency shall be maintained as a distinct entity within the Department.

(b) Reorganization

Section 452 of this title shall not apply to the Agency, including any function or organizational unit of the Agency.

(c) Prohibition on changes to missions

(1) In general

The Secretary may not substantially or significantly reduce, including through a Joint Task Force established under section 348 of this title, the authorities, responsibilities, or functions of the Agency or the capability of the Agency to perform those missions, authorities, responsibilities,[1] except as otherwise specifically provided in an Act enacted after October 4, 2006.

(2) Certain transfers prohibited

No asset, function, or mission of the Agency may be diverted to the principal and continuing use of any other organization, unit, or entity of the Department, including a Joint Task Force established under section 348 of this title, except for details or assignments that do not reduce the capability of the Agency to perform its missions.

(d) Reprogramming and transfer of funds

In reprogramming or transferring funds, the Secretary shall comply with any applicable provisions of any Act making appropriations for the Department for fiscal year 2007, or any succeeding fiscal year, relating to the reprogramming or transfer of funds.

(Pub. L. 107–296, title V, §506, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1400; amended Pub. L. 114–328, div. A, title XIX, §1901(d)(1), Dec. 23, 2016, 130 Stat. 2670.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 506 of Pub. L. 107–296 was renumbered section 502 and is classified to section 312 of this title.

AMENDMENTS

2016—Subsec. (c)(1). Pub. L. 114–328, §1901(d)(1)(A), inserted ", including through a Joint Task Force established under section 348 of this title, after "reduce".

Subsec. (c)(2). Pub. L. 114–328, §1901(d)(1)(B), inserted "including a Joint Task Force established under section 348 of this title," after "Department,".

[1] So in original. Probably should be "authorities, responsibilities, or functions".

§317. Regional offices

(a) In general

There are in the Agency 10 regional offices, as identified by the Administrator.

(b) Management of regional offices

(1) Regional Administrator

Each Regional Office shall be headed by a Regional Administrator who shall be appointed by the Administrator, after consulting with State, local, and tribal government officials in the region. Each Regional Administrator shall report directly to the Administrator and be in the Senior Executive Service.

(2) Qualifications

(A) In general

Each Regional Administrator shall be appointed from among individuals who have a demonstrated ability in and knowledge of emergency management and homeland security.

(B) Considerations

In selecting a Regional Administrator for a Regional Office, the Administrator shall consider the familiarity of an individual with the geographical area and demographic characteristics of the population served by such Regional Office.

(c) Responsibilities

(1) In general

The Regional Administrator shall work in partnership with State, local, and tribal governments, emergency managers, emergency response providers, medical providers, the private sector, nongovernmental organizations, multijurisdictional councils of governments, and regional planning commissions and organizations in the geographical area served by the Regional Office to carry out the responsibilities of a Regional Administrator under this section.

(2) Responsibilities

The responsibilities of a Regional Administrator include—

(A) ensuring effective, coordinated, and integrated regional preparedness, protection, response, recovery, and mitigation activities and programs for natural disasters, acts of terrorism, and other man-made disasters (including planning, training, exercises, and professional development);

(B) assisting in the development of regional capabilities needed for a national catastrophic response system;

(C) coordinating the establishment of effective regional operable and interoperable emergency communications capabilities;

(D) staffing and overseeing 1 or more strike teams within the region under subsection (f), to serve as the focal point of the Federal Government's initial response efforts for natural disasters, acts of terrorism, and other man-made disasters within that region, and otherwise building Federal response capabilities to respond to natural disasters, acts of terrorism, and other man-made disasters within that region;

(E) designating an individual responsible for the development of strategic and operational regional plans in support of the National Response Plan;

(F) fostering the development of mutual aid and other cooperative agreements;

(G) identifying critical gaps in regional capabilities to respond to populations with special needs;

(H) maintaining and operating a Regional Response Coordination Center or its successor;

(I) coordinating with the private sector to help ensure private sector preparedness for natural disasters, acts of terrorism, and other man-made disasters;

(J) assisting State, local, and tribal governments, where appropriate, to preidentify and evaluate suitable sites where a multijurisdictional incident command system may quickly be established and operated from, if the need for such a system arises; and

(K) performing such other duties relating to such responsibilities as the Administrator may require.

(3) Training and exercise requirements

(A) Training

The Administrator shall require each Regional Administrator to undergo specific training periodically to complement the qualifications of the Regional Administrator. Such training, as appropriate, shall include training with respect to the National Incident Management System, the National Response Plan, and such other subjects as determined by the Administrator.

(B) Exercises

The Administrator shall require each Regional Administrator to participate as appropriate in regional and national exercises.

(d) Area offices

(1) In general

There is an Area Office for the Pacific and an Area Office for the Caribbean, as components in the appropriate Regional Offices.

(2) Alaska

The Administrator shall establish an Area Office in Alaska, as a component in the appropriate Regional Office.

(e) Regional Advisory Council

(1) Establishment

Each Regional Administrator shall establish a Regional Advisory Council.

(2) Nominations

A State, local, or tribal government located within the geographic area served by the Regional Office may nominate officials, including Adjutants General and emergency managers, to serve as members of the Regional Advisory Council for that region.

(3) Responsibilities

Each Regional Advisory Council shall—

(A) advise the Regional Administrator on emergency management issues specific to that region;

(B) identify any geographic, demographic, or other characteristics peculiar to any State, local, or tribal government within the region that might make preparedness, protection, response, recovery, or mitigation more complicated or difficult; and

(C) advise the Regional Administrator of any weaknesses or deficiencies in preparedness, protection, response, recovery, and mitigation for any State, local, and tribal government within the region of which the Regional Advisory Council is aware.

(f) Regional Office strike teams

(1) In general

In coordination with other relevant Federal agencies, each Regional Administrator shall oversee multi-agency strike teams authorized under section 5144 of title 42 that shall consist of—

(A) a designated Federal coordinating officer;

(B) personnel trained in incident management;

(C) public affairs, response and recovery, and communications support personnel;

(D) a defense coordinating officer;

(E) liaisons to other Federal agencies;

(F) such other personnel as the Administrator or Regional Administrator determines appropriate; and

(G) individuals from the agencies with primary responsibility for each of the emergency support functions in the National Response Plan.

(2) Other duties

The duties of an individual assigned to a Regional Office strike team from another relevant

agency when such individual is not functioning as a member of the strike team shall be consistent with the emergency preparedness activities of the agency that employs such individual.

(3) Location of members

The members of each Regional Office strike team, including representatives from agencies other than the Department, shall be based primarily within the region that corresponds to that strike team.

(4) Coordination

Each Regional Office strike team shall coordinate the training and exercises of that strike team with the State, local, and tribal governments and private sector and nongovernmental entities which the strike team shall support when a natural disaster, act of terrorism, or other man-made disaster occurs.

(5) Preparedness

Each Regional Office strike team shall be trained as a unit on a regular basis and equipped and staffed to be well prepared to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

(6) Authorities

If the Administrator determines that statutory authority is inadequate for the preparedness and deployment of individuals in strike teams under this subsection, the Administrator shall report to Congress regarding the additional statutory authorities that the Administrator determines are necessary.

(Pub. L. 107–296, title V, §507, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1401; amended Pub. L. 110–53, title IV, §404, Aug. 3, 2007, 121 Stat. 303.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 317, Pub. L. 107–296, title V, §507, Nov. 25, 2002, 116 Stat. 2214, related to the role of the Federal Emergency Management Agency, prior to repeal by Pub. L. 109–295, title VI, §611(4), Oct. 4. 2006, 120 Stat. 1395.

AMENDMENTS

2007—Subsec. (c)(2)(I) to (K). Pub. L. 110–53 added subpars. (I) and (J) and redesignated former subpar. (I) as (K).

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective Mar. 31, 2007, see section 614(b)(3) of Pub. L. 109–295, set out as a note under section 701 of this title.

§318. National Advisory Council

(a) Establishment

Not later than 60 days after October 4, 2006, the Secretary shall establish an advisory body under section 451(a) of this title to ensure effective and ongoing coordination of Federal preparedness, protection, response, recovery, and mitigation for natural disasters, acts of terrorism, and other man-made disasters, to be known as the National Advisory Council.

(b) Responsibilities

(1) In general

The National Advisory Council shall advise the Administrator on all aspects of emergency management. The National Advisory Council shall incorporate State, local, and tribal government and private sector input in the development and revision of the national preparedness goal, the national preparedness system, the National Incident Management System, the National Response Plan, and other related plans and strategies.

(2) Consultation on grants

To ensure input from and coordination with State, local, and tribal governments and emergency response providers, the Administrator shall regularly consult and work with the National Advisory Council on the administration and assessment of grant programs administered by the Department, including with respect to the development of program guidance and the development and evaluation of risk-assessment methodologies, as appropriate.

(c) Membership

(1) In general

The members of the National Advisory Council shall be appointed by the Administrator, and shall, to the extent practicable, represent a geographic (including urban and rural) and substantive cross section of officials, emergency managers, and emergency response providers from State, local, and tribal governments, the private sector, and nongovernmental organizations, including as appropriate—

(A) members selected from the emergency management field and emergency response providers, including fire service, law enforcement, hazardous materials response, emergency medical services, and emergency management personnel, or organizations representing such individuals;

(B) health scientists, emergency and inpatient medical providers, and public health professionals;

(C) experts from Federal, State, local, and tribal governments, and the private sector, representing standards-setting and accrediting organizations, including representatives from the voluntary consensus codes and standards development community, particularly those with expertise in the emergency preparedness and response field;

(D) State, local, and tribal government officials with expertise in preparedness, protection, response, recovery, and mitigation, including Adjutants General;

(E) elected State, local, and tribal government executives;

(F) experts in public and private sector infrastructure protection, cybersecurity, and communications;

(G) representatives of individuals with disabilities and other populations with special needs; and

(H) such other individuals as the Administrator determines to be appropriate.

(2) Coordination with the Departments of Health and Human Services and Transportation

In the selection of members of the National Advisory Council who are health or emergency medical services professionals, the Administrator shall work with the Secretary of Health and Human Services and the Secretary of Transportation.

(3) Ex officio members

The Administrator shall designate 1 or more officers of the Federal Government to serve as ex officio members of the National Advisory Council.

(4) Terms of office

(A) In general

Except as provided in subparagraph (B), the term of office of each member of the National Advisory Council shall be 3 years.

(B) Initial appointments

Of the members initially appointed to the National Advisory Council—

(i) one-third shall be appointed for a term of 1 year; and
(ii) one-third shall be appointed for a term of 2 years.

(d) RESPONSE Subcommittee

(1) Establishment

Not later than 30 days after December 16, 2016, the Administrator shall establish, as a subcommittee of the National Advisory Council, the Railroad Emergency Services Preparedness, Operational Needs, and Safety Evaluation Subcommittee (referred to in this subsection as the "RESPONSE Subcommittee").

(2) Membership

Notwithstanding subsection (c), the RESPONSE Subcommittee shall be composed of the following:

(A) The Deputy Administrator, Protection and National Preparedness of the Federal Emergency Management Agency, or designee.

(B) The Chief Safety Officer of the Pipeline and Hazardous Materials Safety Administration, or designee.

(C) The Associate Administrator for Hazardous Materials Safety of the Pipeline and Hazardous Materials Safety Administration, or designee.

(D) The Assistant Director for Emergency Communications, or designee.

(E) The Director for the Office of Railroad, Pipeline and Hazardous Materials Investigations of the National Transportation Safety Board, or designee.

(F) The Chief Safety Officer and Associate Administrator for Railroad Safety of the Federal Railroad Administration, or designee.

(G) The Assistant Administrator for Security Policy and Industry Engagement of the Transportation Security Administration, or designee.

(H) The Assistant Commandant for Response Policy of the Coast Guard, or designee.

(I) The Assistant Administrator for the Office of Solid Waste and Emergency Response of the Environmental Protection Agency, or designee.

(J) Such other qualified individuals as the co-chairpersons shall jointly appoint as soon as practicable after December 16, 2016, from among the following:

(i) Members of the National Advisory Council that have the requisite technical knowledge and expertise to address rail emergency response issues, including members from the following disciplines:

(I) Emergency management and emergency response providers, including fire service, law enforcement, hazardous materials response, and emergency medical services.

(II) State, local, and tribal government officials.

(ii) Individuals who have the requisite technical knowledge and expertise to serve on the RESPONSE Subcommittee, including at least 1 representative from each of the following:

(I) The rail industry.

(II) Rail labor.

(III) Persons who offer oil for transportation by rail.

(IV) The communications industry.

(V) Emergency response providers, including individuals nominated by national organizations representing State and local governments and emergency responders.

(VI) Emergency response training providers.

(VII) Representatives from tribal organizations.

(VIII) Technical experts.

(IX) Vendors, developers, and manufacturers of systems, facilities, equipment, and capabilities for emergency responder services.

(iii) Representatives of such other stakeholders and interested and affected parties as the co-chairpersons consider appropriate.

(3) Co-chairpersons

The members described in subparagraphs (A) and (B) of paragraph (2) shall serve as the co-chairpersons of the RESPONSE Subcommittee.

(4) Initial meeting

The initial meeting of the RESPONSE Subcommittee shall take place not later than 90 days after December 16, 2016.

(5) Consultation with nonmembers

The RESPONSE Subcommittee and the program offices for emergency responder training and resources shall consult with other relevant agencies and groups, including entities engaged in federally funded research and academic institutions engaged in relevant work and research, which are not represented on the RESPONSE Subcommittee to consider new and developing technologies and methods that may be beneficial to preparedness and response to rail hazardous materials incidents.

(6) Recommendations

The RESPONSE Subcommittee shall develop recommendations, as appropriate, for improving emergency responder training and resource allocation for hazardous materials incidents involving railroads after evaluating the following topics:

(A) The quality and application of training for State and local emergency responders related to rail hazardous materials incidents, including training for emergency responders serving small communities near railroads, including the following:

(i) Ease of access to relevant training for State and local emergency responders, including an analysis of—

(I) the number of individuals being trained;

(II) the number of individuals who are applying;

(III) whether current demand is being met;

(IV) current challenges; and

(V) projected needs.

(ii) Modernization of training course content related to rail hazardous materials incidents, with a particular focus on fluctuations in oil shipments by rail, including regular and ongoing evaluation of course opportunities, adaptation to emerging trends, agency and private sector outreach, effectiveness and ease of access for State and local emergency responders.

(iii) Identification of overlap in training content and identification of opportunities to develop complementary courses and materials among governmental and nongovernmental entities.

(iv) Online training platforms, train-the-trainer, and mobile training options.

(B) The availability and effectiveness of Federal, State, local, and nongovernmental funding levels related to training emergency responders for rail hazardous materials incidents, including emergency responders serving small communities near railroads, including—

(i) identifying overlap in resource allocations;

(ii) identifying cost savings measures that can be implemented to increase training opportunities;

(iii) leveraging government funding with nongovernmental funding to enhance training opportunities and fill existing training gaps;

(iv) adaptation of priority settings for agency funding allocations in response to emerging trends;

(v) historic levels of funding across Federal agencies for rail hazardous materials incident response and training, including funding provided by the private sector to public entities or in conjunction with Federal programs; and

(vi) current funding resources across agencies.

(C) The strategy for integrating commodity flow studies, mapping, and rail and hazardous materials databases for State and local emergency responders and increasing the rate of access to the individual responder in existing or emerging communications technology.

(7) Report

(A) In general

Not later than 1 year after December 16, 2016, the RESPONSE Subcommittee shall submit a report to the National Advisory Council that—

(i) includes the recommendations developed under paragraph (6);

(ii) specifies the timeframes for implementing any such recommendations that do not require congressional action; and

(iii) identifies any such recommendations that do require congressional action.

(B) Review

Not later than 30 days after receiving the report under subparagraph (A), the National Advisory Council shall begin a review of the report. The National Advisory Council may ask for additional clarification, changes, or other information from the RESPONSE Subcommittee to assist in the approval of the recommendations.

(C) Recommendation

Once the National Advisory Council approves the recommendations of the RESPONSE Subcommittee, the National Advisory Council shall submit the report to—

(i) the co-chairpersons of the RESPONSE Subcommittee;

(ii) the head of each other agency represented on the RESPONSE Subcommittee;

(iii) the Committee on Homeland Security and Governmental Affairs of the Senate;

(iv) the Committee on Commerce, Science, and Transportation of the Senate;

(v) the Committee on Homeland Security of the House of Representatives; and

(vi) the Committee on Transportation and Infrastructure of the House of Representatives.

(8) Interim activity

(A) Updates and oversight

After the submission of the report by the National Advisory Council under paragraph (7), the Administrator shall—

(i) provide annual updates to the congressional committees referred to in paragraph (7)(C) regarding the status of the implementation of the recommendations developed under paragraph (6); and

(ii) coordinate the implementation of the recommendations described in paragraph (6)(G)(i), as appropriate.

(B) Sunset

The requirements of subparagraph (A) shall terminate on the date that is 2 years after the date of the submission of the report required under paragraph (7)(A).

(9) Termination

The RESPONSE Subcommittee shall terminate not later than 90 days after the submission of the report required under paragraph (7)(C).

(e) Applicability of chapter 10 of title 5

(1) In general

Notwithstanding section 451(a) of this title and subject to paragraph (2), chapter 10 of title 5, including subsections (a), (b), and (d) of section 1009 of title 5, and section 552b(c) of title 5 shall apply to the National Advisory Council.

(2) Termination

Section 1013(a)(2) of title 5 shall not apply to the National Advisory Council.

(Pub. L. 107–296, title V, §508, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1403; amended Pub. L. 110–53, title I, §102(a), Aug. 3, 2007, 121 Stat. 293; Pub. L. 114–321, §2, Dec. 16, 2016, 130 Stat. 1623; Pub. L. 115–278, §2(g)(4)(A), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 117–286, §4(a)(15), Dec. 27, 2022, 136 Stat. 4306.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 508 of Pub. L. 107–296 was renumbered section 519 and is classified to section 321h of this title.

AMENDMENTS

2022—Subsec. (e). Pub. L. 117–286, §4(a)(15)(A), substituted "chapter 10 of title 5" for "Federal Advisory Committee Act" in heading.

Subsec. (e)(1). Pub. L. 117–286, §4(a)(15)(B), substituted "chapter 10 of title 5, including subsections (a), (b), and (d) of section 1009 of title 5," for "the Federal Advisory Committee Act (5 U.S.C. App.), including subsections (a), (b), and (d) of section 10 of such Act,".

Subsec. (e)(2). Pub. L. 117–286, §4(a)(15)(C), substituted "Section 1013(a)(2) of title 5" for "Section 14(a)(2) of the Federal Advisory Committee Act (5 U.S.C. App.)".

2018—Subsec. (d)(2)(D). Pub. L. 115–278 substituted "The Assistant Director for Emergency Communications" for "The Director of the Office of Emergency Communications of the Department of Homeland Security".

2016—Subsecs. (d), (e). Pub. L. 114–321 added subsec. (d) and redesignated former subsec. (d) as (e).

2007—Subsec. (b). Pub. L. 110–53 designated existing provisions as par. (1), inserted heading, and added par. (2).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

EFFECTIVE DATE

Section effective Mar. 31, 2007, see section 614(b)(3) of Pub. L. 109–295, set out as a note under section 701 of this title.

§319. National Integration Center

(a) In general

There is established in the Agency a National Integration Center.

(b) Responsibilities

(1) In general

The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the National Response Plan, and any successor to such system or plan.

(2) Specific responsibilities

The National Integration Center shall periodically review, and revise as appropriate, the National Incident Management System and the National Response Plan, including—

(A) establishing, in consultation with the Director of the Corporation for National and

Community Service, a process to better use volunteers and donations;

(B) improving the use of Federal, State, local, and tribal resources and ensuring the effective use of emergency response providers at emergency scenes; and

(C) revising the Catastrophic Incident Annex, finalizing and releasing the Catastrophic Incident Supplement to the National Response Plan, and ensuring that both effectively address response requirements in the event of a catastrophic incident.

(c) Incident management

(1) In general

(A) National Response Plan

The Secretary, acting through the Administrator, shall ensure that the National Response Plan provides for a clear chain of command to lead and coordinate the Federal response to any natural disaster, act of terrorism, or other man-made disaster.

(B) Administrator

The chain of the command specified in the National Response Plan shall—

(i) provide for a role for the Administrator consistent with the role of the Administrator as the principal emergency management advisor to the President, the Homeland Security Council, and the Secretary under section 313(c)(4) of this title and the responsibility of the Administrator under the Post-Katrina Emergency Management Reform Act of 2006, and the amendments made by that Act, relating to natural disasters, acts of terrorism, and other man-made disasters; and

(ii) provide for a role for the Federal Coordinating Officer consistent with the responsibilities under section 5143(b) of title 42.

(2) Principal Federal Official; Joint Task Force

The Principal Federal Official (or the successor thereto) or Director of a Joint Task Force established under section 348 of this title shall not—

(A) direct or replace the incident command structure established at the incident; or

(B) have directive authority over the Senior Federal Law Enforcement Official, Federal Coordinating Officer, or other Federal and State officials.

(Pub. L. 107–296, title V, §509, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1405; amended Pub. L. 114–328, div. A, title XIX, §1901(d)(2), Dec. 23, 2016, 130 Stat. 2670.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Post-Katrina Emergency Management Reform Act of 2006, referred to in subsec. (c)(1)(B)(i), is title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1394. For complete classification of this Act to the Code, see Short Title note set out under section 701 of this title and Tables.

PRIOR PROVISIONS

A prior section 509 of Pub. L. 107–296 was renumbered section 520 and is classified to section 321i of this title.

AMENDMENTS

2016—Subsec. (c)(2). Pub. L. 114–328 inserted "; Joint Task Force" after "Official" in heading and "or Director of a Joint Task Force established under section 348 of this title" before "shall" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L.

109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

§320. Credentialing and typing

(a) In general

The Administrator shall enter into a memorandum of understanding with the administrators of the Emergency Management Assistance Compact, State, local, and tribal governments, and organizations that represent emergency response providers, to collaborate on developing standards for deployment capabilities, including for credentialing and typing of incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to natural disasters, acts of terrorism, and other man-made disasters.

(b) Distribution

(1) In general

Not later than 1 year after August 3, 2007, the Administrator shall provide the standards developed under subsection (a), including detailed written guidance, to—

(A) each Federal agency that has responsibilities under the National Response Plan to aid that agency with credentialing and typing incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster; and

(B) State, local, and tribal governments, to aid such governments with credentialing and typing of State, local, and tribal incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster.

(2) Assistance

The Administrator shall provide expertise and technical assistance to aid Federal, State, local, and tribal government agencies with credentialing and typing incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster.

(c) Credentialing and typing of personnel

Not later than 6 months after receiving the standards provided under subsection (b), each Federal agency with responsibilities under the National Response Plan shall ensure that incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other manmade disaster are credentialed and typed in accordance with this section.

(d) Consultation on health care standards

In developing standards for credentialing health care professionals under this section, the Administrator shall consult with the Secretary of Health and Human Services.

(Pub. L. 107–296, title V, §510, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1406; amended Pub. L. 110–53, title IV, §408, Aug. 3, 2007, 121 Stat. 304.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 510 of Pub. L. 107–296 was renumbered section 521 and is classified to section 321j of this title.

Another prior section 510 of Pub. L. 107–296 was classified to section 321 of this title, prior to repeal by Pub. L. 109–295.

AMENDMENTS

2007—Pub. L. 110–53 designated existing provisions as subsec. (a), inserted heading, substituted "for credentialing and typing of incident management personnel, emergency response providers, and other personnel (including temporary personnel) and" for "credentialing of personnel and typing of", and added subsecs. (b) to (d).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

SCOPE OF PRACTICE IN PUBLIC HEALTH EMERGENCY

Pub. L. 119–86, div. A, title V, §542, Apr. 30, 2026, 140 Stat. 807, provided that: "Section 16005(c) of title VI of division B of the Coronavirus Aid, Relief, and Economic Security Act (Public Law 116–136) [set out below] shall be applied as if the language read as follows: 'Subsection (a) shall apply until September 30, 2026.'."

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 117–328, div. F, title V, §543, Dec. 29, 2022, 136 Stat. 4757.

Pub. L. 117–103, div. F, title V, §541, Mar. 15, 2022, 136 Stat. 344.

Pub. L. 116–136, div. B, title VI, §16005, Mar. 27, 2020, 134 Stat. 545, provided that:

"(a) Notwithstanding any other provision of law regarding the licensure of health-care providers, a health-care professional described in subsection (b) may practice the health profession or professions of the health-care professional at any location in any State, the District of Columbia, or Commonwealth, territory, or possession of the United States, or any location designated by the Secretary, regardless of where such health-care professional or the patient is located, so long as the practice is within the scope of the authorized Federal duties of such health-care professional.

"(b) DEFINITION.—As used in this section, the term 'health-care professional' means an individual (other than a member of the Coast Guard, a civilian employee of the Coast Guard, member of the Public Health Service who is assigned to the Coast Guard, or an individual with whom the Secretary, pursuant to 10 U.S.C. 1091, has entered into a personal services contract to carry out health care responsibilities of the Secretary at a medical treatment facility of the Coast Guard) who—

"(1) is—

"(A) an employee of the Department of Homeland Security,

"(B) a detailee to the Department from another Federal agency,

"(C) a personal services contractor of the Department, or

"(D) hired under a Contract for Services;

"(2) performs health care services as part of duties of the individual in that capacity;

"(3) has a current, valid, and unrestricted equivalent license certification that is—

"(A) issued by a State, the District of Columbia, or a Commonwealth, territory, or possession of the United States; and

"(B) for the practice of medicine, osteopathic medicine, dentistry, nursing, emergency medical services, or another health profession; and

"(4) is not affirmatively excluded from practice in the licensing or certifying jurisdiction or in any other jurisdiction.

"(c) Subsection (a) shall apply during the incident period of the emergency declared by the President on March 13, 2020, pursuant to section 501(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act [Pub. L. 93–288] (42 U.S.C. 5121(b) [5191(b)]), and to any subsequent major declaration under section 401 of such Act [42 U.S.C. 5170] that supersedes such emergency declaration."

§321. The National Infrastructure Simulation and Analysis Center

(a) Definition

In this section, the term "National Infrastructure Simulation and Analysis Center" means the

National Infrastructure Simulation and Analysis Center established under section 5195c(d) of title 42.

(b) Authority

(1) In general

There is in the Department the National Infrastructure Simulation and Analysis Center which shall serve as a source of national expertise to address critical infrastructure protection and continuity through support for activities related to—

(A) counterterrorism, threat assessment, and risk mitigation; and

(B) a natural disaster, act of terrorism, or other man-made disaster.

(2) Infrastructure modeling

(A) Particular support

The support provided under paragraph (1) shall include modeling, simulation, and analysis of the systems and assets comprising critical infrastructure, in order to enhance preparedness, protection, response, recovery, and mitigation activities.

(B) Relationship with other agencies

Each Federal agency and department with critical infrastructure responsibilities under Homeland Security Presidential Directive 7, or any successor to such directive, shall establish a formal relationship, including an agreement regarding information sharing, between the elements of such agency or department and the National Infrastructure Simulation and Analysis Center, through the Department.

(C) Purpose

(i) In general

The purpose of the relationship under subparagraph (B) shall be to permit each Federal agency and department described in subparagraph (B) to take full advantage of the capabilities of the National Infrastructure Simulation and Analysis Center (particularly vulnerability and consequence analysis), consistent with its work load capacity and priorities, for real-time response to reported and projected natural disasters, acts of terrorism, and other man-made disasters.

(ii) Recipient of certain support

Modeling, simulation, and analysis provided under this subsection shall be provided to relevant Federal agencies and departments, including Federal agencies and departments with critical infrastructure responsibilities under Homeland Security Presidential Directive 7, or any successor to such directive.

(Pub. L. 107–296, title V, §511, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1406.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 321, Pub. L. 107–296, title V, §510, as added Pub. L. 108–458, title VII, §7303(d), Dec. 17, 2004, 118 Stat. 3844, related to urban and other high risk area communications capabilities, prior to repeal by Pub. L. 109–295, title VI, §611(5), Oct. 4, 2006, 120 Stat. 1395.

§321a. Evacuation plans and exercises

(a) In general

Notwithstanding any other provision of law, and subject to subsection (d), grants made to States or local or tribal governments by the Department through the State Homeland Security Grant Program

or the Urban Area Security Initiative may be used to—

(1) establish programs for the development and maintenance of mass evacuation plans under subsection (b) in the event of a natural disaster, act of terrorism, or other man-made disaster;

(2) prepare for the execution of such plans, including the development of evacuation routes and the purchase and stockpiling of necessary supplies and shelters; and

(3) conduct exercises of such plans.

(b) Plan development

In developing the mass evacuation plans authorized under subsection (a), each State, local, or tribal government shall, to the maximum extent practicable—

(1) establish incident command and decision making processes;

(2) ensure that State, local, and tribal government plans, including evacuation routes, are coordinated and integrated;

(3) identify primary and alternative evacuation routes and methods to increase evacuation capabilities along such routes such as conversion of two-way traffic to one-way evacuation routes;

(4) identify evacuation transportation modes and capabilities, including the use of mass and public transit capabilities, and coordinating and integrating evacuation plans for all populations including for those individuals located in hospitals, nursing homes, and other institutional living facilities;

(5) develop procedures for informing the public of evacuation plans before and during an evacuation, including individuals—

(A) with disabilities or other special needs, including the elderly;

(B) with limited English proficiency; or

(C) who might otherwise have difficulty in obtaining such information; and

(6) identify shelter locations and capabilities.

(c) Assistance

(1) In general

The Administrator may establish any guidelines, standards, or requirements determined appropriate to administer this section and to ensure effective mass evacuation planning for State, local, and tribal areas.

(2) Requested assistance

The Administrator shall make assistance available upon request of a State, local, or tribal government to assist hospitals, nursing homes, and other institutions that house individuals with special needs to establish, maintain, and exercise mass evacuation plans that are coordinated and integrated into the plans developed by that State, local, or tribal government under this section.

(d) Multipurpose funds

Nothing in this section may be construed to preclude a State, local, or tribal government from using grant funds in a manner that enhances preparedness for a natural or man-made disaster unrelated to an act of terrorism, if such use assists such government in building capabilities for terrorism preparedness.

(Pub. L. 107–296, title V, §512, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1407; amended Pub. L. 110–53, title I, §102(b), Aug. 3, 2007, 121 Stat. 293.)

EDITORIAL NOTES

AMENDMENTS

2007—Subsec. (b)(5)(A). Pub. L. 110–53 inserted ", including the elderly" after "needs".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

§321b. Disability Coordinator

(a) In general

After consultation with organizations representing individuals with disabilities, the National Council on Disabilities, and the Interagency Coordinating Council on Preparedness and Individuals with Disabilities, established under Executive Order No. 13347, the Administrator shall appoint a Disability Coordinator. The Disability Coordinator shall report directly to the Administrator, in order to ensure that the needs of individuals with disabilities are being properly addressed in emergency preparedness and disaster relief.

(b) Responsibilities

The Disability Coordinator shall be responsible for—

(1) providing guidance and coordination on matters related to individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(2) interacting with the staff of the Agency, the National Council on Disabilities, the Interagency Coordinating Council on Preparedness and Individuals with Disabilities established under Executive Order No. 13347, other agencies of the Federal Government, and State, local, and tribal government authorities regarding the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(3) consulting with organizations that represent the interests and rights of individuals with disabilities about the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(4) ensuring the coordination and dissemination of best practices and model evacuation plans for individuals with disabilities;

(5) ensuring the development of training materials and a curriculum for training of emergency response providers, State, local, and tribal government officials, and others on the needs of individuals with disabilities;

(6) promoting the accessibility of telephone hotlines and websites regarding emergency preparedness, evacuations, and disaster relief;

(7) working to ensure that video programming distributors, including broadcasters, cable operators, and satellite television services, make emergency information accessible to individuals with hearing and vision disabilities;

(8) ensuring the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

(9) providing guidance and implementing policies to ensure that the rights and wishes of individuals with disabilities regarding post-evacuation residency and relocation are respected;

(10) ensuring that meeting the needs of individuals with disabilities are included in the components of the national preparedness system established under section 744 of this title; and

(11) any other duties as assigned by the Administrator.

(Pub. L. 107–296, title V, §513, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1408.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order No. 13347, referred to in subsecs. (a) and (b)(2), is set out as a note under section 314 of this title.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

§321c. Department and Agency officials

(a) Deputy Administrators

The President may appoint, by and with the advice and consent of the Senate, not more than 4 Deputy Administrators to assist the Administrator in carrying out this subchapter.

(b) United States Fire Administration

The Administrator of the United States Fire Administration shall have a rank equivalent to an assistant secretary of the Department.

(Pub. L. 107–296, title V, §514, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1409; amended Pub. L. 115–278, §2(g)(4)(B), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsecs. (b), (c). Pub. L. 115–278 redesignated subsec. (c) as (b) and struck out former subsec. (b). Prior to amendment, text of subsec. (b) read as follows: "There is in the Department an Assistant Secretary for Cybersecurity and Communications."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective Mar. 31, 2007, see section 614(b)(3) of Pub. L. 109–295, set out as a note under section 701 of this title.

§321d. National Operations Center

(a) Definition

In this section, the term "situational awareness" means information gathered from a variety of sources that, when communicated to emergency managers, decision makers, and other appropriate officials, can form the basis for incident management decisionmaking and steady-state activity.

(b) Establishment

The National Operations Center is the principal operations center for the Department and shall—

(1) provide situational awareness and a common operating picture for the entire Federal Government, and for State, local, tribal, and territorial governments, the private sector, and international partners as appropriate, for events, threats, and incidents involving a natural disaster, act of terrorism, or other man-made disaster;

(2) ensure that critical terrorism and disaster-related information reaches government decision-makers; and

(3) enter into agreements with other Federal operations centers and other homeland security

partners, as appropriate, to facilitate the sharing of information.

(c) State and local emergency responder representation

(1) Establishment of positions

The Secretary shall establish a position, on a rotating basis, for a representative of State and local emergency responders at the National Operations Center established under subsection (b) to ensure the effective sharing of information between the Federal Government and State and local emergency response services.

(2) Management

The Secretary shall manage the position established pursuant to paragraph (1) in accordance with such rules, regulations, and practices as govern other similar rotating positions at the National Operations Center.

(Pub. L. 107–296, title V, §515, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1409; amended Pub. L. 110–376, §8, Oct. 8, 2008, 122 Stat. 4060; Pub. L. 114–328, div. A, title XIX, §1909, Dec. 23, 2016, 130 Stat. 2681.)

EDITORIAL NOTES

AMENDMENTS

2016—Subsec. (a). Pub. L. 114–328, §1909(1), substituted "emergency managers, decision makers, and other appropriate officials" for "emergency managers and decision makers" and inserted "and steady-state activity" before period at end.

Subsec. (b)(1). Pub. L. 114–328, §1909(2)(A), substituted "tribal, and territorial governments, the private sector, and international partners" for "and tribal governments" and "for events, threats, and incidents involving" for "in the event of" and struck out "and" at end.

Subsec. (b)(2). Pub. L. 114–328, §1909(2)(B), substituted "; and" for period at end.

Subsec. (b)(3). Pub. L. 114–328, §1909(2)(C), added par. (3).

Subsec. (c). Pub. L. 114–328, §1909(4)(A), substituted "emergency responder" for "fire service" in heading.

Subsec. (c)(1). Pub. L. 114–328, §1909(4)(B), added par. (1) and struck out former par. (1). Prior to amendment, text read as follows: "The Secretary shall, in consultation with the Administrator of the United States Fire Administration, establish a fire service position at the National Operations Center established under subsection (b) to ensure the effective sharing of information between the Federal Government and State and local fire services."

Subsec. (c)(2), (3). Pub. L. 114–328, §1909(4)(C), (D), redesignated par. (3) as (2) and struck out former par. (2). Prior to amendment, text of par. (2) read as follows: "The Secretary shall designate, on a rotating basis, a State or local fire service official for the position described in paragraph (1)."

2008—Subsec. (c). Pub. L. 110–376 added subsec. (c).

§321e. Repealed. Pub. L. 115–387, §2(c)(1), Dec. 21, 2018, 132 Stat. 5166

Section, Pub. L. 107–296, title V, §516, as added Pub. L. 109–295, title VI, §611(13), Oct. 4, 2006, 120 Stat. 1409; amended Pub. L. 112–166, §2(f)(4), Aug. 10, 2012, 126 Stat. 1285, related to establishment, qualifications, and responsibilities of Chief Medical Officer. See section 597 of this title.

§321f. Nuclear incident response

(a) In general

At the direction of the Secretary (in connection with an actual or threatened terrorist attack, major disaster, or other emergency in the United States), the Nuclear Incident Response Team shall operate as an organizational unit of the Department. While so operating, the Nuclear Incident Response Team shall be subject to the direction, authority, and control of the Secretary.

(b) Rule of construction

Nothing in this subchapter shall be construed to limit the ordinary responsibility of the Secretary of Energy and the Administrator of the Environmental Protection Agency for organizing, training, equipping, and utilizing their respective entities in the Nuclear Incident Response Team, or (subject to the provisions of this subchapter) from exercising direction, authority, and control over them when they are not operating as a unit of the Department.

(Pub. L. 107–296, title V, §517, formerly §504, Nov. 25, 2002, 116 Stat. 2213; renumbered §517, Pub. L. 109–295, title VI, §611(6), Oct. 4, 2006, 120 Stat. 1395.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 314 of this title prior to renumbering by Pub. L. 109–295.

§321g. Conduct of certain public health-related activities

(a) In general

With respect to all public health-related activities to improve State, local, and hospital preparedness and response to chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities and preparedness goals and further develop a coordinated strategy for such activities in collaboration with the Secretary.

(b) Evaluation of progress

In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in such subsection.

(Pub. L. 107–296, title V, §518, formerly §505, Nov. 25, 2002, 116 Stat. 2213; renumbered §518, Pub. L. 109–295, title VI, §611(6), Oct. 4, 2006, 120 Stat. 1395.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 315 of this title prior to renumbering by Pub. L. 109–295.

§321h. Use of national private sector networks in emergency response

To the maximum extent practicable, the Secretary shall use national private sector networks and infrastructure for emergency response to chemical, biological, radiological, nuclear, or explosive disasters, and other major disasters.

(Pub. L. 107–296, title V, §519, formerly §508, Nov. 25, 2002, 116 Stat. 2215; renumbered §519, Pub. L. 109–295, title VI, §611(6), Oct. 4, 2006, 120 Stat. 1395.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 318 of this title prior to renumbering by Pub. L. 109–295.

§321i. Use of commercially available technology, goods, and services

It is the sense of Congress that—

(1) the Secretary should, to the maximum extent possible, use off-the-shelf commercially developed technologies to ensure that the Department's information technology systems allow the Department to collect, manage, share, analyze, and disseminate information securely over multiple channels of communication; and

(2) in order to further the policy of the United States to avoid competing commercially with the private sector, the Secretary should rely on commercial sources to supply the goods and services needed by the Department.

(Pub. L. 107–296, title V, §520, formerly §509, Nov. 25, 2002, 116 Stat. 2215; renumbered §520, Pub. L. 109–295, title VI, §611(6), Oct. 4, 2006, 120 Stat. 1395.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 319 of this title prior to renumbering by Pub. L. 109–295.

§321j. Procurement of security countermeasures for Strategic National Stockpile

(a) Authorization of appropriations

For the procurement of security countermeasures under section 247d–6b(c) of title 42 (referred to in this section as the "security countermeasures program"), there is authorized to be appropriated up to $5,593,000,000 for the fiscal years 2004 through 2013. Of the amounts appropriated under the preceding sentence, not to exceed $3,418,000,000 may be obligated during the fiscal years 2004 through 2008, of which not to exceed $890,000,000 may be obligated during fiscal year 2004. None of the funds made available under this subsection shall be used to procure countermeasures to diagnose, mitigate, prevent, or treat harm resulting from any naturally occurring infectious disease or other public health threat that are not security countermeasures under section 247d–6b(c)(1)(B) of title 42.[1]

(b) Special reserve fund

For purposes of the security countermeasures program, the term "special reserve fund" means the "Biodefense Countermeasures" appropriations account or any other appropriation made under subsection (a).

(c) Availability

Amounts appropriated under subsection (a) become available for a procurement under the security countermeasures program only upon the approval by the President of such availability for the procurement in accordance with paragraph (6)(B) of such program.

(d) Related authorizations of appropriations

(1) Threat assessment capabilities

For the purpose of carrying out the responsibilities of the Secretary for terror threat assessment under the security countermeasures program, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006, for the hiring of professional personnel within the Office of Intelligence and Analysis, who shall be analysts responsible for chemical, biological, radiological, and nuclear threat assessment (including but not limited to analysis of chemical, biological, radiological, and nuclear agents, the means by which such agents could be weaponized or used in a terrorist attack, and the capabilities, plans, and intentions of terrorists and other non-state actors who may have or acquire such agents). All such analysts shall meet the applicable standards and qualifications for the performance of intelligence activities promulgated by the Director of Central Intelligence pursuant to section 403–4 [1] of title 50.

(2) Intelligence sharing infrastructure

For the purpose of carrying out the acquisition and deployment of secure facilities (including

information technology and physical infrastructure, whether mobile and temporary, or permanent) sufficient to permit the Secretary to receive, not later than 180 days after July 21, 2004, all classified information and products to which the Under Secretary for Intelligence and Analysis is entitled under part A of subchapter II, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006.

(Pub. L. 107–296, title V, §521, formerly §510, as added Pub. L. 108–276, §3(b)(2), July 21, 2004, 118 Stat. 852; renumbered §521, Pub. L. 109–295, title VI, §611(7), Oct. 4, 2006, 120 Stat. 1395; amended Pub. L. 109–417, title IV, §403(c), Dec. 19, 2006, 120 Stat. 2874; Pub. L. 110–53, title V, §531(b)(1)(D), Aug. 3, 2007, 121 Stat. 334.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 247d–6b(c)(1)(B) of title 42, referred to in subsec. (a), was in the original "section 319F–2(c)(1)(B)", which was translated as meaning section 319F–2(c)(1)(B) of the Public Health Service Act, to reflect the probable intent of Congress.

Section 403–4 of title 50, referred to in subsec. (d)(1), was repealed and a new section 403–4 enacted by Pub. L. 108–458, title I, §1011(a), Dec. 17, 2004, 118 Stat. 3660, and subsequently editorially reclassified to section 3035 of Title 50, War and National Defense; as so enacted, section 3035 no longer relates to promulgation of standards and qualifications for the performance of intelligence activities.

Part A of subchapter II of this chapter, referred to in subsec. (d)(2), was in the original "subtitle A of title II", meaning subtitle A of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which is classified generally to part A (§121 et seq.) of subchapter II of this chapter. For complete classification of part A to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 320 of this title prior to renumbering by Pub. L. 109–295.

AMENDMENTS

2007—Subsec. (d)(1). Pub. L. 110–53, §531(b)(1)(D)(i), substituted "Office of Intelligence and Analysis" for "Directorate for Information Analysis and Infrastructure Protection".

Subsec. (d)(2). Pub. L. 110–53, §531(b)(1)(D)(ii), substituted "Under Secretary for Intelligence and Analysis" for "Under Secretary for Information Analysis and Infrastructure Protection".

2006—Subsec. (a). Pub. L. 109–417, which directed amendment of section 510(a) of the Homeland Security Act of 2002, Pub. L. 107–296, by inserting a new last sentence, was executed to subsec. (a) of this section to reflect the probable intent of Congress and the redesignation of section 510(a) as 521(a) by Pub. L. 109–295, §611(7).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

[1] *See References in Text note below.*

§321k. Model standards and guidelines for critical infrastructure workers

(a) In general

Not later than 12 months after August 3, 2007, and in coordination with appropriate national

professional organizations, Federal, State, local, and tribal government agencies, and private-sector and nongovernmental entities, the Administrator shall establish model standards and guidelines for credentialing critical infrastructure workers that may be used by a State to credential critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other man-made disaster.

(b) Distribution and assistance

The Administrator shall provide the standards developed under subsection (a), including detailed written guidance, to State, local, and tribal governments, and provide expertise and technical assistance to aid such governments with credentialing critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other manmade disaster.

(Pub. L. 107–296, title V, §522, as added Pub. L. 110–53, title IV, §409(a), Aug. 3, 2007, 121 Stat. 305.)

§321*l*. Guidance and recommendations

(a) In general

Consistent with their responsibilities and authorities under law, as of the day before August 3, 2007, the Administrator and the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the private sector, may develop guidance or recommendations and identify best practices to assist or foster action by the private sector in—

(1) identifying potential hazards and assessing risks and impacts;

(2) mitigating the impact of a wide variety of hazards, including weapons of mass destruction;

(3) managing necessary emergency preparedness and response resources;

(4) developing mutual aid agreements;

(5) developing and maintaining emergency preparedness and response plans, and associated operational procedures;

(6) developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;

(7) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and

(8) developing procedures to respond to requests for information from the media or the public.

(b) Issuance and promotion

Any guidance or recommendations developed or best practices identified under subsection (a) shall be—

(1) issued through the Administrator; and

(2) promoted by the Secretary to the private sector.

(c) Small business concerns

In developing guidance or recommendations or identifying best practices under subsection (a), the Administrator and the Director of the Cybersecurity and Infrastructure Security Agency shall take into consideration small business concerns (under the meaning given that term in section 632 of title 15), including any need for separate guidance or recommendations or best practices, as necessary and appropriate.

(d) Rule of construction

Nothing in this section may be construed to supersede any requirement established under any other provision of law.

(Pub. L. 107–296, title V, §523, as added Pub. L. 110–53, title IX, §901(a), Aug. 3, 2007, 121 Stat. 364; amended Pub. L. 115–278, §2(g)(4)(C), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 117–263, div. G, title LXXI, §7143(c)(1), Dec. 23, 2022, 136 Stat. 3662.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsecs. (a), (c). Pub. L. 117–263 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security".

2018—Subsecs. (a), (c). Pub. L. 115–278 substituted "Director of Cybersecurity and Infrastructure Security" for "Assistant Secretary for Infrastructure Protection".

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out in a note under section 650 of this title.

§321m. Voluntary private sector preparedness accreditation and certification program

(a) Establishment

(1) In general

The Secretary, acting through the officer designated under paragraph (2), shall establish and implement the voluntary private sector preparedness accreditation and certification program in accordance with this section.

(2) Designation of officer

The Secretary shall designate an officer responsible for the accreditation and certification program under this section. Such officer (hereinafter referred to in this section as the "designated officer") shall be one of the following:

(A) The Administrator, based on consideration of—

(i) the expertise of the Administrator in emergency management and preparedness in the United States; and

(ii) the responsibilities of the Administrator as the principal advisor to the President for all matters relating to emergency management in the United States.

(B) The Assistant Secretary for Infrastructure Protection,[1] based on consideration of the expertise of the Assistant Secretary in, and responsibilities for—

(i) protection of critical infrastructure;

(ii) risk assessment methodologies; and

(iii) interacting with the private sector on the issues described in clauses (i) and (ii).

(C) The Under Secretary for Science and Technology, based on consideration of the expertise of the Under Secretary in, and responsibilities associated with, standards.

(3) Coordination

In carrying out the accreditation and certification program under this section, the designated officer shall coordinate with—

(A) the other officers of the Department referred to in paragraph (2), using the expertise and responsibilities of such officers; and

(B) the Special Assistant to the Secretary for the Private Sector, based on consideration of the expertise of the Special Assistant in, and responsibilities for, interacting with the private sector.

(b) Voluntary private sector preparedness standards; voluntary accreditation and certification program for the private sector

(1) Accreditation and certification program

Not later than 210 days after August 3, 2007, the designated officer shall—

(A) begin supporting the development and updating, as necessary, of voluntary preparedness standards through appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards and voluntary consensus standards development organizations; and

(B) in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, each private sector advisory council created under section 112(f)(4) of this title, appropriate representatives of State and local governments, including emergency management officials, and appropriate private sector advisory groups, such as sector coordinating councils and information sharing and analysis centers—

(i) develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification under the program; and

(ii) implement the program under this subsection through any entity with which the designated officer enters into an agreement under paragraph (3)(A), which shall accredit third parties to carry out the certification process under this section.

(2) Program elements

(A) In general

(i) Program

The program developed and implemented under this subsection shall assess whether a private sector entity complies with voluntary preparedness standards.

(ii) Guidelines

In developing the program under this subsection, the designated officer shall develop guidelines for the accreditation and certification processes established under this subsection.

(B) Standards

The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, representatives of appropriate voluntary consensus standards development organizations, each private sector advisory council created under section 112(f)(4) of this title, appropriate representatives of State and local governments, including emergency management officials, and appropriate private sector advisory groups such as sector coordinating councils and information sharing and analysis centers—

(i) shall adopt one or more appropriate voluntary preparedness standards that promote preparedness, which may be tailored to address the unique nature of various sectors within the private sector, as necessary and appropriate, that shall be used in the accreditation and certification program under this subsection; and

(ii) after the adoption of one or more standards under clause (i), may adopt additional voluntary preparedness standards or modify or discontinue the use of voluntary preparedness standards for the accreditation and certification program, as necessary and appropriate to promote preparedness.

(C) Submission of recommendations

In adopting one or more standards under subparagraph (B), the designated officer may receive recommendations from any entity described in that subparagraph relating to appropriate voluntary preparedness standards, including appropriate sector specific standards, for adoption in the program.

(D) Small business concerns

The designated officer and any entity with which the designated officer enters into an agreement under paragraph (3)(A) shall establish separate classifications and methods of

certification for small business concerns (under the meaning given that term in section 632 of title 15) for the program under this subsection.

(E) Considerations

In developing and implementing the program under this subsection, the designated officer shall—

(i) consider the unique nature of various sectors within the private sector, including preparedness standards, business continuity standards, or best practices, established—

(I) under any other provision of Federal law; or

(II) by any Sector Risk Management Agency, as defined under Homeland Security Presidential Directive–7; and

(ii) coordinate the program, as appropriate, with—

(I) other Department private sector related programs; and

(II) preparedness and business continuity programs in other Federal agencies.

(3) Accreditation and certification processes

(A) Agreement

(i) In general

Not later than 210 days after August 3, 2007, the designated officer shall enter into one or more agreements with a highly qualified nongovernmental entity with experience or expertise in coordinating and facilitating the development and use of voluntary consensus standards and in managing or implementing accreditation and certification programs for voluntary consensus standards, or a similarly qualified private sector entity, to carry out accreditations and oversee the certification process under this subsection. An entity entering into an agreement with the designated officer under this clause (hereinafter referred to in this section as a "selected entity") shall not perform certifications under this subsection.

(ii) Contents

A selected entity shall manage the accreditation process and oversee the certification process in accordance with the program established under this subsection and accredit qualified third parties to carry out the certification program established under this subsection.

(B) Procedures and requirements for accreditation and certification

(i) In general

Any selected entity shall collaborate to develop procedures and requirements for the accreditation and certification processes under this subsection, in accordance with the program established under this subsection and guidelines developed under paragraph (2)(A)(ii).

(ii) Contents and use

The procedures and requirements developed under clause (i) shall—

(I) ensure reasonable uniformity in any accreditation and certification processes if there is more than one selected entity; and

(II) be used by any selected entity in conducting accreditations and overseeing the certification process under this subsection.

(iii) Disagreement

Any disagreement among selected entities in developing procedures under clause (i) shall be resolved by the designated officer.

(C) Designation

A selected entity may accredit any qualified third party to carry out the certification process under this subsection.

(D) Disadvantaged business involvement

In accrediting qualified third parties to carry out the certification process under this subsection, a selected entity shall ensure, to the extent practicable, that the third parties include qualified small, minority, women-owned, or disadvantaged business concerns when appropriate. The term "disadvantaged business concern" means a small business that is owned and controlled by socially and economically disadvantaged individuals, as defined in section 124 of title 13, United States Code of Federal Regulations.

(E) Treatment of other certifications

At the request of any entity seeking certification, any selected entity may consider, as appropriate, other relevant certifications acquired by the entity seeking certification. If the selected entity determines that such other certifications are sufficient to meet the certification requirement or aspects of the certification requirement under this section, the selected entity may give credit to the entity seeking certification, as appropriate, to avoid unnecessarily duplicative certification requirements.

(F) Third parties

To be accredited under subparagraph (C), a third party shall—

(i) demonstrate that the third party has the ability to certify private sector entities in accordance with the procedures and requirements developed under subparagraph (B);

(ii) agree to perform certifications in accordance with such procedures and requirements;

(iii) agree not to have any beneficial interest in or any direct or indirect control over—

(I) a private sector entity for which that third party conducts a certification under this subsection; or

(II) any organization that provides preparedness consulting services to private sector entities;

(iv) agree not to have any other conflict of interest with respect to any private sector entity for which that third party conducts a certification under this subsection;

(v) maintain liability insurance coverage at policy limits in accordance with the requirements developed under subparagraph (B); and

(vi) enter into an agreement with the selected entity accrediting that third party to protect any proprietary information of a private sector entity obtained under this subsection.

(G) Monitoring

(i) In general

The designated officer and any selected entity shall regularly monitor and inspect the operations of any third party conducting certifications under this subsection to ensure that the third party is complying with the procedures and requirements established under subparagraph (B) and all other applicable requirements.

(ii) Revocation

If the designated officer or any selected entity determines that a third party is not meeting the procedures or requirements established under subparagraph (B), the selected entity shall—

(I) revoke the accreditation of that third party to conduct certifications under this subsection; and

(II) review any certification conducted by that third party, as necessary and appropriate.

(4) Annual review

(A) In general

The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, appropriate representatives of State

and local governments, including emergency management officials, and each private sector advisory council created under section 112(f)(4) of this title, shall annually review the voluntary accreditation and certification program established under this subsection to ensure the effectiveness of such program (including the operations and management of such program by any selected entity and the selected entity's inclusion of qualified disadvantaged business concerns under paragraph (3)(D)) and make improvements and adjustments to the program as necessary and appropriate.

(B) Review of standards

Each review under subparagraph (A) shall include an assessment of the voluntary preparedness standard or standards used in the program under this subsection.

(5) Voluntary participation

Certification under this subsection shall be voluntary for any private sector entity.

(6) Public listing

The designated officer shall maintain and make public a listing of any private sector entity certified as being in compliance with the program established under this subsection, if that private sector entity consents to such listing.

(c) Rule of construction

Nothing in this section may be construed as—

(1) a requirement to replace any preparedness, emergency response, or business continuity standards, requirements, or best practices established—

(A) under any other provision of federal law; or

(B) by any Sector Risk Management Agency, as those agencies are defined under Homeland Security Presidential Directive–7; or

(2) exempting any private sector entity seeking certification or meeting certification requirements under subsection (b) from compliance with all applicable statutes, regulations, directives, policies, and industry codes of practice.

(Pub. L. 107–296, title V, §524, as added Pub. L. 110–53, title IX, §901(a), Aug. 3, 2007, 121 Stat. 365; amended Pub. L. 116–283, div. H, title XC, §9002(c)(2)(B), Jan. 1, 2021, 134 Stat. 4772.)

EDITORIAL NOTES

AMENDMENTS

2021—Subsec. (b)(2)(E)(i)(II). Pub. L. 116–283, §9002(c)(2)(B)(i), substituted "Sector Risk Management Agency" for "sector-specific agency".

Subsec. (c)(1)(B). Pub. L. 116–283, §9002(c)(2)(B)(ii), substituted "Sector Risk Management Agency" for "sector-specific agency".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to Assistant Secretary for Infrastructure Protection deemed to be a reference to Assistant Director for Infrastructure Security, see section 654(a)(3) of this title. Assistant Secretary for Infrastructure Protection serving on the day before Nov. 16, 2018, authorized to continue to serve as Assistant Director for Infrastructure Security on and after such date, see section 2(b)(4) of Pub. L. 115–278, set out as a note under section 654 of this title.

DEADLINE FOR DESIGNATION OF OFFICER

Pub. L. 110–53, title IX, §901(c), Aug. 3, 2007, 121 Stat. 371, provided that: "The Secretary of Homeland Security shall designate the officer as described in section 524 of the Homeland Security Act of 2002 [6 U.S.C. 321m], as added by subsection (a), by not later than 30 days after the date of the enactment of this Act [Aug. 3, 2007]."

[1] *See Change of Name note below.*

§321n. Acceptance of gifts

(a) Authority

The Secretary may accept and use gifts of property, both real and personal, and may accept gifts of services, including from guest lecturers, for otherwise authorized activities of the Center for Domestic Preparedness that are related to efforts to prevent, prepare for, protect against, or respond to a natural disaster, act of terrorism, or other man-made disaster, including the use of a weapon of mass destruction.

(b) Prohibition

The Secretary may not accept a gift under this section if the Secretary determines that the use of the property or services would compromise the integrity or appearance of integrity of—

(1) a program of the Department; or

(2) an individual involved in a program of the Department.

(c) Report

(1) In general

The Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report disclosing—

(A) any gifts that were accepted under this section during the year covered by the report;

(B) how the gifts contribute to the mission of the Center for Domestic Preparedness; and

(C) the amount of Federal savings that were generated from the acceptance of the gifts.

(2) Publication

Each report required under paragraph (1) shall be made publically available.

(Pub. L. 107–296, title V, §525, as added Pub. L. 111–245, §2(a)(1), Sept. 30, 2010, 124 Stat. 2620.)

§321*o*. Integrated public alert and warning system modernization

(a) In general

To provide timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety, the Administrator shall—

(1) modernize the integrated public alert and warning system of the United States (in this section referred to as the "public alert and warning system") to help ensure that under all conditions the President and, except to the extent the public alert and warning system is in use by the President, Federal agencies and State, tribal, and local governments can alert and warn the civilian population in areas endangered by natural disasters, acts of terrorism, and other man-made disasters or threats to public safety; and

(2) implement the public alert and warning system to disseminate timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety.

(b) Implementation requirements

In carrying out subsection (a), the Administrator shall—

(1) establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system;

(2) include in the public alert and warning system the capability to adapt the distribution and content of communications on the basis of geographic location, risks, and multiple communication

systems and technologies, as appropriate and to the extent technically feasible;

(3) include in the public alert and warning system the capability to alert, warn, and provide equivalent information to individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency, to the extent technically feasible;

(4) ensure that training, tests, and exercises are conducted for the public alert and warning system, including by—

(A) incorporating the public alert and warning system into other training and exercise programs of the Department, as appropriate;

(B) establishing and integrating into the National Incident Management System a comprehensive and periodic training program to instruct and educate Federal, State, tribal, and local government officials in the use of the Common Alerting Protocol enabled Emergency Alert System; and

(C) conducting, not less than once every 3 years, periodic nationwide tests of the public alert and warning system;

(5) to the extent practicable, ensure that the public alert and warning system is resilient and secure and can withstand acts of terrorism and other external attacks;

(6) conduct public education efforts so that State, tribal, and local governments, private entities, and the people of the United States reasonably understand the functions of the public alert and warning system and how to access, use, and respond to information from the public alert and warning system through a general market awareness campaign;

(7) consult, coordinate, and cooperate with the appropriate private sector entities and Federal, State, tribal, and local governmental authorities, including the Regional Administrators and emergency response providers;

(8) consult and coordinate with the Federal Communications Commission, taking into account rules and regulations promulgated by the Federal Communications Commission; and

(9) coordinate with and consider the recommendations of the Integrated Public Alert and Warning System Subcommittee established under section 2(b) of the Integrated Public Alert and Warning System Modernization Act of 2015.

(c) System requirements

The public alert and warning system shall—

(1) to the extent determined appropriate by the Administrator, incorporate multiple communications technologies;

(2) be designed to adapt to, and incorporate, future technologies for communicating directly with the public;

(3) to the extent technically feasible, be designed—

(A) to provide alerts to the largest portion of the affected population feasible, including nonresident visitors and tourists, individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency; and

(B) to improve the ability of remote areas to receive alerts;

(4) promote local and regional public and private partnerships to enhance community preparedness and response;

(5) provide redundant alert mechanisms where practicable so as to reach the greatest number of people; and

(6) to the extent feasible, include a mechanism to ensure the protection of individual privacy.

(d) Use of system

Except to the extent necessary for testing the public alert and warning system, the public alert and warning system shall not be used to transmit a message that does not relate to a natural disaster, act of terrorism, or other man-made disaster or threat to public safety.

(e) Performance reports

(1) In general

Not later than 1 year after April 11, 2016, and annually thereafter through 2018, the Administrator shall make available on the public website of the Agency a performance report, which shall—

(A) establish performance goals for the implementation of the public alert and warning system by the Agency;

(B) describe the performance of the public alert and warning system, including—

(i) the type of technology used for alerts and warnings issued under the system;

(ii) the measures taken to alert, warn, and provide equivalent information to individuals with disabilities, individuals with access and function [1] needs, and individuals with limited-English proficiency; and

(iii) the training, tests, and exercises performed and the outcomes obtained by the Agency;

(C) identify significant challenges to the effective operation of the public alert and warning system and any plans to address these challenges;

(D) identify other necessary improvements to the system; and

(E) provide an analysis comparing the performance of the public alert and warning system with the performance goals established under subparagraph (A).

(2) Congress

The Administrator shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives each report required under paragraph (1).

(Pub. L. 107–296, title V, §526, as added Pub. L. 114–143, §2(a), Apr. 11, 2016, 130 Stat. 327.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 2(b) of the Integrated Public Alert and Warning System Modernization Act of 2015, referred to in subsec. (b)(9), is section 2(b) of Pub. L. 114–143, Apr. 11, 2016, 130 Stat. 329, which is not classified to the Code.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CONSTRUCTION

Pub. L. 114–143, §2(d), Apr. 11, 2016, 130 Stat. 332, provided that:

"(1) DEFINITION.—In this subsection, the term 'participating commercial mobile service provider' has the meaning given that term under section 10.10(f) of title 47, Code of Federal Regulations, as in effect on the date of enactment of this Act [Apr. 11, 2016].

"(2) LIMITATIONS.—Nothing in this Act [enacting this section and provisions set out as a note under section 101 of this title], including an amendment made by this Act, shall be construed—

"(A) to affect any authority—

"(i) of the Department of Commerce;

"(ii) of the Federal Communications Commission; or

"(iii) provided under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.);

"(B) to provide the Secretary of Homeland Security with authority to require any action by the Department of Commerce, the Federal Communications Commission, or any nongovernmental entity;

"(C) to apply to, or to provide the Administrator of the Federal Emergency Management Agency with authority over, any participating commercial mobile service provider;

"(D) to alter in any way the wireless emergency alerts service established under the Warning, Alert, and Response Network Act (47 U.S.C. 1201 et seq.) or any related orders issued by the Federal Communications Commission after October 13, 2006; or

"(E) to provide the Federal Emergency Management Agency with authority to require a State or local jurisdiction to use the integrated public alert and warning system of the United States."

[1] *So in original. Probably should be "functional".*

§321*o*–1. Integrated public alert and warning system

(a) Definitions

In this section—

(1) the term "Administrator" means the Administrator of the Agency;

(2) the term "Agency" means the Federal Emergency Management Agency;

(3) the term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Transportation and Infrastructure of the House of Representatives; and

(C) the Committee on Homeland Security of the House of Representatives;

(4) the term "public alert and warning system" means the integrated public alert and warning system of the United States described in section 321o of this title;

(5) the term "Secretary" means the Secretary of Homeland Security; and

(6) the term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(b) Integrated public alert and warning system

(1) In general

Not later than 1 year after December 20, 2019, the Administrator shall develop minimum requirements for State, Tribal, and local governments to participate in the public alert and warning system and that are necessary to maintain the integrity of the public alert and warning system, including—

(A) guidance on the categories of public emergencies and appropriate circumstances that warrant an alert and warning from State, Tribal, and local governments using the public alert and warning system;

(B) the procedures for State, Tribal, and local government officials to authenticate civil emergencies and initiate, modify, and cancel alerts transmitted through the public alert and warning system, including protocols and technology capabilities for—

(i) the initiation, or prohibition on the initiation, of alerts by a single authorized or unauthorized individual;

(ii) testing a State, Tribal, or local government incident management and warning tool without accidentally initiating an alert through the public alert and warning system; and

(iii) steps a State, Tribal, or local government official should take to mitigate the possibility of the issuance of a false alert through the public alert and warning system;

(C) the standardization, functionality, and interoperability of incident management and warning tools used by State, Tribal, and local governments to notify the public of an emergency through the public alert and warning system;

(D) the annual training and recertification of emergency management personnel on requirements for originating and transmitting an alert through the public alert and warning system;

(E) the procedures, protocols, and guidance concerning the protective action plans that State, Tribal, and local governments shall issue to the public following an alert issued under the public alert and warning system;

(F) the procedures, protocols, and guidance concerning the communications that State, Tribal,

and local governments shall issue to the public following a false alert issued under the public alert and warning system;

(G) a plan by which State, Tribal, and local government officials may, during an emergency, contact each other as well as Federal officials and participants in the Emergency Alert System and the Wireless Emergency Alert System, when appropriate and necessary, by telephone, text message, or other means of communication regarding an alert that has been distributed to the public; and

(H) any other procedure the Administrator considers appropriate for maintaining the integrity of and providing for public confidence in the public alert and warning system.

(2) Coordination with National Advisory Council report

The Administrator shall ensure that the minimum requirements developed under paragraph (1) do not conflict with recommendations made for improving the public alert and warning system provided in the report submitted by the National Advisory Council under section 2(b)(7)(B) of the Integrated Public Alert and Warning System Modernization Act of 2015 (Public Law 114–143; 130 Stat. 332).

(3) Public consultation

In developing the minimum requirements under paragraph (1), the Administrator shall ensure appropriate public consultation and, to the extent practicable, coordinate the development of the requirements with stakeholders of the public alert and warning system, including—

(A) appropriate personnel from Federal agencies, including the National Institute of Standards and Technology, the Agency, and the Federal Communications Commission;

(B) representatives of State and local governments and emergency services personnel, who shall be selected from among individuals nominated by national organizations representing those governments and personnel;

(C) representatives of Federally recognized Indian tribes and national Indian organizations;

(D) communications service providers;

(E) vendors, developers, and manufacturers of systems, facilities, equipment, and capabilities for the provision of communications services;

(F) third-party service bureaus;

(G) the national organization representing the licensees and permittees of noncommercial broadcast television stations;

(H) technical experts from the broadcasting industry;

(I) educators from the Emergency Management Institute; and

(J) other individuals with technical expertise as the Administrator determines appropriate.

(4) Advice to the administrator

In accordance with the Federal Advisory Committee Act (5 U.S.C. App.),[1] the Administrator may obtain advice from a single individual or non-consensus advice from each of the several members of a group without invoking that Act.

(c) Incident management and warning tool validation

(1) In general

The Administrator shall establish a process to ensure that an incident management and warning tool used by a State, Tribal, or local government to originate and transmit an alert through the public alert and warning system meets the requirements developed by the Administrator under subsection (b)(1).

(2) Requirements

The process required to be established under paragraph (1) shall include—

(A) the ability to test an incident management and warning tool in the public alert and warning system lab;

(B) the ability to certify that an incident management and warning tool complies with the applicable cyber frameworks of the Department of Homeland Security and the National

Institute of Standards and Technology;

(C) a process to certify developers of emergency management software; and

(D) requiring developers to provide the Administrator with a copy of and rights of use for ongoing testing of each version of incident management and warning tool software before the software is first used by a State, Tribal, or local government.

(d) Review and update of memoranda of understanding

The Administrator shall review the memoranda of understanding between the Agency and State, Tribal, and local governments with respect to the public alert and warning system to ensure that all agreements ensure compliance with the requirements developed by the Administrator under subsection (b)(1).

(e) Future memoranda

On and after the date that is 60 days after the date on which the Administrator issues the requirements developed under subsection (b)(1), any new memorandum of understanding entered into between the Agency and a State, Tribal, or local government with respect to the public alert and warning system shall comply with those requirements.

(f) Missile alert and warning authorities

(1) In general

(A) Authority

On and after the date that is 120 days after December 20, 2019, the authority to originate an alert warning the public of a missile launch directed against a State using the public alert and warning system shall reside primarily with the Federal Government.

(B) Delegation of authority

The Secretary may delegate the authority described in subparagraph (A) to a State, Tribal, or local entity if, not later than 180 days after December 20, 2019, the Secretary submits a report to the appropriate congressional committees that—

(i) it is not feasible for the Federal Government to alert the public of a missile threat against a State; or

(ii) it is not in the national security interest of the United States for the Federal Government to alert the public of a missile threat against a State.

(C) Activation of system

Upon verification of a missile threat, the President, utilizing established authorities, protocols and procedures, may activate the public alert and warning system.

(D) Rule of construction

Nothing in this paragraph shall be construed to change the command and control relationship between entities of the Federal Government with respect to the identification, dissemination, notification, or alerting of information of missile threats against the United States that was in effect on the day before December 20, 2019.

(2) Required processes

The Secretary, acting through the Administrator, shall establish a process to promptly notify a State warning point, and any State entities that the Administrator determines appropriate, following the issuance of an alert described in paragraph (1)(A) so the State may take appropriate action to protect the health, safety, and welfare of the residents of the State.

(3) Guidance

The Secretary, acting through the Administrator, shall work with the Governor of a State warning point to develop and implement appropriate protective action plans to respond to an alert described in paragraph (1)(A) for that State.

(4) Study and report

Not later than 1 year after December 20, 2019, the Secretary shall—

(A) examine the feasibility of establishing an alert designation under the public alert and warning system that would be used to alert and warn the public of a missile threat while concurrently alerting a State warning point so that a State may activate related protective action plans; and

(B) submit a report of the findings under subparagraph (A), including of the costs and timeline for taking action to implement an alert designation described in subparagraph (A), to—

(i) the Subcommittee on Homeland Security of the Committee on Appropriations of the Senate;

(ii) the Committee on Homeland Security and Governmental Affairs of the Senate;

(iii) the Subcommittee on Homeland Security of the Committee on Appropriations of the House of Representatives;

(iv) the Committee on Transportation and Infrastructure of the House of Representatives; and

(v) the Committee on Homeland Security of the House of Representatives.

(g) Use of integrated public alert and warning system lab

Not later than 1 year after December 20, 2019, the Administrator shall—

(1) develop a program to increase the utilization of the public alert and warning system lab of the Agency by State, Tribal, and local governments to test incident management and warning tools and train emergency management professionals on alert origination protocols and procedures; and

(2) submit to the appropriate congressional committees a report describing—

(A) the impact on utilization of the public alert and warning system lab by State, Tribal, and local governments, with particular attention given to the impact on utilization in rural areas, resulting from the program developed under paragraph (1); and

(B) any further recommendations that the Administrator would make for additional statutory or appropriations authority necessary to increase the utilization of the public alert and warning system lab by State, Tribal, and local governments.

(h) Awareness of alerts and warnings

Not later than 1 year after December 20, 2019, the Administrator shall—

(1) conduct a review of the National Watch Center and each Regional Watch Center of the Agency; and

(2) submit to the appropriate congressional committees a report on the review conducted under paragraph (1), which shall include—

(A) an assessment of the technical capability of the National and Regional Watch Centers described in paragraph (1) to be notified of alerts and warnings issued by a State through the public alert and warning system;

(B) a determination of which State alerts and warnings the National and Regional Watch Centers described in paragraph (1) should be aware of; and

(C) recommendations for improving the ability of the National and Regional Watch Centers described in paragraph (1) to receive any State alerts and warnings that the Administrator determines are appropriate.

(i) Reporting false alerts

Not later than 15 days after the date on which a State, Tribal, or local government official transmits a false alert under the public alert and warning system, the Administrator shall report to the appropriate congressional committees on—

(1) the circumstances surrounding the false alert;

(2) the content, cause, and population impacted by the false alert; and

(3) any efforts to mitigate any negative impacts of the false alert.

(j) Reporting participation rates

The Administrator shall, on an annual basis, report to the appropriate congressional committees on—

(1) participation rates in the public alert and warning system; and

(2) any efforts to expand alert, warning, and interoperable communications to rural and underserved areas.

(k) Timeline for compliance

Each State shall be given a reasonable amount of time to comply with any new rules, regulations, or requirements imposed under this section.

(Pub. L. 116–92, div. A, title XVII, §1756, Dec. 20, 2019, 133 Stat. 1855.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 2(b)(7)(B) of the Integrated Public Alert and Warning System Modernization Act of 2015, referred to in subsec. (b)(2), is section 2(b)(7)(B) of Pub. L. 114–143, Apr. 11, 2016, 130 Stat. 332, which relates to submission of reports by the National Advisory Council and is not classified to the Code.

The Federal Advisory Committee Act, referred to in subsec. (b)(4), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2020, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *See References in Text note below.*

§321p. National planning and education

The Secretary shall, to the extent practicable—

(1) include in national planning frameworks the threat of an EMP or GMD event; and

(2) conduct outreach to educate owners and operators of critical infrastructure, emergency planners, and emergency response providers at all levels of government regarding threats of EMP and GMD.

(Pub. L. 107–296, title V, §527, as added Pub. L. 114–328, div. A, title XIX, §1913(a)(4), Dec. 23, 2016, 130 Stat. 2686.)

§321q. Coordination of Department of Homeland Security efforts related to food, agriculture, and veterinary defense against terrorism

(a) Program required

The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall carry out a program to coordinate the Department's efforts related to defending the food, agriculture, and veterinary systems of the United States against terrorism and other high-consequence events that pose a high risk to homeland security.

(b) Program elements

The coordination program required by subsection (a) shall include, at a minimum, the following:

(1) Providing oversight and management of the Department's responsibilities pursuant to Homeland Security Presidential Directive 9–Defense of United States Agriculture and Food.

(2) Providing oversight and integration of the Department's activities related to veterinary public health, food defense, and agricultural security.

(3) Leading the Department's policy initiatives relating to food, animal, and agricultural incidents, and the impact of such incidents on animal and public health.

(4) Leading the Department's policy initiatives relating to overall domestic preparedness for and collective response to agricultural terrorism.

(5) Coordinating with other Department components, including U.S. Customs and Border Protection, as appropriate, on activities related to food and agriculture security and screening procedures for domestic and imported products.

(6) Coordinating with appropriate Federal departments and agencies.

(7) Other activities as determined necessary by the Secretary.

(c) Rule of construction

Nothing in this section may be construed as altering or superseding the authority of the Secretary of Agriculture or the Secretary of Health and Human Services.

(Pub. L. 107–296, title V, §528, as added Pub. L. 115–43, §2(a), June 30, 2017, 131 Stat. 884; amended Pub. L. 115–387, §2(f)(5), Dec. 21, 2018, 132 Stat. 5168.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–387 substituted "the Countering Weapons of Mass Destruction Office," for "Health Affairs,".

§321r. Transfer of equipment during a public health emergency

(a) Authorization of transfer of equipment

During a public health emergency declared by the Secretary of Health and Human Services under section 247d(a) of title 42, the Secretary, at the request of the Secretary of Health and Human Services, may transfer to the Department of Health and Human Services, on a reimbursable basis, excess personal protective equipment or medically necessary equipment in the possession of the Department.

(b) Determination by Secretaries

(1) In general

In carrying out this section—

(A) before requesting a transfer under subsection (a), the Secretary of Health and Human Services shall determine whether the personal protective equipment or medically necessary equipment is otherwise available; and

(B) before initiating a transfer under subsection (a), the Secretary, in consultation with the heads of each component within the Department, shall—

(i) determine whether the personal protective equipment or medically necessary equipment requested to be transferred under subsection (a) is excess equipment; and

(ii) certify that the transfer of the personal protective equipment or medically necessary equipment will not adversely impact the health or safety of officers, employees, or contractors of the Department.

(2) Notification

The Secretary of Health and Human Services and the Secretary shall each submit to Congress a notification explaining the determination made under subparagraphs (A) and (B), respectively, of paragraph (1).

(3) Required inventory

(A) In general

The Secretary shall—

(i) acting through the Chief Medical Officer of the Department, maintain an inventory of all personal protective equipment and medically necessary equipment in the possession of the Department; and

(ii) make the inventory required under clause (i) available, on a continual basis, to—

(I) the Secretary of Health and Human Services; and

(II) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

(B) Form

Each inventory required to be made available under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(Pub. L. 107–296, title V, §529, as added Pub. L. 117–58, div. G, title IX, §70953(f)(2)(A), Nov. 15, 2021, 135 Stat. 1315.)

§322. Continuity of the economy plan

(a) Requirement

(1) In general

The President shall develop and maintain a plan to maintain and restore the economy of the United States in response to a significant event.

(2) Principles

The plan required under paragraph (1) shall—

(A) be consistent with—

(i) a free market economy; and

(ii) the rule of law; and

(B) respect private property rights.

(3) Contents

The plan required under paragraph (1) shall—

(A) examine the distribution of goods and services across the United States necessary for the reliable functioning of the United States during a significant event;

(B) identify the economic functions of relevant actors, the disruption, corruption, or dysfunction of which would have a debilitating effect in the United States on—

(i) security;

(ii) economic security;

(iii) defense readiness; or

(iv) public health or safety;

(C) identify the critical distribution mechanisms for each economic sector that should be prioritized for operation during a significant event, including—

(i) bulk power and electric transmission systems;

(ii) national and international financial systems, including wholesale payments, stocks, and currency exchanges;

(iii) national and international communications networks, data-hosting services, and cloud services;

(iv) interstate oil and natural gas pipelines; and

(v) mechanisms for the interstate and international trade and distribution of materials, food, and medical supplies, including road, rail, air, and maritime shipping;

(D) identify economic functions of relevant actors, the disruption, corruption, or dysfunction

of which would cause—

(i) catastrophic economic loss;

(ii) the loss of public confidence; or

(iii) the widespread imperilment of human life;

(E) identify the economic functions of relevant actors that are so vital to the economy of the United States that the disruption, corruption, or dysfunction of those economic functions would undermine response, recovery, or mobilization efforts during a significant event;

(F) incorporate, to the greatest extent practicable, the principles and practices contained within Federal plans for the continuity of Government and continuity of operations;

(G) identify—

(i) industrial control networks for which a loss of internet connectivity, a loss of network integrity or availability, an exploitation of a system connected to the network, or another failure, disruption, corruption, or dysfunction would have a debilitating effect in the United States on—

(I) security;

(II) economic security;

(III) defense readiness; or

(IV) public health or safety; and

(ii) for each industrial control network identified under clause (i), risk mitigation measures, including—

(I) the installation of parallel services;

(II) the use of stand-alone analog services; or

(III) the significant hardening of the industrial control network against failure, disruption, corruption, or dysfunction;

(H) identify critical economic sectors for which the preservation of data in a protected, verified, and uncorrupted status would be required for the quick recovery of the economy of the United States in the face of a significant disruption following a significant event;

(I) include a list of raw materials, industrial goods, and other items, the absence of which would significantly undermine the ability of the United States to sustain the functions described in subparagraphs (B), (D), and (E);

(J) provide an analysis of supply chain diversification for the items described in subparagraph (I) in the event of a disruption caused by a significant event;

(K) include—

(i) a recommendation as to whether the United States should maintain a strategic reserve of 1 or more of the items described in subparagraph (I); and

(ii) for each item described in subparagraph (I) for which the President recommends maintaining a strategic reserve under clause (i), an identification of mechanisms for tracking inventory and availability of the item in the strategic reserve;

(L) identify mechanisms in existence on January 1, 2021 and mechanisms that can be developed to ensure that the swift transport and delivery of the items described in subparagraph (I) is feasible in the event of a distribution network disturbance or degradation, including a distribution network disturbance or degradation caused by a significant event;

(M) include guidance for determining the prioritization for the distribution of the items described in subparagraph (I), including distribution to States and Indian Tribes;

(N) consider the advisability and feasibility of mechanisms for extending the credit of the United States or providing other financial support authorized by law to key participants in the economy of the United States if the extension or provision of other financial support—

(i) is necessary to avoid severe economic degradation; or

(ii) allows for the recovery from a significant event;

(O) include guidance for determining categories of employees that should be prioritized to continue to work in order to sustain the functions described in subparagraphs (B), (D), and (E) in the event that there are limitations on the ability of individuals to travel to workplaces or to work remotely, including considerations for defense readiness;

(P) identify critical economic sectors necessary to provide material and operational support to the defense of the United States;

(Q) determine whether the Secretary of Homeland Security, the National Guard, and the Secretary of Defense have adequate authority to assist the United States in a recovery from a severe economic degradation caused by a significant event;

(R) review and assess the authority and capability of heads of other agencies that the President determines necessary to assist the United States in a recovery from a severe economic degradation caused by a significant event; and

(S) consider any other matter that would aid in protecting and increasing the resilience of the economy of the United States from a significant event.

(b) Coordination

In developing the plan required under subsection (a)(1), the President shall—

(1) receive advice from—

(A) the Secretary of Homeland Security;

(B) the Secretary of Defense;

(C) the Secretary of the Treasury;

(D) the Secretary of Health and Human Services;

(E) the Secretary of Commerce;

(F) the Secretary of Transportation;

(G) the Secretary of Energy;

(H) the Administrator of the Small Business Administration; and

(I) the head of any other agency that the President determines necessary to complete the plan;

(2) consult with economic sectors relating to critical infrastructure through sector-coordinated councils, as appropriate;

(3) consult with relevant State, Tribal, and local governments and organizations that represent those governments; and

(4) consult with any other non-Federal entity that the President determines necessary to complete the plan.

(c) Submission to Congress

(1) In general

Not later than 2 years after January 1, 2021, and not less frequently than every 3 years thereafter, the President shall submit the plan required under subsection (a)(1) and the information described in paragraph (2) to—

(A) the majority and minority leaders of the Senate;

(B) the Speaker and the minority leader of the House of Representatives;

(C) the Committee on Armed Services of the Senate;

(D) the Committee on Armed Services of the House of Representatives;

(E) the Committee on Homeland Security and Governmental Affairs of the Senate;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Health, Education, Labor, and Pensions of the Senate;

(H) the Committee on Commerce, Science, and Transportation of the Senate;

(I) the Committee on Energy and Commerce of the House of Representatives;

(J) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(K) the Committee on Finance of the Senate;

(L) the Committee on Financial Services of the House of Representatives;

(M) the Committee on Small Business and Entrepreneurship of the Senate;

(N) the Committee on Small Business of the House of Representatives;
(O) the Committee on Energy and Natural Resources of the Senate;
(P) the Committee on Environment and Public Works of the Senate;
(Q) the Committee on Indian Affairs of the Senate;
(R) the Committee on Oversight and Reform of the House of Representatives;
(S) Committee on the Budget of the House of Representatives; and
(T) any other committee of the Senate or the House of Representatives that has jurisdiction over the subject of the plan.

(2) Additional information

The information described in this paragraph is—
(A) any change to Federal law that would be necessary to carry out the plan required under subsection (a)(1); and
(B) any proposed changes to the funding levels provided in appropriation Acts for the most recent fiscal year that can be implemented in future appropriation Acts or additional resources necessary to—
(i) implement the plan required under subsection (a)(1); or
(ii) maintain any program offices and personnel necessary to—
(I) maintain the plan required under subsection (a)(1) and the plans described in subsection (a)(3)(F); and
(II) conduct exercises, assessments, and updates to the plans described in subclause (I) over time.

(3) Budget of the President

The President may include the information described in paragraph (2)(B) in the budget required to be submitted by the President under section 1105(a) of title 31.

(d) Definitions

In this section:
(1) The term "agency" has the meaning given the term in section 551 of title 5.
(2) The term "economic sector" means a sector of the economy of the United States.
(3) The term "relevant actor" means—
(A) the Federal Government;
(B) a State, local, or Tribal government; or
(C) the private sector.

(4) The term "significant event" means an event that causes severe degradation to economic activity in the United States due to—
(A) a cyber attack; or
(B) another significant event that is natural or human-caused.

(5) The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(Pub. L. 116–283, div. H, title XCVI, §9603, Jan. 1, 2021, 134 Stat. 4829.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

§323. Guidance on how to prevent exposure to and release of PFAS

(a) In general

Not later than 1 year after December 20, 2022, the Secretary of Homeland Security, in consultation with the Administrator of the United States Fire Administration, the Administrator of the Environmental Protection Agency, the Director of the National Institute for Occupational Safety and Health, and the heads of any other relevant agencies, shall—

(1) develop and publish guidance for firefighters and other emergency response personnel on training, education programs, and best practices;

(2) make available a curriculum designed to—

(A) reduce and eliminate exposure to per- and polyfluoroalkyl substances (commonly referred to as "PFAS") from firefighting foam and personal protective equipment;

(B) prevent the release of PFAS from firefighting foam into the environment; and

(C) educate firefighters and other emergency response personnel on foams and non-foam alternatives, personal protective equipment, and other firefighting tools and equipment that do not contain PFAS; and

(3) create an online public repository, which shall be updated on a regular basis, on tools and best practices for firefighters and other emergency response personnel to reduce, limit, and prevent the release of and exposure to PFAS.

(b) Curriculum

(1) In general

For the purpose of developing the curriculum required under subsection (a)(2), the Administrator of the United States Fire Administration shall make recommendations to the Secretary of Homeland Security as to the content of the curriculum.

(2) Consultation

For the purpose of making recommendations under paragraph (1), the Administrator of the United States Fire Administration shall consult with interested entities, as appropriate, including—

(A) firefighters and other emergency response personnel, including national fire service and emergency response organizations;

(B) impacted communities dealing with PFAS contamination;

(C) scientists, including public and occupational health and safety experts, who are studying PFAS and PFAS alternatives in firefighting foam;

(D) voluntary standards organizations engaged in developing standards for firefighter and firefighting equipment;

(E) State fire training academies;

(F) State fire marshals;

(G) manufacturers of firefighting tools and equipment; and

(H) any other relevant entities, as determined by the Secretary of Homeland Security and the Administrator of the United States Fire Administration.

(c) Review

Not later than 3 years after the date on which the guidance and curriculum required under subsection (a) is issued, and not less frequently than once every 3 years thereafter, the Secretary of

Homeland Security, in consultation with the Administrator of the United States Fire Administration, the Administrator of the Environmental Protection Agency, and the Director of the National Institute for Occupational Safety and Health, shall review the guidance and curriculum and, as appropriate, issue updates to the guidance and curriculum.

(d) Applicability of FACA

The Federal Advisory Committee Act (5 U.S.C. App.) [1] shall not apply to this Act.

(e) Rule of construction

Nothing in this Act shall be construed to require the Secretary of Homeland Security to promulgate or enforce regulations under subchapter II of chapter 5 of title 5 (commonly known as the "Administrative Procedure Act").

(Pub. L. 117–248, §2, Dec. 20, 2022, 136 Stat. 2348.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (d), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

CODIFICATION

Section was enacted as part of the Protecting Firefighters from Adverse Substances Act, also known as the PFAS Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *See References in Text note below.*

SUBCHAPTER VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS

§331. Treatment of charitable trusts for members of the Armed Forces of the United States and other governmental organizations

(a) Findings

Congress finds the following:

(1) Members of the Armed Forces of the United States defend the freedom and security of our Nation.

(2) Members of the Armed Forces of the United States have lost their lives while battling the evils of terrorism around the world.

(3) Personnel of the Central Intelligence Agency (CIA) charged with the responsibility of covert observation of terrorists around the world are often put in harm's way during their service to the United States.

(4) Personnel of the Central Intelligence Agency have also lost their lives while battling the evils of terrorism around the world.

(5) Employees of the Federal Bureau of Investigation (FBI) and other Federal agencies charged with domestic protection of the United States put their lives at risk on a daily basis for the freedom and security of our Nation.

(6) United States military personnel, CIA personnel, FBI personnel, and other Federal agents in

the service of the United States are patriots of the highest order.

(7) CIA officer Johnny Micheal Spann became the first American to give his life for his country in the War on Terrorism declared by President George W. Bush following the terrorist attacks of September 11, 2001.

(8) Johnny Micheal Spann left behind a wife and children who are very proud of the heroic actions of their patriot father.

(9) Surviving dependents of members of the Armed Forces of the United States who lose their lives as a result of terrorist attacks or military operations abroad receive a $6,000 death benefit, plus a small monthly benefit.

(10) The current system of compensating spouses and children of American patriots is inequitable and needs improvement.

(b) Designation of Johnny Micheal Spann Patriot Trusts

Any charitable corporation, fund, foundation, or trust (or separate fund or account thereof) which otherwise meets all applicable requirements under law with respect to charitable entities and meets the requirements described in subsection (c) shall be eligible to characterize itself as a "Johnny Micheal Spann Patriot Trust".

(c) Requirements for the designation of Johnny Micheal Spann Patriot Trusts

The requirements described in this subsection are as follows:

(1) Not taking into account funds or donations reasonably necessary to establish a trust, at least 85 percent of all funds or donations (including any earnings on the investment of such funds or donations) received or collected by any Johnny Micheal Spann Patriot Trust must be distributed to (or, if placed in a private foundation, held in trust for) surviving spouses, children, or dependent parents, grandparents, or siblings of 1 or more of the following:

(A) members of the Armed Forces of the United States;

(B) personnel, including contractors, of elements of the intelligence community, as defined in section 3003(4) of title 50;

(C) employees of the Federal Bureau of Investigation; and

(D) officers, employees, or contract employees of the United States Government,

whose deaths occur in the line of duty and arise out of terrorist attacks, military operations, intelligence operations, or law enforcement operations or accidents connected with activities occurring after September 11, 2001, and related to domestic or foreign efforts to curb international terrorism, including the Authorization for Use of Military Force (Public Law 107–40; 115 Stat. 224).

(2) Other than funds or donations reasonably necessary to establish a trust, not more than 15 percent of all funds or donations (or 15 percent of annual earnings on funds invested in a private foundation) may be used for administrative purposes.

(3) No part of the net earnings of any Johnny Micheal Spann Patriot Trust may inure to the benefit of any individual based solely on the position of such individual as a shareholder, an officer or employee of such Trust.

(4) None of the activities of any Johnny Micheal Spann Patriot Trust shall be conducted in a manner inconsistent with any law that prohibits attempting to influence legislation.

(5) No Johnny Micheal Spann Patriot Trust may participate in or intervene in any political campaign on behalf of (or in opposition to) any candidate for public office, including by publication or distribution of statements.

(6) Each Johnny Micheal Spann Patriot Trust shall comply with the instructions and directions of the Director of Central Intelligence, the Attorney General, or the Secretary of Defense relating to the protection of intelligence sources and methods, sensitive law enforcement information, or other sensitive national security information, including methods for confidentially disbursing funds.

(7) Each Johnny Micheal Spann Patriot Trust that receives annual contributions totaling more than $1,000,000 must be audited annually by an independent certified public accounting firm.

Such audits shall be filed with the Internal Revenue Service, and shall be open to public inspection, except that the conduct, filing, and availability of the audit shall be consistent with the protection of intelligence sources and methods, of sensitive law enforcement information, and of other sensitive national security information.

(8) Each Johnny Micheal Spann Patriot Trust shall make distributions to beneficiaries described in paragraph (1) at least once every calendar year, beginning not later than 12 months after the formation of such Trust, and all funds and donations received and earnings not placed in a private foundation dedicated to such beneficiaries must be distributed within 36 months after the end of the fiscal year in which such funds, donations, and earnings are received.

(9)(A) When determining the amount of a distribution to any beneficiary described in paragraph (1), a Johnny Micheal Spann Patriot Trust should take into account the amount of any collateral source compensation that the beneficiary has received or is entitled to receive as a result of the death of an individual described in paragraph (1).

(B) Collateral source compensation includes all compensation from collateral sources, including life insurance, pension funds, death benefit programs, and payments by Federal, State, or local governments related to the death of an individual described in paragraph (1).

(d) Treatment of Johnny Micheal Spann Patriot Trusts

Each Johnny Micheal Spann Patriot Trust shall refrain from conducting the activities described in clauses (i) and (ii) of section 30101(20)(A) of title 52 so that a general solicitation of funds by an individual described in paragraph (1) of section 30125(e) of title 52 will be permissible if such solicitation meets the requirements of paragraph (4)(A) of such section.

(e) Notification of Trust beneficiaries

Notwithstanding any other provision of law, and in a manner consistent with the protection of intelligence sources and methods and sensitive law enforcement information, and other sensitive national security information, the Secretary of Defense, the Director of the Federal Bureau of Investigation, or the Director of Central Intelligence, or their designees, as applicable, may forward information received from an executor, administrator, or other legal representative of the estate of a decedent described in subparagraph (A), (B), (C), or (D) of subsection (c)(1), to a Johnny Micheal Spann Patriot Trust on how to contact individuals eligible for a distribution under subsection (c)(1) for the purpose of providing assistance from such Trust: *Provided*, That, neither forwarding nor failing to forward any information under this subsection shall create any cause of action against any Federal department, agency, officer, agent, or employee.

(f) Regulations

Not later than 90 days after November 25, 2002, the Secretary of Defense, in coordination with the Attorney General, the Director of the Federal Bureau of Investigation, and the Director of Central Intelligence, shall prescribe regulations to carry out this section.

(Pub. L. 107–296, title VI, §601, Nov. 25, 2002, 116 Stat. 2215.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Authorization for Use of Military Force, referred to in subsec. (c)(1), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a

reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

SUBCHAPTER VII—MANAGEMENT

§341. Under Secretary for Management

(a) In general

The Under Secretary for Management shall serve as the Chief Management Officer and principal advisor to the Secretary on matters related to the management of the Department, including management integration and transformation in support of homeland security operations and programs. The Secretary, acting through the Under Secretary for Management, shall be responsible for the management and administration of the Department, including the following:

(1) The budget, appropriations, expenditures of funds, accounting, and finance.

(2) Procurement.

(3) Human resources and personnel.

(4) Information technology and communications systems, including policies and directives to achieve and maintain interoperable communications among the components of the Department.

(5) Facilities, property, equipment, vehicle fleets (under subsection (c)), and other material resources.

(6) Security for personnel, information technology and communications systems, facilities, property, equipment, and other material resources.

(7) Strategic management planning and annual performance planning and identification and tracking of performance measures relating to the responsibilities of the Department.

(8) Grants and other assistance management programs.

(9) The management integration and transformation within each functional management discipline of the Department, including information technology, financial management, acquisition management, and human capital management, to ensure an efficient and orderly consolidation of functions and personnel in the Department, including—

(A) the development of centralized data sources and connectivity of information systems to the greatest extent practicable to enhance program visibility, transparency, and operational effectiveness and coordination;

(B) the development of standardized and automated management information to manage and oversee programs and make informed decisions to improve the efficiency of the Department;

(C) the development of effective program management and regular oversight mechanisms, including clear roles and processes for program governance, sharing of best practices, and access to timely, reliable, and evaluated data on all acquisitions and investments; and

(D) the overall supervision, including the conduct of internal audits and management analyses, of the programs and activities of the Department, including establishment of oversight procedures to ensure a full and effective review of the efforts by components of the Department to implement policies and procedures of the Department for management integration and transformation.

(10) The development of a transition and succession plan, before December 1 of each year in which a Presidential election is held, to guide the transition of Department functions to a new Presidential administration, and making such plan available to the next Secretary and Under Secretary for Management and to the congressional homeland security committees.

(11) Reporting to the Government Accountability Office every six months to demonstrate measurable, sustainable progress made in implementing the corrective action plans of the Department to address the designation of the management functions of the Department on the bi-annual high risk list of the Government Accountability Office, until the Comptroller General of

the United States submits to the appropriate congressional committees written notification of removal of the high-risk designation.

(12) The conduct of internal audits and management analyses of the programs and activities of the Department.

(13) Any other management duties that the Secretary may designate.

(b) Waivers for conducting business with suspended or debarred contractors

Not later than five days after the date on which the Chief Procurement Officer or Chief Financial Officer of the Department issues a waiver of the requirement that an agency not engage in business with a contractor or other recipient of funds listed as a party suspended or debarred from receiving contracts, grants, or other types of Federal assistance in the System for Award Management maintained by the General Services Administration, or any successor thereto, the Under Secretary for Management shall submit to the congressional homeland security committees and the Inspector General of the Department notice of the waiver and an explanation of the finding by the Under Secretary that a compelling reason exists for the waiver.

(c) Vehicle fleets

(1) In general

In carrying out responsibilities regarding vehicle fleets pursuant to subsection (a)(5), the Under Secretary for Management shall be responsible for overseeing and managing vehicle fleets throughout the Department. The Under Secretary shall also be responsible for the following:

(A) Ensuring that components are in compliance with Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) relating to fleet management and use of vehicles from home to work.

(B) Developing and distributing a standardized vehicle allocation methodology and fleet management plan for components to use to determine optimal fleet size in accordance with paragraph (4).

(C) Ensuring that components formally document fleet management decisions.

(D) Approving component fleet management plans, vehicle leases, and vehicle acquisitions.

(2) Component responsibilities

(A) In general

Component heads—

(i) shall—

(I) comply with Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) relating to fleet management and use of vehicles from home to work;

(II) ensure that data related to fleet management is accurate and reliable;

(III) use such data to develop a vehicle allocation tool derived by using the standardized vehicle allocation methodology provided by the Under Secretary for Management to determine the optimal fleet size for the next fiscal year and a fleet management plan; and

(IV) use vehicle allocation methodologies and fleet management plans to develop annual requests for funding to support vehicle fleets pursuant to paragraph (6); and

(ii) may not, except as provided in subparagraph (B), lease or acquire new vehicles or replace existing vehicles without prior approval from the Under Secretary for Management pursuant to paragraph (5)(B).

(B) Exception regarding certain leasing and acquisitions

If exigent circumstances warrant such, a component head may lease or acquire a new vehicle or replace an existing vehicle without prior approval from the Under Secretary for Management. If under such exigent circumstances a component head so leases, acquires, or replaces a vehicle, such component head shall provide to the Under Secretary an explanation of such circumstances.

(3) Ongoing oversight

(A) Quarterly monitoring

In accordance with paragraph (4), the Under Secretary for Management shall collect, on a quarterly basis, information regarding component vehicle fleets, including information on fleet size, composition, cost, and vehicle utilization.

(B) Automated information

The Under Secretary for Management shall seek to achieve a capability to collect, on a quarterly basis, automated information regarding component vehicle fleets, including the number of trips, miles driven, hours and days used, and the associated costs of such mileage for leased vehicles.

(C) Monitoring

The Under Secretary for Management shall track and monitor component information provided pursuant to subparagraph (A) and, as appropriate, subparagraph (B), to ensure that component vehicle fleets are the optimal fleet size and cost effective. The Under Secretary shall use such information to inform the annual component fleet analyses referred to in paragraph (4).

(4) Annual review of component fleet analyses

(A) In general

To determine the optimal fleet size and associated resources needed for each fiscal year beginning with fiscal year 2018, component heads shall annually submit to the Under Secretary for Management a vehicle allocation tool and fleet management plan using information described in paragraph (3)(A). Such tools and plans may be submitted in classified form if a component head determines that such is necessary to protect operations or mission requirements.

(B) Vehicle allocation tool

Component heads shall develop a vehicle allocation tool in accordance with subclause (III) of paragraph (2)(A)(i) that includes an analysis of the following:

(i) Vehicle utilization data, including the number of trips, miles driven, hours and days used, and the associated costs of such mileage for leased vehicles, in accordance with such paragraph.

(ii) The role of vehicle fleets in supporting mission requirements for each component.

(iii) Any other information determined relevant by such component heads.

(C) Fleet management plans

Component heads shall use information described in subparagraph (B) to develop a fleet management plan for each such component. Such fleet management plans shall include the following:

(i) A plan for how each such component may achieve optimal fleet size determined by the vehicle allocation tool required under such subparagraph, including the elimination of excess vehicles in accordance with paragraph (5), if applicable.

(ii) A cost benefit analysis supporting such plan.

(iii) A schedule each such component will follow to obtain optimal fleet size.

(iv) Any other information determined relevant by component heads.

(D) Review

The Under Secretary for Management shall review and make a determination on the results of each component's vehicle allocation tool and fleet management plan under this paragraph to ensure each such component's vehicle fleets are the optimal fleet size and that components are in compliance with applicable Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) pursuant to paragraph (2) relating to fleet

management and use of vehicles from home to work. The Under Secretary shall use such tools and plans when reviewing annual component requests for vehicle fleet funding in accordance with paragraph (6).

(5) Guidance to develop fleet management plans

The Under Secretary for Management shall provide guidance, pursuant to paragraph (1)(B) on how component heads may achieve optimal fleet size in accordance with paragraph (4), including processes for the following:

(A) Leasing or acquiring additional vehicles or replacing existing vehicles, if determined necessary.

(B) Disposing of excess vehicles that the Under Secretary determines should not be reallocated under subparagraph (C).

(C) Reallocating excess vehicles to other components that may need temporary or long-term use of additional vehicles.

(6) Annual review of vehicle fleet funding requests

As part of the annual budget process, the Under Secretary for Management shall review and make determinations regarding annual component requests for funding for vehicle fleets. If component heads have not taken steps in furtherance of achieving optimal fleet size in the prior fiscal year pursuant to paragraphs (4) and (5), the Under Secretary shall provide rescission recommendations to the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives and the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate regarding such component vehicle fleets.

(7) Accountability for vehicle fleet management

(A) Prohibition on certain new vehicle leases and acquisitions

The Under Secretary for Management and component heads may not approve in any fiscal year beginning with fiscal year 2019 a vehicle lease, acquisition, or replacement request if such component heads did not comply in the prior fiscal year with paragraph (4).

(B) Prohibition on certain performance compensation

No Department official with vehicle fleet management responsibilities may receive annual performance compensation in pay in any fiscal year beginning with fiscal year 2019 if such official did not comply in the prior fiscal year with paragraph (4).

(C) Prohibition on certain car services

Notwithstanding any other provision of law, no senior executive service official of the Department whose office has a vehicle fleet may receive access to a car service in any fiscal year beginning with fiscal year 2019 if such official did not comply in the prior fiscal year with paragraph (4).

(8) Motor pool

(A) In general

The Under Secretary for Management may determine the feasibility of operating a vehicle motor pool to permit components to share vehicles as necessary to support mission requirements to reduce the number of excess vehicles in the Department.

(B) Requirements

The determination of feasibility of operating a vehicle motor pool under subparagraph (A) shall—

(i) include—

(I) regions in the United States in which multiple components with vehicle fleets are located in proximity to one another, or a significant number of employees with authorization to use vehicles are located; and

(II) law enforcement vehicles;

(ii) cover the National Capital Region; and
(iii) take into account different mission requirements.

(C) Report

The Secretary shall include in the Department's next annual performance report required under current law the results of the determination under this paragraph.

(9) Definitions

In this subsection:

(A) Component head

The term "component head" means the head of any component of the Department with a vehicle fleet.

(B) Excess vehicle

The term "excess vehicle" means any vehicle that is not essential to support mission requirements of a component.

(C) Optimal fleet size

The term "optimal fleet size" means, with respect to a particular component, the appropriate number of vehicles to support mission requirements of such component.

(D) Vehicle fleet

The term "vehicle fleet" means all owned, commercially leased, or Government-leased vehicles of the Department or of a component of the Department, as the case may be, including vehicles used for law enforcement and other purposes.

(d) Appointment and evaluation

The Under Secretary for Management shall—

(1) be appointed by the President, by and with the advice and consent of the Senate, from among persons who have—

(A) extensive executive level leadership and management experience in the public or private sector;

(B) strong leadership skills;

(C) a demonstrated ability to manage large and complex organizations; and

(D) a proven record in achieving positive operational results;

(2) enter into an annual performance agreement with the Secretary that shall set forth measurable individual and organizational goals; and

(3) be subject to an annual performance evaluation by the Secretary, who shall determine as part of each such evaluation whether the Under Secretary for Management has made satisfactory progress toward achieving the goals set out in the performance agreement required under paragraph (2).

(e) [1] System for Award Management consultation

The Under Secretary for Management shall require that all Department contracting and grant officials consult the System for Award Management (or successor system) as maintained by the General Services Administration prior to awarding a contract or grant or entering into other transactions to ascertain whether the selected contractor is excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and non-financial assistance and benefits.

(e) [1] Interoperable communications defined

In this section, the term "interoperable communications" has the meaning given that term in section 194(g) of this title.

(Pub. L. 107–296, title VII, §701, Nov. 25, 2002, 116 Stat. 2218; Pub. L. 110–53, title XXIV, §2405(a), (b), Aug. 3, 2007, 121 Stat. 548; Pub. L. 114–29, §3, July 6, 2015, 129 Stat. 421; Pub. L. 114–328, div. A, title XIX, §1903(b), Dec. 23, 2016, 130 Stat. 2673; Pub. L. 115–38, §2, June 6, 2017, 131 Stat. 855.)

EDITORIAL NOTES

AMENDMENTS

2017—Subsec. (a)(5). Pub. L. 115–38, §2(1), inserted "vehicle fleets (under subsection (c))," after "equipment,".

Subsecs. (c) to (e). Pub. L. 115–38, §2(2), (3), added subsec. (c), redesignated former subsec. (c) as (d), and redesignated former subsec. (d), relating to System for Award Management consultation, as (e).

2016—Subsec. (a)(9) to (13). Pub. L. 114–328, §1903(b)(1), added pars. (9) to (11), redesignated former pars. (10) and (11) as (12) and (13), respectively, and struck out former par. (9). Prior to amendment, text of par. (9) read as follows: "The management integration and transformation process, as well as the transition process, to ensure an efficient and orderly consolidation of functions and personnel in the Department and transition, including—

"(A) the development of a management integration strategy for the Department, and

"(B) before December 1 of any year in which a Presidential election is held, the development of a transition and succession plan, to be made available to the incoming Secretary and Under Secretary for Management, to guide the transition of management functions to a new Administration."

Subsec. (b). Pub. L. 114–328, §1903(b)(2), added subsec. (b) and struck out former subsec. (b) which related to maintenance of immigration statistics by the Under Secretary for Management and transfer of certain functions of the Statistics Branch of the Office of Policy and Planning of the Immigration and Naturalization Service to the Under Secretary for Management.

Subsecs. (d), (e). Pub. L. 114–328, §1903(b)(3), (4), added subsec. (d) and redesignated former subsec. (d), defining interoperable communications, as (e).

2015—Subsec. (a)(4). Pub. L. 114–29, §3(1), inserted before period at end ", including policies and directives to achieve and maintain interoperable communications among the components of the Department".

Subsec. (d). Pub. L. 114–29, §3(2), added subsec. (d).

2007—Subsec. (a). Pub. L. 110–53, §2405(a)(1), inserted in introductory provisions "The Under Secretary for Management shall serve as the Chief Management Officer and principal advisor to the Secretary on matters related to the management of the Department, including management integration and transformation in support of homeland security operations and programs."

Subsec. (a)(7). Pub. L. 110–53, §2405(a)(2), added par. (7) and struck out former par. (7) which read as follows: "Identification and tracking of performance measures relating to the responsibilities of the Department."

Subsec. (a)(9). Pub. L. 110–53, §2405(a)(3), added par. (9) and struck out former par. (9) which read as follows: "The transition and reorganization process, to ensure an efficient and orderly transfer of functions and personnel to the Department, including the development of a transition plan."

Subsec. (c). Pub. L. 110–53, §2405(b), added subsec. (c).

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEADLINE FOR APPOINTMENT; INCUMBENT

Pub. L. 110–53, title XXIV, §2405(c), Aug. 3, 2007, 121 Stat. 549, provided that:

"(1) DEADLINE FOR APPOINTMENT.—Not later than 90 days after the date of the enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall name an individual who meets the qualifications of section 701 of the Homeland Security Act (6 U.S.C. 341), as amended by subsections (a) and (b), to serve as the Under Secretary of Homeland Security for Management. The Secretary may submit the name of the individual who serves in the position of Under Secretary of Homeland Security for Management on the date of enactment of this Act together with a statement that informs the Congress that the individual meets the qualifications of such section as so amended.

"(2) INCUMBENT.—The incumbent serving as Under Secretary of Homeland Security for Management on November 4, 2008, is authorized to continue serving in that position until a successor is confirmed, to ensure continuity in the management functions of the Department."

[1] *So in original. There are two subsecs. (e).*

§342. Chief Financial Officer

(a) In general

The Chief Financial Officer shall perform functions as specified in chapter 9 of title 31 and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time, shall also report to the Under Secretary for Management.

(b) Program analysis and evaluation function

(1) Establishment of Office of Program Analysis and Evaluation

Not later than 90 days after October 16, 2004, the Secretary shall establish an Office of Program Analysis and Evaluation within the Department (in this section referred to as the "Office").

(2) Responsibilities

The Office shall perform the following functions:

(A) Analyze and evaluate plans, programs, and budgets of the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed pursuant to section 454(b)(2) of this title.

(B) Develop and perform analyses and evaluations of alternative plans, programs, personnel levels, and budget submissions for the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed pursuant to section 454(b)(2) of this title.

(C) Establish policies for, and oversee the integration of, the planning, programming, and budgeting system of the Department.

(D) Review and ensure that the Department meets performance-based budget requirements established by the Office of Management and Budget.

(E) Provide guidance for, and oversee the development of, the Future Years Homeland Security Program of the Department, as specified under section 454 of this title.

(F) Ensure that the costs of Department programs, including classified programs, are presented accurately and completely.

(G) Oversee the preparation of the annual performance plan for the Department and the program and performance section of the annual report on program performance for the Department, consistent with sections 1115 and 1116, respectively, of title 31.

(H) Provide leadership in developing and promoting improved analytical tools and methods for analyzing homeland security planning and the allocation of resources.

(I) Any other responsibilities delegated by the Secretary consistent with an effective program analysis and evaluation function.

(3) Director of Program Analysis and Evaluation

There shall be a Director of Program Analysis and Evaluation, who—

(A) shall be a principal staff assistant to the Chief Financial Officer of the Department for program analysis and evaluation; and

(B) shall report to an official no lower than the Chief Financial Officer.

(4) Reorganization

(A) In general

The Secretary may allocate or reallocate the functions of the Office, or discontinue the Office, in accordance with section 452(a) of this title.

(B) Exemption from limitations

Section 452(b) of this title shall not apply to any action by the Secretary under this paragraph.

(c) Notification regarding transfer or reprogramming of funds

In any case in which appropriations available to the Department or any officer of the Department are transferred or reprogrammed and notice of such transfer or reprogramming is submitted to the Congress (including any officer, office, or Committee of the Congress), the Chief Financial Officer of the Department shall simultaneously submit such notice to the Select Committee on Homeland Security (or any successor to the jurisdiction of that committee) and the Committee on Government Reform of the House of Representatives, and to the Committee on Governmental Affairs of the Senate.

(Pub. L. 107–296, title VII, §702, Nov. 25, 2002, 116 Stat. 2219; Pub. L. 108–330, §§3(d)(1)(B), 6, 7, Oct. 16, 2004, 118 Stat. 1276, 1278, 1279.)

EDITORIAL NOTES

AMENDMENTS

2004—Pub. L. 108–330, §§6, 7, designated existing provisions as subsec. (a), inserted heading, and added subsecs. (b) and (c).

Pub. L. 108–330, §3(d)(1)(B), substituted "shall perform functions as specified in chapter 9 of title 31 and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time, shall also report to the Under Secretary for Management" for "shall report to the Secretary, or to another official of the Department, as the Secretary may direct".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Select Committee on Homeland Security, which was established by House Resolution 449, One Hundred Seventh Congress, June 19, 2002, and reestablished by section 4 of House Resolution 5, One Hundred Eighth Congress, Jan. 4, 2005, was not reestablished in the One Hundred Ninth Congress. Rule X(1)(i) of the Rules of the House of Representatives, One Hundred Ninth Congress, as amended by section 2 of House Resolution 5, One Hundred Ninth Congress, Jan. 4, 2005, established a Committee on Homeland Security. For jurisdiction of the Select Committee on Homeland Security and of the Committee on Homeland Security, see section 4 of House Resolution 5, One Hundred Eighth Congress, and Rule X(1)(i) of the Rules of the House, One Hundred Ninth Congress.

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

FINDINGS

Pub. L. 108–330, §2, Oct. 16, 2004, 118 Stat. 1275, provided that: "The Congress finds the following:

"(1) Influential financial management leadership is of vital importance to the mission success of the Department of Homeland Security. For this reason, the Chief Financial Officer of the Department must be a key figure in the Department's management.

"(2) To provide a sound financial leadership structure, the provisions of law enacted by the Chief Financial Officers Act of 1990 (Public Law 101–576) [see Short Title of 1990 Amendment note set out under section 501 of Title 31, Money and Finance] provide that the Chief Financial Officer of each of the Federal executive departments is to be a Presidential appointee who reports directly to the Secretary of that

department on financial management matters. Because the Department of Homeland Security was only recently created, the provisions enacted by that Act must be amended to include the Department within these provisions.

"(3) The Department of Homeland Security was created by consolidation of 22 separate Federal agencies, each with its own accounting and financial management system. None of these systems was developed with a view to executing the mission of the Department of Homeland Security to prevent terrorist attacks within the United States, reduce the Nation's vulnerability to terrorism, and minimize the damage and assist in the recovery from terrorist attacks. For these reasons, a strong Chief Financial Officer is needed within the Department both to consolidate financial management operations, and to insure that management control systems are comprehensively designed to achieve the mission and execute the strategy of the Department.

"(4) The provisions of law enacted by the Chief Financial Officers Act of 1990 require agency Chief Financial Officers to improve the financial information available to agency managers and the Congress. Those provisions also specify that agency financial management systems must provide for the systematic measurement of performance. In the case of the Department of Homeland Security, therefore, it is vitally important that management control systems be designed with a clear view of a homeland security strategy, including the priorities of the Department in addressing those risks of terrorism deemed most significant based upon a comprehensive assessment of potential threats, vulnerabilities, criticality, and consequences. For this reason, Federal law should be amended to clearly state the responsibilities of the Chief Financial Officer of the Department of Homeland Security to provide management control information, for the benefit of managers within the Department and to help inform the Congress, that permits an assessment of the Department's performance in executing a homeland security strategy."

§343. Chief Information Officer

(a) In general

The Chief Information Officer shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

(b) Geospatial information functions

(1) Definitions

As used in this subsection:

(A) Geospatial information

The term "geospatial information" means graphical or digital data depicting natural or manmade physical features, phenomena, or boundaries of the earth and any information related thereto, including surveys, maps, charts, remote sensing data, and images.

(B) Geospatial technology

The term "geospatial technology" means any technology utilized by analysts, specialists, surveyors, photogrammetrists, hydrographers, geodesists, cartographers, architects, or engineers for the collection, storage, retrieval, or dissemination of geospatial information, including—

(i) global satellite surveillance systems;
(ii) global position systems;
(iii) geographic information systems;
(iv) mapping equipment;
(v) geocoding technology; and
(vi) remote sensing devices.

(2) Office of Geospatial Management

(A) Establishment

The Office of Geospatial Management is established within the Office of the Chief Information Officer.

(B) Geospatial Information Officer

(i) Appointment

The Office of Geospatial Management shall be administered by the Geospatial Information Officer, who shall be appointed by the Secretary and serve under the direction of the Chief Information Officer.

(ii) Functions

The Geospatial Information Officer shall assist the Chief Information Officer in carrying out all functions under this section and in coordinating the geospatial information needs of the Department.

(C) Coordination of geospatial information

The Chief Information Officer shall establish and carry out a program to provide for the efficient use of geospatial information, which shall include—

(i) providing such geospatial information as may be necessary to implement the critical infrastructure protection programs;

(ii) providing leadership and coordination in meeting the geospatial information requirements of those responsible for planning, prevention, mitigation, assessment and response to emergencies, critical infrastructure protection, and other functions of the Department; and

(iii) coordinating with users of geospatial information within the Department to assure interoperability and prevent unnecessary duplication.

(D) Responsibilities

In carrying out this subsection, the responsibilities of the Chief Information Officer shall include—

(i) coordinating the geospatial information needs and activities of the Department;

(ii) implementing standards, as adopted by the Director of the Office of Management and Budget under the processes established under section 216 of the E-Government Act of 2002 (44 U.S.C. 3501 note), to facilitate the interoperability of geospatial information pertaining to homeland security among all users of such information within—

(I) the Department;

(II) State and local government; and

(III) the private sector;

(iii) coordinating with the Federal Geographic Data Committee and carrying out the responsibilities of the Department pursuant to Office of Management and Budget Circular A–16 and Executive Order 12906; and

(iv) making recommendations to the Secretary and the Executive Director of the Office for State and Local Government Coordination and Preparedness on awarding grants to—

(I) fund the creation of geospatial data; and

(II) execute information sharing agreements regarding geospatial data with State, local, and tribal governments.

(3) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this subsection for each fiscal year.

(Pub. L. 107–296, title VII, §703, Nov. 25, 2002, 116 Stat. 2219; Pub. L. 108–458, title VIII, §8201(b), Dec. 17, 2004, 118 Stat. 3865.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 216 of the E-Government Act of 2002, referred to in subsec. (b)(2)(D)(ii), is section 216 of Pub. L. 107–347, which is set out in a note under section 3501 of Title 44, Public Printing and Documents.

Executive Order 12906, referred to in subsec. (b)(2)(D)(iii), is set out as a note under section 1457 of Title 43, Public Lands.

AMENDMENTS

2004—Pub. L. 108–458 designated existing provisions as subsec. (a), inserted heading, and added subsec. (b).

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 108–458, title VIII, §8201(a), Dec. 17, 2004, 118 Stat. 3865, provided that: "Congress makes the following findings:

"(1) Geospatial technologies and geospatial data improve government capabilities to detect, plan for, prepare for, and respond to disasters in order to save lives and protect property.

"(2) Geospatial data improves the ability of information technology applications and systems to enhance public security in a cost-effective manner.

"(3) Geospatial information preparedness in the United States, and specifically in the Department of Homeland Security, is insufficient because of—

"(A) inadequate geospatial data compatibility;

"(B) insufficient geospatial data sharing; and

"(C) technology interoperability barriers."

§344. Chief Human Capital Officer

(a) In general

The Chief Human Capital Officer shall report directly to the Under Secretary for Management.

(b) Responsibilities

In addition to the responsibilities set forth in chapter 14 of title 5 and other applicable law, the Chief Human Capital Officer of the Department shall—

(1) develop and implement strategic workforce planning policies, including with respect to leader development and employee engagement, that are consistent with Government-wide leading principles, in line with Department strategic human capital goals and priorities, and informed by best practices within the Federal Government and the private sector, taking into account the special requirements of members of the Armed Forces serving in the Coast Guard;

(2) use performance measures to evaluate, on an ongoing basis, Department-wide strategic workforce planning efforts;

(3) develop, improve, and implement policies that, to the extent practicable, are informed by employee feedback, including compensation flexibilities available to Federal agencies where appropriate, to recruit, hire, train, and retain the workforce of the Department, in coordination with all components of the Department;

(4) identify methods for managing and overseeing human capital programs and initiatives, including leader development and employee engagement programs, in coordination with the head of each component of the Department;

(5) develop a career path framework and create opportunities for leader development in coordination with all components of the Department that is informed by an assessment, carried out by the Chief Human Capital Officer, of the learning and developmental needs of employees in supervisory and nonsupervisory roles across the Department and appropriate workforce planning initiatives;

(6) lead the efforts of the Department for managing employee resources, including training and development opportunities, in coordination with each component of the Department;

(7) work to ensure the Department is implementing human capital programs and initiatives and effectively educating each component of the Department about these programs and initiatives;

(8) identify and eliminate unnecessary and duplicative human capital policies and guidance;

(9) maintain a catalogue of available employee development opportunities, including the Homeland Security Rotation Program pursuant to section 414 of this title, departmental leadership development programs, interagency development programs, and other rotational programs;

(10) ensure that employee discipline and adverse action programs comply with the requirements of all pertinent laws, rules, regulations, and Federal guidance, and ensure due process for employees;

(11) analyze each Department or Government-wide Federal workforce satisfaction or morale survey not later than 90 days after the date of the publication of each such survey and submit to the Secretary such analysis, including, as appropriate, recommendations to improve workforce satisfaction or morale within the Department;

(12) review and approve all component employee engagement action plans to ensure such plans include initiatives responsive to the root cause of employee engagement challenges, as well as outcome-based performance measures and targets to track the progress of such initiatives;

(13) provide input concerning the hiring and performance of the Chief Human Capital Officer or comparable official in each component of the Department; and

(14) ensure that all employees of the Department are informed of their rights and remedies under chapters 12 and 23 of title 5.

(c) Component strategies

(1) In general

Each component of the Department shall, in coordination with the Chief Human Capital Officer of the Department, develop a 5-year workforce strategy for the component that will support the goals, objectives, and performance measures of the Department for determining the proper balance of Federal employees and private labor resources.

(2) Strategy requirements

In developing the strategy required under paragraph (1), each component shall consider the effect on human resources associated with creating additional Federal full-time equivalent positions, converting private contractors to Federal employees, or relying on the private sector for goods and services.

(d) Chief Learning and Engagement Officer

The Chief Human Capital Officer may designate an employee of the Department to serve as a Chief Learning and Engagement Officer to assist the Chief Human Capital Officer in carrying out this section.

(e) Annual submission

Not later than 90 days after the date on which the Secretary submits the annual budget justification for the Department, the Secretary shall submit to the congressional homeland security committees a report that includes a table, delineated by component with actual and enacted amounts, including—

(1) information on the progress within the Department of fulfilling the workforce strategies developed under subsection (c);

(2) information on employee development opportunities catalogued pursuant to paragraph (9) of subsection (b) and any available data on participation rates, attrition rates, and impacts on retention and employee satisfaction;

(3) information on the progress of Departmentwide strategic workforce planning efforts as determined under paragraph (2) of subsection (b);

(4) information on the activities of the steering committee established pursuant to section 351(a) of this title, including the number of meetings, types of materials developed and distributed, and recommendations made to the Secretary;

(5) the number of on-board staffing for Federal employees from the prior fiscal year;

(6) the total contract hours submitted by each prime contractor as part of the service contract inventory required under section 743 of the Financial Services and General Government Appropriations Act, 2010 (division C of Public Law 111–117; 31 U.S.C. 501 note); and

(7) the number of full-time equivalent personnel identified under the Intergovernmental Personnel Act of 1970 (42 U.S.C. 4701 et seq.).

(f) Limitation

Nothing in this section overrides or otherwise affects the requirements specified in section 468 of this title.

(Pub. L. 107–296, title VII, §704, Nov. 25, 2002, 116 Stat. 2219; Pub. L. 114–328, div. A, title XIX, §1904, Dec. 23, 2016, 130 Stat. 2674; Pub. L. 117–81, div. F, title LXIV, §6403, Dec. 27, 2021, 135 Stat. 2399.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Intergovernmental Personnel Act of 1970, referred to in subsec. (e)(7), is Pub. L. 91–648, Jan. 5, 1971, 84 Stat. 1909, which is classified principally to chapter 62 (§4701 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 4701 of Title 42 and Tables.

AMENDMENTS

2021—Subsec. (b)(1). Pub. L. 117–81, §6403(a)(1), inserted ", including with respect to leader development and employee engagement," after "policies" and "and informed by best practices within the Federal Government and the private sector," after "priorities,", and substituted ", in line" for "and in line".

Subsec. (b)(2). Pub. L. 117–81, §6403(1)(B), substituted "use performance measures to evaluate, on an ongoing basis," for "develop performance measures to provide a basis for monitoring and evaluating".

Subsec. (b)(3). Pub. L. 117–81, §6403(1)(C), inserted "that, to the extent practicable, are informed by employee feedback" after "policies".

Subsec. (b)(4). Pub. L. 117–81, §6403(1)(D), inserted "including leader development and employee engagement programs," before "in coordination".

Subsec. (b)(5). Pub. L. 117–81, §6403(1)(E), inserted "that is informed by an assessment, carried out by the Chief Human Capital Officer, of the learning and developmental needs of employees in supervisory and nonsupervisory roles across the Department and appropriate workforce planning initiatives" before semicolon at end.

Subsec. (b)(9) to (12). Pub. L. 117–81, §6403(1)(G), added pars. (9) to (12). Former pars. (9) and (10) redesignated (13) and (14), respectively.

Subsec. (b)(13), (14). Pub. L. 117–81, §6403(1)(F), redesignated pars. (9) and (10) as (13) and (14), respectively.

Subsec. (d). Pub. L. 117–81, §6403(3), added subsec. (d). Former subsec. (d) redesignated (e).

Subsec. (e). Pub. L. 117–81, §6403(2), (4), redesignated subsec. (d) as (e), inserted pars. (2) to (4), and redesignated former pars. (2) to (4) as (5) to (7), respectively.

Subsec. (f). Pub. L. 117–81, §6403(2), redesignated subsec. (e) as (f).

2016—Pub. L. 114–328 amended section generally. Prior to amendment, text read as follows: "The Chief Human Capital Officer shall report to the Secretary, or to another official of the Department, as the Secretary may direct and shall ensure that all employees of the Department are informed of their rights and remedies under chapters 12 and 23 of title 5 by—

"(1) participating in the 2302(c) Certification Program of the Office of Special Counsel;

"(2) achieving certification from the Office of Special Counsel of the Department's compliance with section 2302(c) of title 5; and

"(3) informing Congress of such certification not later than 24 months after November 25, 2002."

§345. Establishment of Officer for Civil Rights and Civil Liberties

(a) In general

The Officer for Civil Rights and Civil Liberties, who shall report directly to the Secretary, shall—

(1) review and assess information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of the Department;

(2) make public through the Internet, radio, television, or newspaper advertisements information on the responsibilities and functions of, and how to contact, the Officer;

(3) assist the Secretary, directorates, and offices of the Department to develop, implement, and periodically review Department policies and procedures to ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities;

(4) oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department;

(5) coordinate with the Privacy Officer to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports regarding such programs, policies, and procedures; and

(6) investigate complaints and information indicating possible abuses of civil rights or civil liberties, unless the Inspector General of the Department determines that any such complaint or information should be investigated by the Inspector General.

(b) Report

The Secretary shall submit to the President of the Senate, the Speaker of the House of Representatives, and the appropriate committees and subcommittees of Congress on an annual basis a report on the implementation of this section, including the use of funds appropriated to carry out this section, and detailing any allegations of abuses described under subsection (a)(1) and any actions taken by the Department in response to such allegations.

(Pub. L. 107–296, title VII, §705, Nov. 25, 2002, 116 Stat. 2219; Pub. L. 108–458, title VIII, §8303, Dec. 17, 2004, 118 Stat. 3867.)

EDITORIAL NOTES

AMENDMENTS

2004—Subsec. (a). Pub. L. 108–458, §8303(1), reenacted heading without change and amended introductory provisions generally. Prior to amendment, introductory provisions read as follows: "The Secretary shall appoint in the Department an Officer for Civil Rights and Civil Liberties, who shall—".

Subsec. (a)(1). Pub. L. 108–458, §8303(2), amended par. (1) generally. Prior to amendment, par. (1) read as follows: "review and assess information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees and officials of the Department; and".

Subsec. (a)(3) to (6). Pub. L. 108–458, §8303(3), (4), added pars. (3) to (6).

§346. Consolidation and co-location of offices

Not later than 1 year after November 25, 2002, the Secretary shall develop and submit to Congress a plan for consolidating and co-locating—

(1) any regional offices or field offices of agencies that are transferred to the Department under this chapter, if such officers [1] are located in the same municipality; and

(2) portions of regional and field offices of other Federal agencies, to the extent such offices perform functions that are transferred to the Secretary under this chapter.

(Pub. L. 107–296, title VII, §706, Nov. 25, 2002, 116 Stat. 2220.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in pars. (1) and (2), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this

chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

[1] So in original. Probably should be "offices".

§347. Quadrennial homeland security review

(a) Requirement

(1) Quadrennial reviews required

In fiscal year 2009, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a "quadrennial homeland security review").

(2) Scope of reviews

Each quadrennial homeland security review shall be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.

(3) Consultation

The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with—

(A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture the Secretary of Energy,,[1] and the Director of National Intelligence;

(B) key officials of the Department, including the Under Secretary for Strategy, Policy, and Plans;

(C) representatives from appropriate advisory committees established pursuant to section 451 of this title, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49; and

(D) other relevant governmental and nongovernmental entities, including State, local, and tribal government officials, members of Congress, private sector representatives, academics, and other policy experts.

(4) Relationship with future years homeland security program

The Secretary shall ensure that each review conducted under this section is coordinated with the Future Years Homeland Security Program required under section 454 of this title.

(b) Contents of review

In each quadrennial homeland security review, the Secretary shall—

(1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan;

(2) outline and prioritize the full range of the critical homeland security mission areas of the Nation based on the risk assessment required pursuant to subsection (c)(2)(B);

(3) describe, to the extent practicable, the interagency cooperation, preparedness of Federal response assets, infrastructure, resources required, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy,

required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(4) identify, to the extent practicable, the resources required to execute the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2), including any resources identified from redundant, wasteful, or unnecessary capabilities or capacities that may be redirected to better support other existing capabilities or capacities, as the case may be; and

(5) include an assessment of the organizational alignment of the Department with the national homeland security strategy referred to in paragraph (1) and the homeland security mission areas outlined under paragraph (2).

(c) Reporting

(1) In general

Not later than 60 days after the date of the submission of the President's budget for the fiscal year after the fiscal year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.

(2) Contents of report

Each report submitted under paragraph (1) shall include—

(A) the results of the quadrennial homeland security review;

(B) a risk assessment of the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review or for purposes of the quadrennial EMP and GMD risk assessment under section 195f(d)(1)(E) of this title;

(C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the Nation, as required under subsection (b)(2);

(D) to the extent practicable, a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, resources required, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2);

(E) an assessment of the organizational alignment of the Department with the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2), including the Department's organizational structure, management systems, budget and accounting systems, human resources systems, procurement systems, and physical and technical infrastructure;

(F) to the extent practicable, a discussion of cooperation among Federal agencies in the effort to promote national homeland security;

(G) to the extent practicable, a discussion of cooperation between the Federal Government and State, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats and risks to national homeland security; and

(H) any other matter the Secretary considers appropriate.

(3) Documentation

The Secretary shall retain and, upon request, provide to Congress the following documentation regarding each quadrennial homeland security review:

(A) Records regarding the consultation carried out pursuant to subsection (a)(3), including the following:

(i) All written communications, including communications sent out by the Secretary and feedback submitted to the Secretary through technology, online communications tools, in-person discussions, and the interagency process.

(ii) Information on how feedback received by the Secretary informed each such quadrennial homeland security review.

(B) Information regarding the risk assessment required pursuant to subsection (c)(2)(B), including the following:

(i) The risk model utilized to generate such risk assessment.

(ii) Information, including data used in the risk model, utilized to generate such risk assessment.

(iii) Sources of information, including other risk assessments, utilized to generate such risk assessment.

(iv) Information on assumptions, weighing factors, and subjective judgments utilized to generate such risk assessment, together with information on the rationale or basis thereof.

(4) Public availability

The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on the Internet website of the Department.

(d) Review

Not later than 90 days after the submission of each report required under subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the degree to which the findings and recommendations developed in the quadrennial homeland security review that is the subject of such report were integrated into the acquisition strategy and expenditure plans for the Department.

(e) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this section.

(Pub. L. 107–296, title VII, §707, as added Pub. L. 110–53, title XXIV, §2401(a), Aug. 3, 2007, 121 Stat. 543; amended Pub. L. 114–328, div. A, title XIX, §1902(b), Dec. 23, 2016, 130 Stat. 2672; Pub. L. 116–92, div. A, title XVII, §1740(b), Dec. 20, 2019, 133 Stat. 1824; Pub. L. 117–263, div. G, title LXXI, §7141(a), Dec. 23, 2022, 136 Stat. 3652.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (a)(3)(C), (D). Pub. L. 117–263, §7141(a)(1), added subpar. (C) and redesignated former subpar. (C) as (D).

Subsec. (b)(2). Pub. L. 117–263, §7141(a)(2)(A), inserted "based on the risk assessment required pursuant to subsection (c)(2)(B)" before semicolon at end.

Subsec. (b)(3). Pub. L. 117–263, §7141(a)(2)(B), inserted ", to the extent practicable," after "describe" and substituted "resources required" for "budget plan".

Subsec. (b)(4). Pub. L. 117–263, §7141(a)(2)(C), inserted ", to the extent practicable," after "identify" and substituted "resources required to" for "budget plan required to provide sufficient resources to successfully" and ", including any resources identified from redundant, wasteful, or unnecessary capabilities or capacities that may be redirected to better support other existing capabilities or capacities, as the case may be; and" for semicolon at end.

Subsec. (b)(6). Pub. L. 117–263, §7141(a)(2)(D), (E), struck out par. (6) which read as follows: "review and assess the effectiveness of the mechanisms of the Department for executing the process of turning the requirements developed in the quadrennial homeland security review into an acquisition strategy and expenditure plan within the Department."

Subsec. (c)(1). Pub. L. 117–263, §7141(a)(3)(A), substituted "60 days after the date of the submission of the President's budget for the fiscal year after the fiscal year" for "December 31 of the year".

Subsec. (c)(2)(B). Pub. L. 117–263, §7141(a)(3)(B)(i), substituted "risk assessment of" for "description of the threats to".

Subsec. (c)(2)(C). Pub. L. 117–263, §7141(a)(3)(B)(ii), inserted ", as required under subsection (b)(2)" before semicolon at end.

Subsec. (c)(2)(D). Pub. L. 117–263, §7141(a)(3)(B)(iii), inserted "to the extent practicable," before "a

description" and substituted "resources required" for "budget plan".

Subsec. (c)(2)(F). Pub. L. 117–263, §7141(a)(3)(B)(iv), inserted "to the extent practicable," before "a discussion" and struck out "the status of" before "cooperation".

Subsec. (c)(2)(G). Pub. L. 117–263, §7141(a)(3)(B)(v), inserted "to the extent practicable," before "a discussion", "and risks" before "to national homeland", and "and" after semicolon at end and struck out "the status of" before "cooperation".

Subsec. (c)(2)(H), (I). Pub. L. 117–263, §7141(a)(3)(B)(vi), (vii), redesignated subpar. (I) as (H) and struck out former subpar. (H) which read as follows: "an explanation of any underlying assumptions used in conducting the review; and".

Subsec. (c)(3), (4). Pub. L. 117–263, §7141(a)(3)(C), (D), added par. (3) and redesignated former par. (3) as (4).

Subsecs. (d), (e). Pub. L. 117–263, §7141(a)(4), (5), added subsec. (d) and redesignated former subsec. (d) as (e).

2019—Subsec. (a)(3)(A). Pub. L. 116–92, §1740(b)(1), inserted "the Secretary of Energy," after "the Secretary of Agriculture".

Subsec. (c)(2)(B). Pub. L. 116–92, §1740(b)(2), which directed insertion of "or for purposes of the quadrennial EMP and GMD risk assessment under section 195f(d)(1)(E) of this title" after review, was executed by making the insertion after "review" as if quotation marks had appeared around the word in the directory language, to reflect the probable intent of Congress.

2016—Subsec. (a)(3)(B). Pub. L. 114–328 inserted ", including the Under Secretary for Strategy, Policy, and Plans" after "Department".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2022 AMENDMENT

Pub. L. 117–263, div. G, title LXXI, §7141(b), Dec. 23, 2022, 136 Stat. 3654, provided that: "The amendments made by this Act [probably means "this section", amending this section] shall apply with respect to a quadrennial homeland security review conducted after December 31, 2021."

PREPARATION FOR FIRST QUADRENNIAL HOMELAND SECURITY REVIEW

Pub. L. 110–53, title XXIV, §2401(b), Aug. 3, 2007, 121 Stat. 546, provided that:

"(1) IN GENERAL.—During fiscal years 2007 and 2008, the Secretary of Homeland Security shall make preparations to conduct the first quadrennial homeland security review under section 707 of the Homeland Security Act of 2002 [6 U.S.C. 347], as added by subsection (a), in fiscal year 2009, including—

"(A) determining the tasks to be performed;

"(B) estimating the human, financial, and other resources required to perform each task;

"(C) establishing the schedule for the execution of all project tasks;

"(D) ensuring that these resources will be available as needed; and

"(E) all other preparations considered necessary by the Secretary.

"(2) REPORT.—Not later than 60 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary shall submit to Congress and make publicly available on the Internet website of the Department of Homeland Security a detailed resource plan specifying the estimated budget and number of staff members that will be required for preparation of the first quadrennial homeland security review."

[1] *So in original.*

§348. Joint task forces

(a) Definition

In this section, the term "situational awareness" means knowledge and unified understanding of unlawful cross-border activity, including—

(1) threats and trends concerning illicit trafficking and unlawful crossings;

(2) the ability to forecast future shifts in such threats and trends;

(3) the ability to evaluate such threats and trends at a level sufficient to create actionable plans; and

(4) the operational capability to conduct continuous and integrated surveillance of the air, land, and maritime borders of the United States.

(b) Joint task forces

(1) Establishment

The Secretary may establish and operate departmental Joint Task Forces to conduct joint operations using personnel and capabilities of the Department for the purposes specified in paragraph (2).

(2) Purposes

(A) In general

Subject to subparagraph (B), the purposes referred to in paragraph (1) are or relate to the following:

(i) Securing the land and maritime borders of the United States.

(ii) Homeland security crises.

(iii) Establishing regionally-based operations.

(B) Limitation

(i) In general

The Secretary may not establish a Joint Task Force for any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or an incident for which the Federal Emergency Management Agency has primary responsibility for management of the response under subchapter V of this chapter, including section 314(a)(3)(A) of this title, unless the responsibilities of such a Joint Task Force—

(I) do not include operational functions related to incident management, including coordination of operations; and

(II) are consistent with the requirements of paragraphs (3) and (4)(A) of section 313(c) and section 319(c) of this title, and section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

(ii) Responsibilities and functions not reduced

Nothing in this section may be construed to reduce the responsibilities or functions of the Federal Emergency Management Agency or the Administrator of the Agency under subchapter V of this chapter or any other provision of law, including the diversion of any asset, function, or mission from the Agency or the Administrator of the Agency pursuant to section 316 of this title.

(3) Joint task force directors

(A) Director

Each Joint Task Force established and operated pursuant to paragraph (1) shall be headed by a Director, appointed by the President, for a term of not more than two years. The Secretary shall submit to the President recommendations for such appointments after consulting with the heads of the components of the Department with membership on any such Joint Task Force. Any Director appointed by the President shall be—

(i) a current senior official of the Department with not less than one year of significant leadership experience at the Department; or

(ii) if no suitable candidate is available at the Department, an individual with—

(I) not less than one year of significant leadership experience in a Federal agency since the establishment of the Department; and

(II) a demonstrated ability in, knowledge of, and significant experience working on the issues to be addressed by any such Joint Task Force.

(B) Extension

The Secretary may extend the appointment of a Director of a Joint Task Force under subparagraph (A) for not more than two years if the Secretary determines that such an extension is in the best interest of the Department.

(4) Joint Task Force deputy directors

For each Joint Task Force, the Secretary shall appoint a Deputy Director who shall be an official of a different component or office of the Department than the Director of such Joint Task Force.

(5) Responsibilities

The Director of a Joint Task Force, subject to the oversight, direction, and guidance of the Secretary, shall—

(A) when established for the purpose referred to in paragraph (2)(A)(i), maintain situational awareness within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(B) provide operational plans and requirements for standard operating procedures and contingency operations within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(C) plan and execute joint task force activities within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(D) set and accomplish strategic objectives through integrated operational planning and execution;

(E) exercise operational direction over personnel and equipment from components and offices of the Department allocated to the Joint Task Force to accomplish the objectives of the Joint Task Force;

(F) when established for the purpose referred to in paragraph (2)(A)(i), establish operational and investigative priorities within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(G) coordinate with foreign governments and other Federal, State, and local agencies, as appropriate, to carry out the mission of the Joint Task Force; and

(H) carry out other duties and powers the Secretary determines appropriate.

(6) Personnel and resources

(A) In general

The Secretary may, upon request of the Director of a Joint Task Force, and giving appropriate consideration of risk to the other primary missions of the Department, allocate to such Joint Task Force on a temporary basis personnel and equipment of components and offices of the Department.

(B) Cost neutrality

A Joint Task Force may not require more resources than would have otherwise been required by the Department to carry out the duties assigned to such Joint Task Force if such Joint Task Force had not been established.

(C) Location of operations

In establishing a location of operations for a Joint Task Force, the Secretary shall, to the extent practicable, use existing facilities that integrate efforts of components of the Department and State, local, tribal, or territorial law enforcement or military entities.

(D) Consideration of impact

When reviewing requests for allocation of component personnel and equipment under subparagraph (A), the Secretary shall consider the impact of such allocation on the ability of the donating component or office to carry out the primary missions of the Department, and in the case of the Coast Guard, the missions specified in section 468 of this title.

(E) Limitation

Personnel and equipment of the Coast Guard allocated under this paragraph may be used only to carry out operations and investigations related to the missions specified in section 468 of this title.

(F) Report

The Secretary shall, at the time the budget of the President is submitted to Congress for a fiscal year under section 1105(a) of title 31, submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report on the total funding, personnel, and other resources that each component or office of the Department allocated under this paragraph to each Joint Task Force to carry out the mission of such Joint Task Force during the fiscal year immediately preceding each such report, and a description of the degree to which the resources drawn from each component or office impact the primary mission of such component or office.

(7) Component resource authority

As directed by the Secretary—

(A) each Director of a Joint Task Force shall be provided sufficient resources from relevant components and offices of the Department and the authority necessary to carry out the missions and responsibilities of such Joint Task Force required under this section;

(B) the resources referred to in subparagraph (A) shall be under the operational authority, direction, and control of the Director of the Joint Task Force to which such resources are assigned; and

(C) the personnel and equipment of each Joint Task Force shall remain under the administrative direction of the head of the component or office of the Department that provided such personnel or equipment.

(8) Joint Task Force staff

(A) In general

Each Joint Task Force shall have a staff, composed of personnel from relevant components and offices of the Department, to assist the Director of such Joint Task Force in carrying out the mission and responsibilities of such Joint Task Force.

(B) Report

The Secretary shall include in the report submitted under paragraph (6)(F)—

(i) the number of personnel of each component or office permanently assigned to each Joint Task Force; and

(ii) the number of personnel of each component or office assigned on a temporary basis to each Joint Task Force.

(9) Mission; establishment of performance metrics

The Secretary shall—

(A) using leading practices in performance management and lessons learned by other law enforcement task forces and joint operations, establish—

(i) the mission, strategic goals, and objectives of each Joint Task Force;

(ii) the criteria for terminating each Joint Task Force;

(iii) outcome-based and other appropriate performance metrics for evaluating the effectiveness of each Joint Task Force with respect to the mission, strategic goals, and objectives established pursuant to clause (i), including—

(I) targets for each Joint Task Force to achieve by not later than one and three years after such establishment; and

(II) a description of the methodology used to establish such metrics; and

(iv) a staffing plan for each Joint Task Force;

(B) not later than 120 days after December 23, 2022, and 120 days after the establishment of a new Joint Task Force, as appropriate, submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate the mission, strategic goals, objectives, and metrics established under subparagraph (A); and

(C) not later than December 23, 2024, and annually thereafter, submit to the committees specified in subparagraph (B) a report containing information regarding—

(i) the progress in implementing the outcome-based and other appropriate performance metrics established pursuant to subparagraph (A)(iii);

(ii) the staffing plan developed for each Joint Task Force pursuant to subparagraph (A)(iv); and

(iii) any modification to the mission, strategic goals, and objectives of each Joint Task Force, and a description of, and rationale for, any such modifications.

(10) Joint duty training program

(A) In general

The Secretary shall—

(i) establish a joint duty training program in the Department for the purposes of—

(I) enhancing coordination within the Department; and

(II) promoting workforce professional development; and

(ii) tailor such joint duty training program to improve joint operations as part of the Joint Task Forces.

(B) Elements

The joint duty training program established under subparagraph (A) shall address, at a minimum, the following topics:

(i) National security strategy.

(ii) Strategic and contingency planning.

(iii) Command and control of operations under joint command.

(iv) International engagement.

(v) The homeland security enterprise.

(vi) Interagency collaboration.

(vii) Leadership.

(viii) Specific subject matters relevant to the Joint Task Force, including matters relating to the missions specified in section 468 of this title, to which the joint duty training program is assigned.

(C) Training required

(i) Directors and deputy directors

Except as provided in clauses (iii) and (iv), an individual shall complete the joint duty training program before being appointed Director or Deputy Director of a Joint Task Force.

(ii) Joint Task Force staff

Each official serving on the staff of a Joint Task Force shall complete the joint duty training program within the first year of assignment to such Joint Task Force.

(iii) Exception

Clause (i) shall not apply to the first Director or Deputy Director appointed to a Joint Task Force on or after December 23, 2016.

(iv) Waiver

The Secretary may waive the application of clause (i) if the Secretary determines that such a waiver is in the interest of homeland security or necessary to carry out the mission for

which a Joint Task Force was established.

(11) Notification of Joint Task Force formation or termination

(A) In general

Not later than seven days after establishing or terminating a Joint Task Force under this subsection, the Secretary shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a notification regarding such establishment or termination, as the case may be. The contents of any such notification shall include the following:

(i) The criteria and conditions required to establish or terminate the Joint Task Force at issue.

(ii) The primary mission, strategic goals, objectives, and plan of operations of such Joint Task Force.

(iii) If such notification is a notification of termination, information on the effectiveness of such Joint Task Force as measured by the outcome-based performance metrics and other appropriate performance metrics established pursuant to paragraph (9)(A)(iii).

(iv) The funding and resources required to establish or terminate such Joint Task Force.

(v) The number of personnel of each component or office permanently assigned to such Joint Task Force.

(vi) The number of personnel of each component and office assigned on a temporary basis to such Joint Task Force.

(vii) If such notification is a notification of establishment, the anticipated costs of establishing and operating such Joint Task Force.

(viii) If such notification is a notification of termination, funding allocated in the immediately preceding fiscal year to such Joint Task Force for—

(I) operations, notwithstanding such termination; and

(II) activities associated with such termination.

(ix) The anticipated establishment or actual termination date of such Joint Task Force, as the case may be.

(B) Waiver authority

The Secretary may waive the requirement under subparagraph (A) in the event of an emergency circumstance that imminently threatens the protection of human life or property.

(12) Review

(A) In general

Not later than one year after December 23, 2022, the Comptroller General of the United States shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate an assessment of the effectiveness of the Secretary's utilization of the authority provided under this section for the purposes specified in subsection (b)(2) as among the range of options available to the Secretary to conduct joint operations among departmental components and offices and a review of the Joint Task Forces established under this subsection.

(B) Contents

The review required under subparagraph (A) shall include—

(i) an assessment of methodology utilized to determine whether to establish or terminate

each Joint Task Force; and

(ii) an assessment of the effectiveness of oversight over each Joint Task Force, with specificity regarding the Secretary's utilization of outcome-based or other appropriate performance metrics (established pursuant to paragraph (9)(A)(iii)) to evaluate the effectiveness of each Joint Task Force in measuring progress with respect to the mission, strategic goals, and objectives (established pursuant to paragraph (9)(A)(i)) of such Joint Task Force.

(13) Sunset

This section expires on September 30, 2026.

(c) Joint duty assignment program

After establishing the joint duty training program under subsection (b)(10), the Secretary shall establish a joint duty assignment program within the Department for the purposes of enhancing coordination in the Department and promoting workforce professional development.

(Pub. L. 107–296, title VII, §708, as added Pub. L. 114–328, div. A, title XIX, §1901(b), Dec. 23, 2016, 130 Stat. 2665; amended Pub. L. 117–263, div. G, title LXXI, §7111(b), Dec. 23, 2022, 136 Stat. 3625; Pub. L. 118–103, §2(a), Oct. 1, 2024, 138 Stat. 1584.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (b)(2)(B)(i), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

AMENDMENTS

2024—Subsec. (b)(9)(A)(iv). Pub. L. 118–103, §2(a)(1)(A), added cl. (iv).

Subsec. (b)(9)(C). Pub. L. 118–103, §2(a)(1)(B), amended subpar. (C) generally. Prior to amendment, subpar. (C) read as follows: "not later than one year after December 23, 2022, and annually thereafter, submit to the committees specified in subparagraph (B) a report that contains information on the progress in implementing the outcome-based and other appropriate performance metrics established pursuant to subparagraph (A)(iii)."

Subsec. (b)(13). Pub. L. 118–103, §2(a)(2), substituted "2026" for "2024".

2022—Subsec. (b)(8). Pub. L. 117–263, §7111(b)(1), amended par. (8) generally. Prior to amendment, text read as follows: "Each Joint Task Force shall have a staff, composed of officials from relevant components and offices of the Department, to assist the Director of such Joint Task Force in carrying out the mission and responsibilities of such Joint Task Force."

Subsec. (b)(9). Pub. L. 117–263, §7111(b)(2)(A), substituted "Mission; establishment" for "Establishment" in heading.

Subsec. (b)(9)(A). Pub. L. 117–263, §7111(b)(2)(B), amended subpar. (A) generally. Prior to amendment, subpar. (A) read as follows: "establish outcome-based and other appropriate performance metrics to evaluate the effectiveness of each Joint Task Force;".

Subsec. (b)(9)(B). Pub. L. 117–263, §7111(b)(2)(C), substituted "December 23, 2022" for "December 23, 2016" and "; and" for period at end and inserted "mission, strategic goals, objectives, and" before "metrics".

Subsec. (b)(9)(C). Pub. L. 117–263, §7111(b)(2)(D), amended subpar. (C) generally. Prior to amendment, subpar. (C) read as follows: "not later than January 31 of each year beginning in 2017, submit to each committee specified in subparagraph (B) a report that contains the evaluation described in subparagraph (A)."

Subsec. (b)(11). Pub. L. 117–263, §7111(b)(3)(A), inserted "or termination" after "formation" in heading.

Subsec. (b)(11)(A). Pub. L. 117–263, §7111(b)(3)(B), amended subpar. (A) generally. Prior to amendment, subpar. (A) read as follows: "Not later than 90 days before establishing a Joint Task Force under this subsection, the Secretary shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the Committee on Homeland Security and the Committee on

Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a notification regarding such establishment."

Subsec. (b)(12)(A). Pub. L. 117–263, §7111(b)(4)(A), substituted "one year after December 23, 2022, the Comptroller General of the United States" for "January 31, 2018, and January 31, 2021, the Inspector General of the Department" and inserted "an assessment of the effectiveness of the Secretary's utilization of the authority provided under this section for the purposes specified in subsection (b)(2) as among the range of options available to the Secretary to conduct joint operations among departmental components and offices and" before "a review of the Joint Task Forces".

Subsec. (b)(12)(B). Pub. L. 117–263, §7111(b)(4)(B)(i), substituted "review" for "reviews" in introductory provisions.

Subsec. (b)(12)(B)(i), (ii). Pub. L. 117–263, §7111(b)(4)(B)(ii), amended cls. (i) and (ii) generally. Prior to amendment, cls. (i) and (ii) read as follows:

"(i) an assessment of the effectiveness of the structure of each Joint Task Force; and

"(ii) recommendations for enhancements to such structure to strengthen the effectiveness of each Joint Task Force."

Subsec. (b)(13). Pub. L. 117–263, §7111(b)(5), substituted "2024" for "2022".

STATUTORY NOTES AND RELATED SUBSIDIARIES

ANNUAL BRIEFING

Pub. L. 118–103, §2(b), Oct. 1, 2024, 138 Stat. 1584, provided that:

"(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act [Oct. 1, 2024], and annually thereafter, the Secretary of Homeland Security shall brief—

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(B) the Committee on Commerce, Science, and Transportation of the Senate;

"(C) the Committee on Homeland Security of the House of Representatives; and

"(D) the Committee on Transportation and Infrastructure of the House of Representatives.

"(2) TOPICS.—Each briefing required under paragraph (1) shall cover the latest staffing and resource assessment at Joint Task Force-East, including—

"(A)(i) a determination of whether the current staffing levels of Joint Task Force-East are sufficient to successfully advance the mission, strategic goals, and objectives of such Joint Task Force; and

"(ii) if such determination reveals insufficient staffing levels, the cost, timeline, and strategy for increasing such staffing levels; and

"(B)(i) a determination of whether sufficient resources are being provided for Joint Task Force-East in accordance with section 708(b)(7)(a) of the Homeland Security Act of 2002 (6 U.S.C. 348(b)(7)(a)); and

"(ii) if such determination reveals insufficient resource levels, the cost, timeline, and strategy for providing any remaining resource requirements."

TRANSITION PROVISIONS

Pub. L. 114–328, div. A, title XIX, §1901(c), Dec. 23, 2016, 130 Stat. 2670, provided that: "An individual serving as a Director of a Joint Task Force of the Department of Homeland Security in existence on the day before the date of the enactment of this section [Dec. 23, 2016] may serve as the Director of such Joint Task Force on and after such date of enactment until a Director of such Joint Task Force is appointed pursuant to subparagraph (A) of section 708(b)(3) [6 U.S.C. 348(b)(3)], as added by subsection (a) of this section."

§349. Office of Strategy, Policy, and Plans

(a) In general

There is established in the Department an Office of Strategy, Policy, and Plans.

(b) Head of Office

The Office of Strategy, Policy, and Plans shall be headed by an Under Secretary for Strategy, Policy, and Plans, who shall serve as the principal policy advisor to the Secretary. The Under Secretary for Strategy, Policy, and Plans shall be appointed by the President, by and with the advice and consent of the Senate.

(c) Functions

The Under Secretary for Strategy, Policy, and Plans shall—

(1) lead, conduct, and coordinate Department-wide policy development and implementation and strategic planning;

(2) develop and coordinate policies to promote and ensure quality, consistency, and integration for the programs, components, offices, and activities across the Department;

(3) develop and coordinate strategic plans and long-term goals of the Department with risk-based analysis and planning to improve operational mission effectiveness, including consultation with the Secretary regarding the quadrennial homeland security review under section 347 of this title;

(4) manage Department leadership councils and provide analytics and support to such councils;

(5) manage international coordination and engagement for the Department;

(6) review and incorporate, as appropriate, external stakeholder feedback into Department policy; and

(7) carry out such other responsibilities as the Secretary determines appropriate.

(d) Deputy Under Secretary

(1) In general

The Secretary may—

(A) establish within the Office of Strategy, Policy, and Plans a position of Deputy Under Secretary to support the Under Secretary for Strategy, Policy, and Plans in carrying out the Under Secretary's responsibilities; and

(B) appoint a career employee to such position.

(2) Limitation on establishment of Deputy Under Secretary positions

A Deputy Under Secretary position (or any substantially similar position) within the Office of Strategy, Policy, and Plans may not be established except for the position provided for by paragraph (1), unless the Secretary receives prior authorization from Congress.

(3) Definitions

For purposes of paragraph (1)—

(A) the term "career employee" means any employee (as such term is defined in section 2105 of title 5), but does not include a political appointee; and

(B) the term "political appointee" means any employee who occupies a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

(e) Coordination by Department components

To ensure consistency with the policy priorities of the Department, the head of each component of the Department shall coordinate with the Office of Strategy, Policy, and Plans in establishing or modifying policies or strategic planning guidance with respect to each such component.

(f) Homeland Security statistics and joint analysis

(1) Homeland Security statistics

The Under Secretary for Strategy, Policy, and Plans shall—

(A) establish standards of reliability and validity for statistical data collected and analyzed by the Department;

(B) be provided by the heads of all components of the Department with statistical data maintained by the Department regarding the operations of the Department;

(C) conduct or oversee analysis and reporting of such data by the Department as required by law or as directed by the Secretary; and

(D) ensure the accuracy of metrics and statistical data provided to Congress.

(2) Transfer of responsibilities

There shall be transferred to the Under Secretary for Strategy, Policy, and Plans the

maintenance of all immigration statistical information of U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and United States Citizenship and Immigration Services, which shall include information and statistics of the type contained in the publication entitled "Yearbook of Immigration Statistics" prepared by the Office of Immigration Statistics, including region-by-region statistics on the aggregate number of applications and petitions filed by an alien (or filed on behalf of an alien) and denied, and the reasons for such denials, disaggregated by category of denial and application or petition type.

(g) Assistant Secretary

(1) In general

There is established within the Office of Strategy, Policy, and Plans an Assistant Secretary, who shall assist the Secretary in carrying out the duties under paragraph (2) and the responsibilities under paragraph (3). Notwithstanding section 113(a)(1) of this title, the Assistant Secretary established under this paragraph shall be appointed by the President without the advice and consent of the Senate.

(2) Duties

At the direction of the Secretary, the Assistant Secretary established under paragraph (1) shall be responsible for policy formulation regarding matters relating to economic security and trade, as such matters relate to the mission and the operations of the Department.

(3) Additional responsibilities

In addition to the duties specified in paragraph (2), the Assistant Secretary established under paragraph (1), at the direction of the Secretary, may—

(A) oversee—

(i) coordination of supply chain policy; and

(ii) assessments and reports to Congress related to critical economic security domains;

(B) coordinate with stakeholders in other Federal departments and agencies and nongovernmental entities with trade and economic security interests, authorities, and responsibilities; and

(C) perform such additional duties as the Secretary or the Under Secretary of Strategy, Policy, and Plans may prescribe.

(4) Definitions

In this subsection:

(A) Critical economic security domain

The term "critical economic security domain" means any infrastructure, industry, technology, or intellectual property (or combination thereof) that is essential for the economic security of the United States.

(B) Economic security

The term "economic security" has the meaning given such term in section 474(c)(2) of this title.

(h) Limitation

Nothing in this section overrides or otherwise affects the requirements specified in section 468 of this title.

(Pub. L. 107–296, title VII, §709, as added Pub. L. 114–328, div. A, title XIX, §1902(a), Dec. 23, 2016, 130 Stat. 2670; amended Pub. L. 117–263, div. G, title LXXI, §7116(b), Dec. 23, 2022, 136 Stat. 3637.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsecs. (g), (h). Pub. L. 117–263 added subsec. (g) and redesignated former subsec. (g) as (h).

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 117–263, div. G, title LXXI, §7116(c), Dec. 23, 2022, 136 Stat. 3638, provided that: "Nothing in this section [amending this section and enacting provisions set out as a note under section 451 of this title] or the amendments made by this section may be construed to affect or diminish the authority otherwise granted to any other officer of the Department of Homeland Security."

§350. Workforce health and medical support

(a) In general

The Under Secretary for Management shall be responsible for workforce-focused health and medical activities of the Department. The Under Secretary for Management may further delegate responsibility for those activities, as appropriate.

(b) Responsibilities

The Under Secretary for Management, in coordination with the Chief Medical Officer, shall—

(1) provide oversight and coordinate the medical and health activities of the Department for the human and animal personnel of the Department;

(2) establish medical, health, veterinary, and occupational health exposure policy, guidance, strategies, and initiatives for the human and animal personnel of the Department;

(3) as deemed appropriate by the Under Secretary, provide medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on occupational medical and public health issues;

(4) serve as the primary representative for the Department on agreements regarding the detail of Commissioned Corps officers of the Public Health Service of the Department of Health and Human Services to the Department, except that components of the Department shall retain authority for funding, determination of specific duties, and supervision of such detailed Commissioned Corps officers; and

(5) perform such other duties relating to the responsibilities described in this subsection as the Secretary may require.

(Pub. L. 107–296, title VII, §710, as added Pub. L. 115–387, §2(d), Dec. 21, 2018, 132 Stat. 5167.)

§351. Employee engagement

(a) Steering committee

Not later than 120 days after December 27, 2021, the Secretary shall establish an employee engagement steering committee, including representatives from operational components, headquarters, and field personnel, including supervisory and nonsupervisory personnel, and employee labor organizations that represent Department employees, and chaired by the Under Secretary for Management, to carry out the following activities:

(1) Identify factors that have a negative impact on employee engagement, morale, and communications within the Department, such as perceptions about limitations on career progression, mobility, or development opportunities, collected through employee feedback platforms, including through annual employee surveys, questionnaires, and other communications, as appropriate.

(2) Identify, develop, and distribute initiatives and best practices to improve employee engagement, morale, and communications within the Department, including through annual employee surveys, questionnaires, and other communications, as appropriate.

(3) Monitor efforts of each component to address employee engagement, morale, and communications based on employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate.

(4) Advise the Secretary on efforts to improve employee engagement, morale, and communications within specific components and across the Department.

(5) Conduct regular meetings and report, not less than once per quarter, to the Under Secretary for Management, the head of each component, and the Secretary on Departmentwide efforts to improve employee engagement, morale, and communications.

(b) Action plan; reporting

The Secretary, acting through the Chief Human Capital Officer, shall—

(1) not later than 120 days after the date of the establishment of the employee engagement steering committee under subsection (a), issue a Departmentwide employee engagement action plan, reflecting input from the steering committee and employee feedback provided through annual employee surveys, questionnaires, and other communications in accordance with paragraph (1) of such subsection, to execute strategies to improve employee engagement, morale, and communications within the Department; and

(2) require the head of each component to—

(A) develop and implement a component-specific employee engagement plan to advance the action plan required under paragraph (1) that includes performance measures and objectives, is informed by employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate, and sets forth how employees and, where applicable, their labor representatives are to be integrated in developing programs and initiatives;

(B) monitor progress on implementation of such action plan; and

(C) provide to the Chief Human Capital Officer and the steering committee quarterly reports on actions planned and progress made under this paragraph.

(c) Termination

This section shall terminate on the date that is five years after December 27, 2021.

(Pub. L. 107–296, title VII, §711, as added Pub. L. 117–81, div. F, title LXIV, §6401(a), Dec. 27, 2021, 135 Stat. 2397.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

SUBMISSIONS TO CONGRESS

Pub. L. 117–81, div. F, title LXIV, §6401(c), Dec. 27, 2021, 135 Stat. 2398, provided that:

"(1) DEPARTMENT-WIDE EMPLOYEE ENGAGEMENT ACTION PLAN.—The Secretary of Homeland Security, acting through the Chief Human Capital Officer of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the Department-wide employee engagement action plan required under subsection (b)(1) of section 711 of the Homeland Security Act of 2002 [this section] (as added by subsection (a) of this section) not later than 30 days after the issuance of such plan under such subsection (b)(1).

"(2) COMPONENT-SPECIFIC EMPLOYEE ENGAGEMENT PLANS.—Each head of a component of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the component-specific employee engagement plan of each such component required under subsection (b)(2) of section 711 of the Homeland Security Act of 2002 [this section] not later than 30 days after the issuance of each such plan under such subsection (b)(2)."

§352. Annual employee award program

(a) In general

The Secretary may establish an annual employee award program to recognize Department

employees or groups of employees for significant contributions to the achievement of the Department's goals and missions. If such a program is established, the Secretary shall—

(1) establish within such program categories of awards, each with specific criteria, that emphasize honoring employees who are at the nonsupervisory level;

(2) publicize within the Department how any employee or group of employees may be nominated for an award;

(3) establish an internal review board comprised of representatives from Department components, headquarters, and field personnel to submit to the Secretary award recommendations regarding specific employees or groups of employees;

(4) select recipients from the pool of nominees submitted by the internal review board under paragraph (3) and convene a ceremony at which employees or groups of employees receive such awards from the Secretary; and

(5) publicize such program within the Department.

(b) Internal review board

The internal review board described in subsection (a)(3) shall, when carrying out its function under such subsection, consult with representatives from operational components and headquarters, including supervisory and nonsupervisory personnel, and employee labor organizations that represent Department employees.

(c) Rule of construction

Nothing in this section may be construed to authorize additional funds to carry out the requirements of this section or to require the Secretary to provide monetary bonuses to recipients of an award under this section.

(Pub. L. 107–296, title VII, §712, as added Pub. L. 117–81, div. F, title LXIV, §6402(a), Dec. 27, 2021, 135 Stat. 2398.)

§353. Acquisition professional career program

(a) Establishment

There is established in the Department an acquisition professional career program to develop a cadre of acquisition professionals within the Department.

(b) Administration

The Under Secretary for Management shall administer the acquisition professional career program established pursuant to subsection (a).

(c) Program requirements

The Under Secretary for Management shall carry out the following with respect to the acquisition professional career program.[1]

(1) Designate the occupational series, grades, and number of acquisition positions throughout the Department to be included in the program and manage centrally such positions.

(2) Establish and publish on the Department's website eligibility criteria for candidates to participate in the program.

(3) Carry out recruitment efforts to attract candidates—

(A) from institutions of higher education, including such institutions with established acquisition specialties and courses of study, historically Black colleges and universities, and Hispanic-serving institutions;

(B) with diverse work experience outside of the Federal Government; or

(C) with military service.

(4) Hire eligible candidates for designated positions under the program.

(5) Develop a structured program comprised of acquisition training, on-the-job experience,

Department-wide rotations, mentorship, shadowing, and other career development opportunities for program participants.

(6) Provide, beyond required training established for program participants, additional specialized acquisition training, including small business contracting and innovative acquisition techniques training.

(d) Reports

Not later than one year after December 27, 2021, and annually thereafter through 2027, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the acquisition professional career program. Each such report shall include the following information:

(1) The number of candidates approved for the program.

(2) The number of candidates who commenced participation in the program, including generalized information on such candidates' backgrounds with respect to education and prior work experience, but not including personally identifiable information.

(3) A breakdown of the number of participants hired under the program by type of acquisition position.

(4) A list of Department components and offices that participated in the program and information regarding length of time of each program participant in each rotation at such components or offices.

(5) Program attrition rates and post-program graduation retention data, including information on how such data compare to the prior year's data, as available.

(6) The Department's recruiting efforts for the program.

(7) The Department's efforts to promote retention of program participants.

(e) Definitions

In this section:

(1) Hispanic-serving institution

The term "Hispanic-serving institution" has the meaning given such term in section 1101a of title 20.

(2) Historically Black colleges and universities

The term "historically Black colleges and universities" has the meaning given the term "part B institution" in section 1061(2) of title 20.

(3) Institution of higher education

The term "institution of higher education" has the meaning given such term in section 1001 of title 20.

(Pub. L. 107–296, title VII, §713, as added Pub. L. 117–81, div. F, title LXIV, §6405(a), Dec. 27, 2021, 135 Stat. 2401.)

[1] *So in original. Probably should be a colon.*

SUBCHAPTER VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

PART A—COORDINATION WITH NON-FEDERAL ENTITIES

§361. Office for State and Local Government Coordination

(a) Establishment

There is established within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments.

(b) Responsibilities

The Office established under subsection (a) shall—

(1) coordinate the activities of the Department relating to State and local government;

(2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism;

(3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and

(4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

(Pub. L. 107–296, title VIII, §801, Nov. 25, 2002, 116 Stat. 2220.)

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13629. ESTABLISHING THE WHITE HOUSE HOMELAND SECURITY PARTNERSHIP COUNCIL

Ex. Ord. No. 13629, Oct. 26, 2012, 77 F.R. 66353, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to advance the Federal Government's use of local partnerships to address homeland security challenges, it is hereby ordered as follows:

SECTION 1. *Policy*. The purpose of this order is to maximize the Federal Government's ability to develop local partnerships in the United States to support homeland security priorities. Partnerships are collaborative working relationships in which the goals, structure, and roles and responsibilities of the relationships are mutually determined. Collaboration enables the Federal Government and its partners to use resources more efficiently, build on one another's expertise, drive innovation, engage in collective action, broaden investments to achieve shared goals, and improve performance. Partnerships enhance our ability to address homeland security priorities, from responding to natural disasters to preventing terrorism, by utilizing diverse perspectives, skills, tools, and resources.

The National Security Strategy emphasizes the importance of partnerships, underscoring that to keep our Nation safe "we must tap the ingenuity outside government through strategic partnerships with the private sector, nongovernmental organizations, foundations, and community-based organizations. Such partnerships are critical to U.S. success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing." This approach recognizes that, given the complexities and range of challenges, we must institutionalize an all-of-Nation effort to address the evolving threats to the United States.

SEC. 2. *White House Homeland Security Partnership Council and Steering Committee*.

(a) *White House Homeland Security Partnership Council*. There is established a White House Homeland Security Partnership Council (Council) to foster local partnerships—between the Federal Government and the private sector, nongovernmental organizations, foundations, community-based organizations, and State, local, tribal, and territorial government and law enforcement—to address homeland security challenges. The Council shall be chaired by the Assistant to the President for Homeland Security and Counterterrorism (Chair), or a designee from the National Security Staff.

(b) *Council Membership*.

(i) Pursuant to the nomination process established in subsection (b)(ii) of this section, the Council shall be composed of Federal officials who are from field offices of the executive departments, agencies, and bureaus (agencies) that are members of the Steering Committee established in subsection (c) of this section, and who have demonstrated an ability to develop, sustain, and institutionalize local partnerships to address policy priorities.

(ii) The nomination process and selection criteria for members of the Council shall be established by the

Steering Committee. Based on those criteria, agency heads may select and present to the Steering Committee their nominee or nominees to represent them on the Council. The Steering Committee shall consider all of the nominees and decide by consensus which of the nominees shall participate on the Council. Each member agency on the Steering Committee, with the exception of the Office of the Director of National Intelligence, may have at least one representative on the Council.

(c) *Steering Committee*. There is also established a Steering Committee, chaired by the Chair of the Council, to provide guidance to the Council and perform other functions as set forth in this order. The Steering Committee shall include a representative at the Deputy agency head level, or that representative's designee, from the following agencies:

(i) Department of State;
(ii) Department of the Treasury;
(iii) Department of Defense;
(iv) Department of Justice;
(v) Department of the Interior;
(vi) Department of Agriculture;
(vii) Department of Commerce;
(viii) Department of Labor;
(ix) Department of Health and Human Services;
(x) Department of Housing and Urban Development;
(xi) Department of Transportation;
(xii) Department of Energy;
(xiii) Department of Education;
(xiv) Department of Veterans Affairs;
(xv) Department of Homeland Security;
(xvi) Office of the Director of National Intelligence;
(xvii) Environmental Protection Agency;
(xviii) Small Business Administration; and
(xix) Federal Bureau of Investigation.

At the invitation of the Chair, representatives of agencies not listed in subsection (c) of this section or other executive branch entities may attend and participate in Steering Committee meetings as appropriate.

(d) *Administration*. The Chair or a designee shall convene meetings of the Council and Steering Committee, determine their agendas, and coordinate their work. The Council may establish subgroups consisting exclusively of Council members or their designees, as appropriate.

SEC. 3. *Mission and Function of the Council and Steering Committee*. (a) The Council shall, consistent with guidance from the Steering Committee:

(i) advise the Chair and Steering Committee members on priorities, challenges, and opportunities for local partnerships to support homeland security priorities, as well as regularly report to the Steering Committee on the Council's efforts;

(ii) promote homeland security priorities and opportunities for collaboration between Federal Government field offices and State, local, tribal, and territorial stakeholders;

(iii) advise and confer with State, local, tribal, and territorial stakeholders and agencies interested in expanding or building local homeland security partnerships;

(iv) raise awareness of local partnership best practices that can support homeland security priorities;

(v) as appropriate, conduct outreach to representatives of the private sector, nongovernmental organizations, foundations, community-based organizations, and State, local, tribal, and territorial government and law enforcement entities with relevant expertise for local homeland security partnerships, and collaborate with other Federal Government bodies; and

(vi) convene an annual meeting to exchange key findings, progress, and best practices.

(b) The Steering Committee shall:

(i) determine the scope of issue areas the Council will address and its operating protocols, in consultation with the Office of Management and Budget;

(ii) establish the nomination process and selection criteria for members of the Council as set forth in section 2(b)(ii) of this order;

(iii) provide guidance to the Council on the activities set forth in subsection (a) of this section; and

(iv) within 1 year of the selection of the Council members, and annually thereafter, provide a report on the work of the Council to the President through the Chair.

SEC. 4. *General Provisions*. (a) The heads of agencies participating in the Steering Committee shall assist and provide information to the Council, consistent with applicable law, as may be necessary to implement this

order. Each agency shall bear its own expense for participating in the Council.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof;

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals; or

(iii) the functions of the Overseas Security Advisory Council.

(c) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to the National Security Staff deemed to be a reference to the National Security Council Staff, see Ex. Ord. No. 13657, set out as a note under section 3021 of Title 50, War and National Defense.]

PART B—INSPECTOR GENERAL

§371. Repealed. Pub. L. 108–7, div. L, §104(c)(1), Feb. 20, 2003, 117 Stat. 531

Section, Pub. L. 107–296, title VIII, §811, Nov. 25, 2002, 116 Stat. 2221, related to authority of Secretary of Homeland Security with respect to Inspector General.

PART C—UNITED STATES SECRET SERVICE

§381. Functions transferred

In accordance with subchapter XII, there shall be transferred to the Secretary the functions, personnel, assets, and obligations of the United States Secret Service, which shall be maintained as a distinct entity within the Department, including the functions of the Secretary of the Treasury relating thereto.

(Pub. L. 107–296, title VIII, §821, Nov. 25, 2002, 116 Stat. 2224.)

§382. Use of proceeds derived from criminal investigations

(a) United States Secret Service use of proceeds derived from criminal investigations

During fiscal year 2014 and thereafter, with respect to any undercover investigative operation of the United States Secret Service (hereafter referred to in this section as the "Secret Service") that is necessary for the detection and prosecution of crimes against the United States—

(1) sums appropriated for the Secret Service, including unobligated balances available from prior fiscal years, may be used for purchasing property, buildings, and other facilities, and for leasing space, within the United States, the District of Columbia, and the territories and possessions of the United States, without regard to sections 1341 and 3324 of title 31, section 8141 of title 40, sections 6301(a), (b)(1) to (3) and 6306(a) of title 41, and section 3901 and chapter 45 of title 41;

(2) sums appropriated for the Secret Service, including unobligated balances available from prior fiscal years, may be used to establish or to acquire proprietary corporations or business entities as part of such undercover operation, and to operate such corporations or business entities

on a commercial basis, without regard to sections 9102 and 9103 of title 31;

(3) sums appropriated for the Secret Service, including unobligated balances available from prior fiscal years and the proceeds from such undercover operation, may be deposited in banks or other financial institutions, without regard to section 648 of title 18 and section 3302 of title 31; and

(4) proceeds from such undercover operation may be used to offset necessary and reasonable expenses incurred in such operation, without regard to section 3302 of title 31.

(b) Written certification

The authority set forth in subsection (a) may be exercised only upon the written certification of the Director of the Secret Service or designee that any action authorized by any paragraph of such subsection is necessary for the conduct of an undercover investigative operation. Such certification shall continue in effect for the duration of such operation, without regard to fiscal years.

(c) Deposit of proceeds in Treasury

As soon as practicable after the proceeds from an undercover investigative operation with respect to which an action is authorized and carried out under paragraphs (3) and (4) of subsection (a) are no longer necessary for the conduct of such operation, such proceeds or the balance of such proceeds remaining at the time shall be deposited in the Treasury of the United States as miscellaneous receipts.

(d) Reporting and deposit of proceeds upon disposition of certain business entities

If a corporation or business entity established or acquired as part of an undercover investigative operation under paragraph (2) of subsection (a) with a net value of over $50,000 is to be liquidated, sold, or otherwise disposed of, the Secret Service, as much in advance as the Director or designee determines is practicable, shall report the circumstance to the Secretary of Homeland Security. The proceeds of the liquidation, sale, or other disposition, after obligations are met, shall be deposited in the Treasury of the United States as miscellaneous receipts.

(e) Financial audits and reports

(1) The Secret Service shall conduct detailed financial audits of closed undercover investigative operations for which a written certification was made pursuant to subsection (b) on a quarterly basis and shall report the results of the audits in writing to the Secretary of Homeland Security.

(2) The Secretary of Homeland Security shall annually submit to the Committees on Appropriations of the Senate and House of Representatives, at the time that the President's budget is submitted under section 1105(a) of title 31, a summary of such audits.

(Pub. L. 109–295, title V, §532, Oct. 4, 2006, 120 Stat. 1384; Pub. L. 110–161, div. E, title V, §527, Dec. 26, 2007, 121 Stat. 2074; Pub. L. 110–329, div. D, title V, §520, Sept. 30, 2008, 122 Stat. 3684; Pub. L. 111–83, title V, §519, Oct. 28, 2009, 123 Stat. 2171; Pub. L. 112–10, div. B, title VI, §1652, Apr. 15, 2011, 125 Stat. 147; Pub. L. 112–74, div. D, title V, §518, Dec. 23, 2011, 125 Stat. 972; Pub. L. 113–6, div. D, title V, §518, Mar. 26, 2013, 127 Stat. 369; Pub. L. 113–76, div. F, title V, §518, Jan. 17, 2014, 128 Stat. 272.)

EDITORIAL NOTES

CODIFICATION

In subsec. (a)(1), "sections 6301(a), (b)(1) to (3) and 6306(a) of title 41," substituted for "sections 3732(a) and 3741 of the Revised Statutes of the United States (41 U.S.C. 11(a) and 22)," and "section 3901 and chapter 45 of title 41" substituted for "sections 304(a) and 305 of the Federal Property and Administrative Services Act of 1949 (41 U.S.C 254(a) and 255)" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

Section was enacted as part of the appropriation act cited in the credit to this section, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2014—Subsec. (a). Pub. L. 113–76 substituted "2014 and thereafter" for "2013" in introductory provisions.
2013—Subsec. (a). Pub. L. 113–6 substituted "2013" for "2012" in introductory provisions.
2011—Subsec. (a). Pub. L. 112–74 substituted "2012" for "2011" in introductory provisions.
Pub. L. 112–10 substituted "2011" for "2010" in introductory provisions.
2009—Subsec. (a). Pub. L. 111–83 substituted "2010" for "2009" in introductory provisions.
2008—Subsec. (a). Pub. L. 110–329 substituted "2009" for "2008" in introductory provisions.
2007—Subsec. (a). Pub. L. 110–161 substituted "2008" for "2007" in introductory provisions.

§383. National Computer Forensics Institute

(a) In general; mission

There is authorized for fiscal years 2023 through 2028 within the United States Secret Service a National Computer Forensics Institute (in this section referred to as the "Institute"). The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, and judges, as well as participants in the United States Secret Service's network of cyber fraud task forces who are Federal employees, members of the uniformed services, or State, local, Tribal, or territorial employees, regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections.

(b) Curriculum

In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections. Education and training provided pursuant to subsection (a) shall relate to the following:

(1) Investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, including relating to instances involving illicit use of digital assets and emerging trends in cybersecurity and electronic crime.

(2) Conducting forensic examinations of computers, mobile devices, and other information systems.

(3) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

(4) Methods to obtain, process, store, and admit digital evidence in court.

(c) Principles

In carrying out the functions specified in subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and information related to cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a). When selecting participants for such training, the Institute shall prioritize, to the extent reasonable and practicable, providing education and training to individuals from geographically-diverse jurisdictions throughout the United States, and the Institute shall prioritize, to the extent reasonable and practicable, State, local, tribal, and territorial law enforcement officers, prosecutors, judges, and other employees.

(d) Equipment

The Institute may provide recipients of education and training provided pursuant to subsection (a) with computer equipment, hardware, software, manuals, and tools for investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems.

(e) Cyber Fraud Task Forces

The Institute shall facilitate the expansion of the network of Cyber Fraud Task Forces of the United States Secret Service through the addition of recipients of education and training provided

pursuant to subsection (a) educated and trained by the Institute.

(f) Savings provision

All authorized activities and functions carried out by the Institute at any location as of the day before November 2, 2017, are authorized to continue to be carried out at any such location on and after such date.

(g) Expenses

The Director of the United States Secret Service may pay for all or a part of the education, training, or equipment provided by the Institute, including relating to the travel, transportation, and subsistence expenses of recipients of education and training provided pursuant to subsection (a).

(h) Annual reports to Congress

(1) In general

The Secretary shall include in the annual report required under section 1116 of title 31 information regarding the activities of the Institute, including, where possible, the following:

(A) An identification of jurisdictions with recipients of the education and training provided pursuant to subsection (a) during such year.

(B) Information relating to the costs associated with that education and training.

(C) Any information regarding projected future demand for the education and training provided pursuant to subsection (a).

(D) Impacts of the activities of the Institute on the capability of jurisdictions to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats.

(E) A description of the nomination process for potential recipients of the information and training provided pursuant to subsection (a).

(F) Any other issues determined relevant by the Secretary.

(2) Exception

Any information required under paragraph (1) that is submitted as part of the annual budget submitted by the President to Congress under section 1105 of title 31 is not required to be included in the report required under paragraph (1).

(i) Definitions

In this section:

(1) Cybersecurity threat

The term "cybersecurity threat" has the meaning given such term in section 1501 of this title.

(2) Incident

The term "incident" has the meaning given such term in section 659(a) [1] of this title.

(3) Information system

The term "information system" has the meaning given such term in section 1501(9) of this title.

(Pub. L. 107–296, title VIII, §822, as added Pub. L. 115–76, §2(a), Nov. 2, 2017, 131 Stat. 1246; amended Pub. L. 117–263, div. G, title LXXI, §7123, Dec. 23, 2022, 136 Stat. 3641.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 659(a) of this title, referred to in subsec. (i)(2), was amended by Pub. L. 117–263, §7143(b)(2)(D)(i), and no longer defines the term "incident". Reference to term "incident" as defined in this chapter deemed to be a reference to that term as defined in section 650(12) of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7123(1), substituted, in heading, "In general; mission" for "In

general", in first sentence, "2023 through 2028" for "2017 through 2022", and, in second sentence, "The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, and judges, as well as participants in the United States Secret Service's network of cyber fraud task forces who are Federal employees, members of the uniformed services, or State, local, Tribal, or territorial employees, regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections." for "The Institute shall disseminate information related to the investigation and prevention of cyber and electronic crime and related threats, and educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges."

Subsec. (b). Pub. L. 117–263, §7123(2), amended subsec. (b) generally. Prior to amendment, subsec. (b) related to the functions of the Institute.

Subsec. (c). Pub. L. 117–263, §7123(3), substituted "cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)" for "cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors" and inserted at end "When selecting participants for such training, the Institute shall prioritize, to the extent reasonable and practicable, providing education and training to individuals from geographically-diverse jurisdictions throughout the United States, and the Institute shall prioritize, to the extent reasonable and practicable, State, local, tribal, and territorial law enforcement officers, prosecutors, judges, and other employees."

Subsec. (d). Pub. L. 117–263, §7123(4), substituted "recipients of education and training provided pursuant to subsection (a)" for "State, local, tribal, and territorial law enforcement officers" and "for investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems" for "necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations".

Subsec. (e). Pub. L. 117–263, §7123(5), in heading, substituted "Cyber Fraud Task Forces" for "Electronic Crime Task Forces" and, in text, substituted "Cyber Fraud" for "Electronic Crime", "recipients of education and training provided pursuant to subsection (a)" for "State, local, tribal, and territorial law enforcement officers", and "by" for "at".

Subsecs. (g) to (i). Pub. L. 117–263, §7123(6), added subsecs. (g) to (i).

[1] *See References in Text note below.*

PART D—ACQUISITIONS

§391. Research and development projects

(a) Authority

Until September 30, 2024, and subject to subsection (d),[1] the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) In general

When the Secretary carries out basic, applied, and advanced research and development projects, including the expenditure of funds for such projects, the Secretary may exercise the same authority (subject to the same limitations and conditions) with respect to such research and projects as the Secretary of Defense may exercise under section 4021 of title 10 (except for subsections (b) and (f)), after making a determination that the use of a contract, grant, or cooperative agreement for such project is not feasible or appropriate. The annual report required under subsection (b) [1] of this section, as applied to the Secretary by this paragraph, shall be submitted to the President of the Senate and the Speaker of the House of Representatives.

(2) Prototype projects

The Secretary—

(A) may, under the authority of paragraph (1), carry out prototype projects under section 4022 of title 10; and

(B) in applying the authorities of such section 4022, the Secretary shall perform the functions of the Secretary of Defense as prescribed in such section.

(b) Procurement of temporary and intermittent services

The Secretary may—

(1) procure the temporary or intermittent services of experts or consultants (or organizations thereof) in accordance with section 3109(b) of title 5; and

(2) whenever necessary due to an urgent homeland security need, procure temporary (not to exceed 1 year) or intermittent personal services, including the services of experts or consultants (or organizations thereof), without regard to the pay limitations of such section 3109.

(c) Additional requirements

(1) In general

The authority of the Secretary under this section shall terminate September 30, 2024, unless before that date the Secretary—

(A) issues policy guidance detailing the appropriate use of that authority; and

(B) provides training to each employee that is authorized to exercise that authority.

(2) Report

The Secretary shall provide an annual report to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives detailing the projects for which the authority granted by subsection (a) was used, the rationale for its use, the funds spent using that authority, the outcome of each project for which that authority was used, and the results of any audits of such projects.

(d) Definition of nontraditional Government contractor

In this section, the term "nontraditional Government contractor" has the same meaning as the term "nontraditional defense contractor" as defined in section 4022(e) of title 10.

(Pub. L. 107–296, title VIII, §831, Nov. 25, 2002, 116 Stat. 2224; Pub. L. 110–161, div. E, title V, §572, Dec. 26, 2007, 121 Stat. 2093; Pub. L. 110–329, div. D, title V, §537, Sept. 30, 2008, 122 Stat. 3687; Pub. L. 111–83, title V, §531, Oct. 28, 2009, 123 Stat. 2174; Pub. L. 112–10, div. B, title VI, §1651, Apr. 15, 2011, 125 Stat. 146; Pub. L. 112–74, div. D, title V, §527, Dec. 23, 2011, 125 Stat. 974; Pub. L. 113–6, div. D, title V, §525, Mar. 26, 2013, 127 Stat. 371; Pub. L. 113–76, div. F, title V, §525, Jan. 17, 2014, 128 Stat. 273; Pub. L. 114–4, title V, §523, Mar. 4, 2015, 129 Stat. 65; Pub. L. 114–113, div. F, title V, §523, Dec. 18, 2015, 129 Stat. 2516; Pub. L. 115–31, div. F, title V, §514, May 5, 2017, 131 Stat. 427; Pub. L. 117–81, div. A, title XVII, §1702(c)(1), Dec. 27, 2021, 135 Stat. 2155; Pub. L. 117–263, div. G, title LXXII, §7227(b), Dec. 23, 2022, 136 Stat. 3675.)

EDITORIAL NOTES

REFERENCES IN TEXT

Subsection (d), referred to in subsec. (a), was redesignated subsec. (c) of this section by Pub. L. 112–74, div. D, title V, §527(3), Dec. 23, 2011, 125 Stat. 974.

Subsection (b) of this section, referred to in subsec. (a)(1), probably means the former subsec. (b) of this section which related to annual reports by the Comptroller General and which was struck out by Pub. L. 112–74, div. D, title V, §527(2), Dec. 23, 2011, 125 Stat. 974. See 2011 Amendment note for subsec. (b) below.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7227(b)(1)(A), substituted "September 30, 2024" for "September 30, 2017" in introductory provisions.

Subsec. (a)(2). Pub. L. 117–263, §7227(b)(1)(B), amended par. (2) generally. Prior to amendment, text read

as follows: "The Secretary may, under the authority of paragraph (1), carry out prototype projects in accordance with the requirements and conditions provided for carrying out prototype projects under section 845 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160). In applying the authorities of that section 845, subsection (c) of that section shall apply with respect to prototype projects under this paragraph, and the Secretary shall perform the functions of the Secretary of Defense under subsection (d) thereof."

Subsec. (c)(1). Pub. L. 117–263, §7227(b)(2), substituted "September 30, 2024" for "September 30, 2017" in introductory provisions.

Subsec. (d). Pub. L. 117–263, §7227(b)(3), substituted "section 4022(e) of title 10." for "section 845(e) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160; 10 U.S.C. 2371 note)."

2021—Subsec. (a)(1). Pub. L. 117–81 substituted "section 4021" for "section 2371".

2017—Subsec. (a). Pub. L. 115–31, §514(1), substituted "Until September 30, 2017," for "Until September 30, 2016," in introductory provisions.

Subsec. (c)(1). Pub. L. 115–31, §514(2), substituted "September 30, 2017," for "September 30, 2016," in introductory provisions.

2015—Subsec. (a). Pub. L. 114–113, §523(1), substituted "Until September 30, 2016," for "Until September 30, 2015," in introductory provisions.

Pub. L. 114–4, §523(1), substituted "Until September 30, 2015," for "Until September 30, 2014," in introductory provisions.

Subsec. (c)(1). Pub. L. 114–113, §523(2), substituted "September 30, 2016," for "September 30, 2015," in introductory provisions.

Pub. L. 114–4, §523(2), substituted "September 30, 2015," for "September 30, 2014," in introductory provisions.

2014—Subsec. (a). Pub. L. 113–76, §525(1), substituted "Until September 30, 2014," for "Until September 30, 2013," in introductory provisions.

Subsec. (c)(1). Pub. L. 113–76, §525(2), substituted "September 30, 2014," for "September 30, 2013," in introductory provisions.

2013—Subsec. (a). Pub. L. 113–6, §525(1), substituted "Until September 30, 2013," for "Until September 30, 2012," in introductory provisions.

Subsec. (c)(1). Pub. L. 113–6, §525(2), substituted "September 30, 2013," for "September 30, 2012," in introductory provisions.

2011—Subsec. (a). Pub. L. 112–74, §527(1), substituted "Until September 30, 2012," for "Until September 30, 2011" in introductory provisions.

Pub. L. 112–10, §1651(1), substituted "Until September 30, 2011" for "Until September 30, 2010" in introductory provisions.

Subsec. (b). Pub. L. 112–74, §527(2), (3), redesignated subsec. (c) as (b) and struck out former subsec. (b). Text read as follows: "Not later than 2 years after the effective date of this chapter, and annually thereafter, the Comptroller General shall report to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate on—

"(1) whether use of the authorities described in subsection (a) of this section attracts nontraditional Government contractors and results in the acquisition of needed technologies; and

"(2) if such authorities were to be made permanent, whether additional safeguards are needed with respect to the use of such authorities.".

Subsec. (c). Pub. L. 112–74, §527(3), redesignated subsec. (d) as (c). Former subsec. (c) redesignated (b).

Subsec. (c)(1). Pub. L. 112–74, §527(4), substituted "September 30, 2012," for "September 30, 2011" in introductory provisions.

Subsec. (d). Pub. L. 112–74, §527(3), redesignated subsec. (e) as (d). Former subsec. (d) redesignated (c).

Subsec. (d)(1). Pub. L. 112–10, §1651(2), substituted "September 30, 2011" for "September 30, 2010" in introductory provisions.

2009—Subsec. (a). Pub. L. 111–83, §531(1), substituted "September 30, 2010," for "September 30, 2009" in introductory provisions.

Subsec. (d)(1). Pub. L. 111–83, §531(2), substituted "September 30, 2010," for "September 30, 2009," in introductory provisions.

2008—Subsec. (a). Pub. L. 110–329, §537(1), substituted "Until September 30, 2009 and subject to subsection (d)," for "Until September 30, 2008," in introductory provisions.

Subsecs. (d), (e). Pub. L. 110–329, §537(2), (3), added subsec. (d) and redesignated former subsec. (d) as (e).

2007—Subsec. (a). Pub. L. 110–161 substituted "Until September 30, 2008" for "During the 5-year period

following the effective date of this chapter" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EXTENSION OF SECRETARY'S AUTHORITY

Prior to amendment by section 7227(b)(1)(A), (2) of Pub. L. 117–263, extensions of the Secretary's authority in subsecs. (a) and (c)(1) of this section were provided as follows:

Pub. L. 117–103, div. F, title V, §529(a), Mar. 15, 2022, 136 Stat. 340, provided that subsecs. (a) and (c)(1) of this section would be applied by substituting Sept. 30, 2022, for Sept. 30, 2017.

Pub. L. 116–260, div. F, title V, §531(a), Dec. 27, 2020, 134 Stat. 1473, provided that subsecs. (a) and (c)(1) of this section would be applied by substituting Sept. 30, 2021, for Sept. 30, 2017.

Pub. L. 116–93, div. D, title V, §531(a), Dec. 20, 2019, 133 Stat. 2530, provided that subsecs. (a) and (c)(1) of this section would be applied by substituting Sept. 30, 2020, for Sept. 30, 2017.

Pub. L. 116–6, div. A, title V, §541(a), as added by Pub. L. 116–26, title III, §302, July 1, 2019, 133 Stat. 1021, provided that subsecs. (a) and (c)(1) of this section would be applied by substituting Sept. 30, 2019, for Sept. 30, 2017.

Pub. L. 115–141, div. F, title V, §538(a), Mar. 23, 2018, 132 Stat. 632, provided that subsecs. (a) and (c)(1) of this section would be applied by substituting Sept. 30, 2018, for Sept. 30, 2017.

DOCUMENTATION REQUIREMENTS FOR MAJOR ACQUISITION PROGRAMS

Pub. L. 114–113, div. F, title V, §561, Dec. 18, 2015, 129 Stat. 2521, provided that:

"(a) Each major acquisition program of the Department of Homeland Security, as defined in Department of Homeland Security Management Directive 102–2, shall meet established acquisition documentation requirements for its acquisition program baseline established in the Department of Homeland Security Instruction Manual 102–01–001 and the Department of Homeland Security Acquisition Instruction/Guidebook 102–01–001, Appendix K.

"(b) The Department shall report to the Committees on Appropriations of the Senate and the House of Representatives in the Comprehensive Acquisition Status Report and its quarterly updates, required under the heading 'Office of the Under Secretary for Management' of this Act [div. F of Pub. L. 114–113, 129 Stat. 2493], on any major acquisition program that does not meet such documentation requirements and the schedule by which the program will come into compliance with these requirements.

"(c) None of the funds made available by this or any other Act for any fiscal year may be used for a major acquisition program that is out of compliance with such documentation requirements for more than two years except that funds may be used solely to come into compliance with such documentation requirements or to terminate the program."

[1] *See References in Text note below.*

§392. Personal services

The Secretary—

(1) may procure the temporary or intermittent services of experts or consultants (or organizations thereof) in accordance with section 3109 of title 5; and

(2) may, whenever necessary due to an urgent homeland security need, procure temporary (not to exceed 1 year) or intermittent personal services, including the services of experts or consultants (or organizations thereof), without regard to the pay limitations of such section 3109.

(Pub. L. 107–296, title VIII, §832, Nov. 25, 2002, 116 Stat. 2225.)

§393. Special streamlined acquisition authority

(a) Authority

(1) In general

The Secretary may use the authorities set forth in this section with respect to any procurement

made during the period beginning on the effective date of this chapter and ending September 30, 2007, if the Secretary determines in writing that the mission of the Department (as described in section 111 of this title) would be seriously impaired without the use of such authorities.

(2) Delegation

The authority to make the determination described in paragraph (1) may not be delegated by the Secretary to an officer of the Department who is not appointed by the President with the advice and consent of the Senate.

(3) Notification

Not later than the date that is 7 days after the date of any determination under paragraph (1), the Secretary shall submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate—

(A) notification of such determination; and

(B) the justification for such determination.

(b) Increased micro-purchase threshold for certain procurements

(1) In general

The Secretary may designate certain employees of the Department to make procurements described in subsection (a) for which in the administration of section 1902 of title 41 the amount specified in subsections (a), (d), and (e) of such section 1902 shall be deemed to be $7,500.

(2) Number of employees

The number of employees designated under paragraph (1) shall be—

(A) fewer than the number of employees of the Department who are authorized to make purchases without obtaining competitive quotations, pursuant to section 1902(d) of title 41;

(B) sufficient to ensure the geographic dispersal of the availability of the use of the procurement authority under such paragraph at locations reasonably considered to be potential terrorist targets; and

(C) sufficiently limited to allow for the careful monitoring of employees designated under such paragraph.

(3) Review

Procurements made under the authority of this subsection shall be subject to review by a designated supervisor on not less than a monthly basis. The supervisor responsible for the review shall be responsible for no more than 7 employees making procurements under this subsection.

(c) Simplified acquisition procedures

(1) In general

With respect to a procurement described in subsection (a), the Secretary may deem the simplified acquisition threshold referred to in section 134 of title 41 to be—

(A) in the case of a contract to be awarded and performed, or purchase to be made, within the United States, $200,000; and

(B) in the case of a contract to be awarded and performed, or purchase to be made, outside of the United States, $300,000.

(2) Omitted

(d) Application of certain commercial items authorities

(1) In general

With respect to a procurement described in subsection (a), the Secretary may deem any item or service to be a commercial item for the purpose of Federal procurement laws.

(2) Limitation

The $5,000,000 limitation provided in section 1901(a)(2) of title 41 and section 3305(a)(2) of title 41 shall be deemed to be $7,500,000 for purposes of property or services under the authority

of this subsection.

(3) Certain authority

Authority under a provision of law referred to in paragraph (2) that expires under section 4202(e) of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106; 10 U.S.C. 2304 note) shall, notwithstanding such section, continue to apply for a procurement described in subsection (a).

(e) Report

Not later than 180 days after the end of fiscal year 2005, the Comptroller General shall submit to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives a report on the use of the authorities provided in this section. The report shall contain the following:

(1) An assessment of the extent to which property and services acquired using authorities provided under this section contributed to the capacity of the Federal workforce to facilitate the mission of the Department as described in section 111 of this title.

(2) An assessment of the extent to which prices for property and services acquired using authorities provided under this section reflected the best value.

(3) The number of employees designated by each executive agency under subsection (b)(1).

(4) An assessment of the extent to which the Department has implemented subsections (b)(2) and (b)(3) to monitor the use of procurement authority by employees designated under subsection (b)(1).

(5) Any recommendations of the Comptroller General for improving the effectiveness of the implementation of the provisions of this section.

(Pub. L. 107–296, title VIII, §833, Nov. 25, 2002, 116 Stat. 2225.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsec. (a)(1), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

Section 4202(e) of the Clinger-Cohen Act of 1996, referred to in subsec. (d)(3), is section 4202(e) of Pub. L. 104–106, which is set out as a note under section 2304 of Title 10, Armed Forces.

CODIFICATION

In subsec. (b)(1), "section 1902 of title 41" substituted for "section 32 of the Office of Federal Procurement Policy Act (41 U.S.C. 428)" and "subsections (a), (d), and (e) of such section 1902" substituted for "subsections (c), (d), and (f) of such section 32" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

In subsec. (b)(2)(A), "section 1902(d) of title 41" substituted for "section 32(c) of the Office of Federal Procurement Policy Act (41 U.S.C. 428(c))" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

In subsec. (c)(1), "section 134 of title 41" substituted for "section 4(11) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(11))" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

In subsec. (d)(2), "section 1901(a)(2) of title 41" substituted for "section 31(a)(2) of the Office of Federal Procurement Policy Act (41 U.S.C. 427(a)(2))" and "section 3305(a)(2) of title 41" substituted for "section 303(g)(1)(B) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(g)(1)(B))" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

Section is comprised of section 833 of Pub. L. 107–296. Subsec. (c)(2) of section 833 of Pub. L. 107–296 amended section 416 of former Title 41, Public Contracts.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§394. Unsolicited proposals

(a) Regulations required

Within 1 year of November 25, 2002, the Federal Acquisition Regulation shall be revised to include regulations with regard to unsolicited proposals.

(b) Content of regulations

The regulations prescribed under subsection (a) shall require that before initiating a comprehensive evaluation, an agency contact point shall consider, among other factors, that the proposal—

(1) is not submitted in response to a previously published agency requirement; and

(2) contains technical and cost information for evaluation and overall scientific, technical or socioeconomic merit, or cost-related or price-related factors.

(Pub. L. 107–296, title VIII, §834, Nov. 25, 2002, 116 Stat. 2227.)

§395. Prohibition on contracts with corporate expatriates

(a) In general

The Secretary may not enter into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation under subsection (b), or any subsidiary of such an entity.

(b) Inverted domestic corporation

For purposes of this section, a foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) the entity completes before, on, or after November 25, 2002, the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) after the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(A) in the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(B) in the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) the expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

(c) Definitions and special rules

(1) Rules for application of subsection (b)

In applying subsection (b) for purposes of subsection (a), the following rules shall apply:

(A) Certain stock disregarded

There shall not be taken into account in determining ownership for purposes of subsection (b)(2)—

(i) stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(1).

(B) Plan deemed in certain cases

If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(C) Certain transfers disregarded

The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(D) Special rule for related partnerships

For purposes of applying subsection (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of title 26) shall be treated as I [1] partnership.

(E) Treatment of certain rights

The Secretary shall prescribe such regulations as may be necessary to—

(i) treat warrants, options, contracts to acquire stock, convertible debt instruments, and other similar interests as stock; and

(ii) treat stock as not stock.

(2) Expanded affiliated group

The term "expanded affiliated group" means an affiliated group as defined in section 1504(a) of title 26 (without regard to section 1504(b) of such title), except that section 1504 of such title shall be applied by substituting "more than 50 percent" for "at least 80 percent" each place it appears.

(3) Foreign incorporated entity

The term "foreign incorporated entity" means any entity which is, or but for subsection (b) would be, treated as a foreign corporation for purposes of title 26.

(4) Other definitions

The terms "person", "domestic", and "foreign" have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of title 26, respectively.

(d) Waivers

The Secretary shall waive subsection (a) with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(Pub. L. 107–296, title VIII, §835, Nov. 25, 2002, 116 Stat. 2227; Pub. L. 108–7, div. L, §101(2), Feb. 20, 2003, 117 Stat. 528; Pub. L. 108–334, title V, §523, Oct. 18, 2004, 118 Stat. 1320.)

EDITORIAL NOTES

AMENDMENTS

2004—Subsec. (a). Pub. L. 108–334, §523(1), inserted before period at end ", or any subsidiary of such an entity".

Subsec. (b)(1). Pub. L. 108–334, §523(2), inserted "before, on, or" after "completes".

Subsec. (c)(1)(B). Pub. L. 108–334, §523(3), struck out "which is after November 25, 2002, and" after "beginning on the date".

Subsec. (d). Pub. L. 108–334, §523(4), substituted "national" for "homeland".

2003—Subsec. (d). Pub. L. 108–7 struck out ", or to prevent the loss of any jobs in the United States or prevent the Government from incurring any additional costs that otherwise would not occur" before period at end.

[1] *So in original.*

§396. Lead system integrator; financial interests

(a) In general

With respect to contracts entered into after July 1, 2007, and except as provided in subsection (b), no entity performing lead system integrator functions in the acquisition of a major system by the Department of Homeland Security may have any direct financial interest in the development or construction of any individual system or element of any system of systems.

(b) Exception

An entity described in subsection (a) may have a direct financial interest in the development or construction of an individual system or element of a system of systems if—

(1) the Secretary of Homeland Security certifies to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Transportation and Infrastructure of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science and Transportation of the Senate that—

(A) the entity was selected by the Department of Homeland Security as a contractor to develop or construct the system or element concerned through the use of competitive procedures; and

(B) the Department took appropriate steps to prevent any organizational conflict of interest in the selection process; or

(2) the entity was selected by a subcontractor to serve as a lower-tier subcontractor, through a process over which the entity exercised no control.

(c) Construction

Nothing in this section shall be construed to preclude an entity described in subsection (a) from performing work necessary to integrate two or more individual systems or elements of a system of systems with each other.

(d) Regulations update

Not later than July 1, 2007, the Secretary of Homeland Security shall update the acquisition regulations of the Department of Homeland Security in order to specify fully in such regulations the matters with respect to lead system integrators set forth in this section. Included in such regulations shall be: (1) a precise and comprehensive definition of the term "lead system integrator", modeled after that used by the Department of Defense; and (2) a specification of various types of contracts and fee structures that are appropriate for use by lead system integrators in the production, fielding, and sustainment of complex systems.

(Pub. L. 110–28, title VI, §6405, May 25, 2007, 121 Stat. 176.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§397. Requirements to buy certain items related to national security interests

(a) Definitions

In this section:

(1) Covered item

The term "covered item" means any of the following:

(A) Footwear provided as part of a uniform.

(B) Uniforms.

(C) Holsters and tactical pouches.

(D) Patches, insignia, and embellishments.

(E) Chemical, biological, radiological, and nuclear protective gear.

(F) Body armor components intended to provide ballistic protection for an individual, consisting of 1 or more of the following:

(i) Soft ballistic panels.

(ii) Hard ballistic plates.

(iii) Concealed armor carriers worn under a uniform.

(iv) External armor carriers worn over a uniform.

(G) Any other item of clothing or protective equipment as determined appropriate by the Secretary.

(2) Frontline operational component

The term "frontline operational component" means any of the following entities of the Department:

(A) U.S. Customs and Border Protection.

(B) U.S. Immigration and Customs Enforcement.

(C) The United States Secret Service.

(D) The Transportation Security Administration.

(E) The Federal Protective Service.

(F) The Federal Emergency Management Agency.

(G) The Federal Law Enforcement Training Centers.

(H) The Cybersecurity and Infrastructure Security Agency.

(b) Requirements

(1) In general

The Secretary shall ensure that any procurement of a covered item for a frontline operational component meets the following criteria:

(A)(i) To the maximum extent possible, not less than one-third of funds obligated in a specific fiscal year for the procurement of such covered items shall be covered items that are manufactured or supplied in the United States by entities that qualify as small business concerns, as such term is described under section 632 of title 15.

(ii) Covered items may only be supplied pursuant to subparagraph (A) to the extent that United States entities that qualify as small business concerns—

(I) are unable to manufacture covered items in the United States; and

(II) meet the criteria identified in subparagraph (B).

(B) Each contractor with respect to the procurement of such a covered item, including the

end-item manufacturer of such a covered item—

(i) is an entity registered with the System for Award Management (or successor system) administered by the General Services Administration; and

(ii) is in compliance with ISO 9001:2015 of the International Organization for Standardization (or successor standard) or a standard determined appropriate by the Secretary to ensure the quality of products and adherence to applicable statutory and regulatory requirements.

(C) Each supplier of such a covered item with an insignia (such as any patch, badge, or emblem) and each supplier of such an insignia, if such covered item with such insignia or such insignia, as the case may be, is not produced, applied, or assembled in the United States, shall—

(i) store such covered item with such insignia or such insignia in a locked area;

(ii) report any pilferage or theft of such covered item with such insignia or such insignia occurring at any stage before delivery of such covered item with such insignia or such insignia; and

(iii) destroy any such defective or unusable covered item with insignia or insignia in a manner established by the Secretary, and maintain records, for three years after the creation of such records, of such destruction that include the date of such destruction, a description of the covered item with insignia or insignia destroyed, the quantity of the covered item with insignia or insignia destroyed, and the method of destruction.

(2) Waiver

(A) In general

In the case of a national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.) or a major disaster declared by the President under section 5170 of title 42, the Secretary may waive a requirement in subparagraph (A), (B) or (C) of paragraph (1) if the Secretary determines there is an insufficient supply of a covered item that meets such requirement.

(B) Notice

Not later than 60 days after the date on which the Secretary determines a waiver under subparagraph (A) is necessary, the Secretary shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives notice of such determination, which shall include the following:

(i) Identification of the national emergency or major disaster declared by the President.

(ii) Identification of the covered item for which the Secretary intends to issue the waiver.

(iii) A description of the demand for the covered item and corresponding lack of supply from contractors able to meet the criteria described in subparagraph (B) or (C) of paragraph (1).

(c) Pricing

The Secretary shall ensure that covered items are purchased at a fair and reasonable price, consistent with the procedures and guidelines specified in the Federal Acquisition Regulation.

(d) Report

Not later than one year after December 23, 2022, and annually thereafter, the Secretary shall provide to the Committee on Homeland Security, the Committee on Oversight and Reform, the Committee on Small Business, and the Committee on Appropriations of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs, the Committee on Small Business and Entrepreneurship, and the Committee on Appropriations of the Senate a briefing on instances in which vendors have failed to meet deadlines for delivery of covered items and corrective actions taken by the Department in response to such instances.

(e) Effective date

This section applies with respect to a contract entered into by the Department or any frontline operational component on or after the date that is 180 days after December 23, 2022.

(Pub. L. 107–296, title VIII, §836, as added Pub. L. 117–263, div. G, title LXXI, §7112(a), Dec. 23, 2022, 136 Stat. 3628.)

EDITORIAL NOTES

REFERENCES IN TEXT

The National Emergencies Act, referred to in subsec. (b)(2)(A), is Pub. L. 94–412, Sept. 14, 1976, 90 Stat. 1255, which is classified principally to chapter 34 (§1601 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of Title 50 and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

PART E—HUMAN RESOURCES MANAGEMENT

§411. Establishment of human resources management system

(a) Authority

(1) Sense of Congress

It is the sense of Congress that—

(A) it is extremely important that employees of the Department be allowed to participate in a meaningful way in the creation of any human resources management system affecting them;

(B) such employees have the most direct knowledge of the demands of their jobs and have a direct interest in ensuring that their human resources management system is conducive to achieving optimal operational efficiencies;

(C) the 21st century human resources management system envisioned for the Department should be one that benefits from the input of its employees; and

(D) this collaborative effort will help secure our homeland.

(2), (3) Omitted

(b) Effect on personnel

(1) Nonseparation or nonreduction in grade or compensation of full-time personnel and part-time personnel holding permanent positions

Except as otherwise provided in this chapter, the transfer under this chapter of full-time personnel (except special Government employees) and part-time personnel holding permanent positions shall not cause any such employee to be separated or reduced in grade or compensation for 1 year after the date of transfer to the Department.

(2) Positions compensated in accordance with Executive Schedule

Any person who, on the day preceding such person's date of transfer pursuant to this chapter,

held a position compensated in accordance with the Executive Schedule prescribed in chapter 53 of title 5 and who, without a break in service, is appointed in the Department to a position having duties comparable to the duties performed immediately preceding such appointment shall continue to be compensated in such new position at not less than the rate provided for such position, for the duration of the service of such person in such new position.

(3) Coordination rule

Any exercise of authority under chapter 97 of title 5, including under any system established under such chapter, shall be in conformance with the requirements of this subsection.

(Pub. L. 107–296, title VIII, §841, Nov. 25, 2002, 116 Stat. 2229.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (b)(1), (2), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

Section is comprised of section 841 of Pub. L. 107–296. Subsec. (a)(2), (3) of section 841 of Pub. L. 107–296 enacted chapter 97 (§9701) of Title 5, Government Organization and Employees.

STATUTORY NOTES AND RELATED SUBSIDIARIES

INDEPENDENT INVESTIGATION AND IMPLEMENTATION PLAN

Pub. L. 117–81, div. F, title LXIV, §6404, Dec. 27, 2021, 135 Stat. 2400, provided that:

"(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Dec. 27, 2021], the Comptroller General of the United States shall investigate whether the application in the Department of Homeland Security of discipline and adverse actions for managers and non-managers are administered in an equitable and consistent manner that results in the same or substantially similar disciplinary outcomes across the Department that are appropriately calibrated to address the identified misconduct, taking into account relevant aggravating and mitigating factors.

"(b) CONSULTATION.—In carrying out the investigation described in subsection (a), the Comptroller General of the United States shall consult with the Under Secretary for Management of the Department of Homeland Security and the employee engagement steering committee established pursuant to subsection (b)(1) of section 711 of the Homeland Security Act of 2002 [6 U.S.C. 351(b)(1)] (as added by section 6401(a) of this Act).

"(c) ACTION BY UNDER SECRETARY FOR MANAGEMENT.—Upon completion of the investigation described in subsection (a), the Under Secretary for Management of the Department of Homeland Security shall review the findings and recommendations of such investigation and implement a plan, in consultation with the employee engagement steering committee established pursuant to subsection (b)(1) of section 711 of the Homeland Security Act of 2002, to correct any relevant deficiencies identified by the Comptroller General of the United States in such investigation. The Under Secretary for Management shall direct the employee engagement steering committee to review such plan to inform committee activities and action plans authorized under such section 711 [6 U.S.C. 351]."

§412. Labor-management relations

(a) Limitation on exclusionary authority

(1) In general

No agency or subdivision of an agency which is transferred to the Department pursuant to this chapter shall be excluded from the coverage of chapter 71 of title 5 as a result of any order issued under section 7103(b)(1) of such title 5 after June 18, 2002, unless—

(A) the mission and responsibilities of the agency (or subdivision) materially change; and

(B) a majority of the employees within such agency (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) Exclusions allowable

Nothing in paragraph (1) shall affect the effectiveness of any order to the extent that such order excludes any portion of an agency or subdivision of an agency as to which—

(A) recognition as an appropriate unit has never been conferred for purposes of chapter 71 of such title 5; or

(B) any such recognition has been revoked or otherwise terminated as a result of a determination under subsection (b)(1).

(b) Provisions relating to bargaining units

(1) Limitation relating to appropriate units

Each unit which is recognized as an appropriate unit for purposes of chapter 71 of title 5 as of the day before the effective date of this chapter (and any subdivision of any such unit) shall, if such unit (or subdivision) is transferred to the Department pursuant to this chapter, continue to be so recognized for such purposes, unless—

(A) the mission and responsibilities of such unit (or subdivision) materially change; and

(B) a majority of the employees within such unit (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

(2) Limitation relating to positions or employees

No position or employee within a unit (or subdivision of a unit) as to which continued recognition is given in accordance with paragraph (1) shall be excluded from such unit (or subdivision), for purposes of chapter 71 of such title 5, unless the primary job duty of such position or employee—

(A) materially changes; and

(B) consists of intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

In the case of any positions within a unit (or subdivision) which are first established on or after the effective date of this chapter and any employees first appointed on or after such date, the preceding sentence shall be applied disregarding subparagraph (A).

(c) Waiver

If the President determines that the application of subsections (a), (b), and (d) would have a substantial adverse impact on the ability of the Department to protect homeland security, the President may waive the application of such subsections 10 days after the President has submitted to Congress a written explanation of the reasons for such determination.

(d) Coordination rule

No other provision of this chapter or of any amendment made by this chapter may be construed or applied in a manner so as to limit, supersede, or otherwise affect the provisions of this section, except to the extent that it does so by specific reference to this section.

(e) Rule of construction

Nothing in section 9701(e) of title 5 shall be considered to apply with respect to any agency or subdivision of any agency, which is excluded from the coverage of chapter 71 of title 5 by virtue of an order issued in accordance with section 7103(b) of such title 5 and the preceding provisions of this section (as applicable), or to any employees of any such agency or subdivision or to any individual or entity representing any such employees or any representatives thereof.

(Pub. L. 107–296, title VIII, §842, Nov. 25, 2002, 116 Stat. 2234.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsecs. (a)(1), (b)(1), and (d), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The effective date of this chapter, referred to in subsec. (b), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

§413. Use of counternarcotics enforcement activities in certain employee performance appraisals

(a) In general

Each subdivision of the Department that is a National Drug Control Program Agency shall include as one of the criteria in its performance appraisal system, for each employee directly or indirectly involved in the enforcement of Federal, State, or local narcotics laws, the performance of that employee with respect to the enforcement of Federal, State, or local narcotics laws, relying to the greatest extent practicable on objective performance measures, including—

(1) the contribution of that employee to seizures of narcotics and arrests of violators of Federal, State, or local narcotics laws; and

(2) the degree to which that employee cooperated with or contributed to the efforts of other employees, either within the Department or other Federal, State, or local agencies, in counternarcotics enforcement.

(b) Definitions

For purposes of this section—

(1) the term "National Drug Control Program Agency" means—

(A) a National Drug Control Program Agency [1], as defined in section 1701(7) [2] of title 21 (as last in effect); and

(B) any subdivision of the Department that has a significant counternarcotics responsibility, as determined by—

(i) the counternarcotics officer, appointed under section 458 of this title; or

(ii) if applicable, the counternarcotics officer's successor in function (as determined by the Secretary); and

(2) the term "performance appraisal system" means a system under which periodic appraisals of job performance of employees are made, whether under chapter 43 of title 5, or otherwise.

(Pub. L. 107–296, title VIII, §843, as added Pub. L. 108–458, title VII, §7408(a), Dec. 17, 2004, 118 Stat. 3854.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1701(7) of title 21, referred to in subsec. (b)(1)(A), was redesignated section 1701(11) of title 21 by Pub. L. 115–271, title VIII, §8216(4), Oct. 24, 2018, 132 Stat. 4117.

[1] So in original. Probably should be "agency".

[2] See References in Text note below.

§414. Homeland Security Rotation Program

(a) [1] Establishment

(1) In general

Not later than 180 days after October 4, 2006, the Secretary shall establish the Homeland Security Rotation Program (in this section referred to as the "Rotation Program") for employees of the Department. The Rotation Program shall use applicable best practices, including those from the Chief Human Capital Officers Council.

(2) Goals

The Rotation Program established by the Secretary shall—

(A) be established in accordance with the Human Capital Strategic Plan of the Department;

(B) provide middle and senior level employees in the Department the opportunity to broaden their knowledge through exposure to other components of the Department;

(C) expand the knowledge base of the Department by providing for rotational assignments of employees to other components;

(D) build professional relationships and contacts among the employees in the Department;

(E) invigorate the workforce with exciting and professionally rewarding opportunities;

(F) incorporate Department human capital strategic plans and activities, and address critical human capital deficiencies, recruitment and retention efforts, and succession planning within the Federal workforce of the Department; and

(G) complement and incorporate (but not replace) rotational programs within the Department in effect on October 4, 2006.

(3) Administration

(A) In general

The Chief Human Capital Officer shall administer the Rotation Program.

(B) Responsibilities

The Chief Human Capital Officer shall—

(i) provide oversight of the establishment and implementation of the Rotation Program;

(ii) establish a framework that supports the goals of the Rotation Program and promotes cross-disciplinary rotational opportunities;

(iii) establish eligibility for employees to participate in the Rotation Program and select participants from employees who apply;

(iv) establish incentives for employees to participate in the Rotation Program, including promotions and employment preferences;

(v) ensure that the Rotation Program provides professional education and training;

(vi) ensure that the Rotation Program develops qualified employees and future leaders with broad-based experience throughout the Department;

(vii) provide for greater interaction among employees in components of the Department; and

(viii) coordinate with rotational programs within the Department in effect on October 4, 2006.

(4) Allowances, privileges, and benefits

All allowances, privileges, rights, seniority, and other benefits of employees participating in the Rotation Program shall be preserved.

(5) Reporting

Not later than 180 days after the date of the establishment of the Rotation Program, the Secretary shall submit a report on the status of the Rotation Program, including a description of

the Rotation Program, the number of employees participating, and how the Rotation Program is used in succession planning and leadership development to the appropriate committees of Congress.

(Pub. L. 107–296, title VIII, §844, as added Pub. L. 109–295, title VI, §622(a), Oct. 4, 2006, 120 Stat. 1416.)

[1] *So in original. There is no subsec. (b).*

§415. Homeland Security Education Program

(a) Establishment

The Secretary, acting through the Administrator, shall establish a graduate-level Homeland Security Education Program in the National Capital Region to provide educational opportunities to senior Federal officials and selected State and local officials with homeland security and emergency management responsibilities. The Administrator shall appoint an individual to administer the activities under this section.

(b) Leveraging of existing resources

To maximize efficiency and effectiveness in carrying out the Program, the Administrator shall use existing Department-reviewed Master's Degree curricula in homeland security, including curricula pending accreditation, together with associated learning materials, quality assessment tools, digital libraries, exercise systems and other educational facilities, including the National Domestic Preparedness Consortium, the National Fire Academy, and the Emergency Management Institute. The Administrator may develop additional educational programs, as appropriate.

(c) Student enrollment

(1) Sources

The student body of the Program shall include officials from Federal, State, local, and tribal governments, and from other sources designated by the Administrator.

(2) Enrollment priorities and selection criteria

The Administrator shall establish policies governing student enrollment priorities and selection criteria that are consistent with the mission of the Program.

(3) Diversity

The Administrator shall take reasonable steps to ensure that the student body represents racial, gender, and ethnic diversity.

(d) Service commitment

(1) In general

Before any employee selected for the Program may be assigned to participate in the program, the employee shall agree in writing—

(A) to continue in the service of the agency sponsoring the employee during the 2-year period beginning on the date on which the employee completes the program, unless the employee is involuntarily separated from the service of that agency for reasons other than a reduction in force; and

(B) to pay to the Government the amount of the additional expenses incurred by the Government in connection with the employee's education if the employee is voluntarily separated from the service to the agency before the end of the period described in subparagraph (A).

(2) Payment of expenses

(A) Exemption

An employee who leaves the service of the sponsoring agency to enter into the service of another agency in any branch of the Government shall not be required to make a payment under paragraph (1)(B), unless the head of the agency that sponsored the education of the employee notifies that employee before the date on which the employee enters the service of the other agency that payment is required under that paragraph.

(B) Amount of payment

If an employee is required to make a payment under paragraph (1)(B), the agency that sponsored the education of the employee shall determine the amount of the payment, except that such amount may not exceed the pro rata share of the expenses incurred for the time remaining in the 2-year period.

(3) Recovery of payment

If an employee who is required to make a payment under this subsection does not make the payment, a sum equal to the amount of the expenses incurred by the Government for the education of that employee is recoverable by the Government from the employee or his estate by—

(A) setoff against accrued pay, compensation, amount of retirement credit, or other amount due the employee from the Government; or

(B) such other method as is provided by lay [1] for the recovery of amounts owing to the Government.

(Pub. L. 107–296, title VIII, §845, as added Pub. L. 109–295, title VI, §623(a), Oct. 4, 2006, 120 Stat. 1418.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

The reference to the "Administrator" in text probably means the Administrator of the Federal Emergency Management Agency. Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

[1] So in original. Probably should be "law".

§416. Use of protective equipment or measures by employees

None of the funds made available in this or any other Act for fiscal year 2013 and thereafter may be used to propose or effect a disciplinary or adverse action, with respect to any Department of Homeland Security employee who engages regularly with the public in the performance of his or her official duties solely because that employee elects to utilize protective equipment or measures, including but not limited to surgical masks, N95 respirators, gloves, or hand-sanitizers, where use of such equipment or measures is in accord with Department of Homeland Security policy, and Centers for Disease Control and Prevention and Office of Personnel Management guidance.

(Pub. L. 113–6, div. D, title V, §540, Mar. 26, 2013, 127 Stat. 373.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in text, means div. D of Pub. L. 113–6, Mar. 26, 2013, 127 Stat. 342, known as the Department of Homeland Security Appropriations Act, 2013. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2013, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§417. Rotational cybersecurity research program

To enhance the Department's cybersecurity capacity, the Secretary may establish a rotational research, development, and training program for—

(1) detail to the Cybersecurity and Infrastructure Security Agency (including the national cybersecurity and communications integration center authorized by section 659 of this title) of Coast Guard Academy graduates and faculty; and

(2) detail to the Coast Guard Academy, as faculty, of individuals with expertise and experience in cybersecurity who are employed by—

(A) the Agency (including the center);

(B) the Directorate of Science and Technology; or

(C) institutions that have been designated by the Department as a Center of Excellence for Cyber Defense, or the equivalent.

(Pub. L. 107–296, title VIII, §846, as added Pub. L. 116–283, div. G, title LVXXXII [LXXXII], §8278(a), Jan. 1, 2021, 134 Stat. 4687.)

PART F—FEDERAL EMERGENCY PROCUREMENT FLEXIBILITY

§421. Definition

In this part, the term "executive agency" has the meaning given that term under section 133 of title 41.

(Pub. L. 107–296, title VIII, §851, Nov. 25, 2002, 116 Stat. 2235.)

EDITORIAL NOTES

CODIFICATION

In text, "section 133 of title 41" substituted for "section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1))" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

§422. Procurements for defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack

The authorities provided in this part apply to any procurement of property or services by or for an executive agency that, as determined by the head of the executive agency, are to be used to facilitate defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack, but only if a solicitation of offers for the procurement is issued during the 1-year period beginning on November 25, 2002.

(Pub. L. 107–296, title VIII, §852, Nov. 25, 2002, 116 Stat. 2235.)

§423. Increased simplified acquisition threshold for procurements in support of humanitarian or peacekeeping operations or contingency operations

(a) Temporary threshold amounts

For a procurement referred to in section 422 of this title that is carried out in support of a humanitarian or peacekeeping operation or a contingency operation, the simplified acquisition threshold definitions shall be applied as if the amount determined under the exception provided for such an operation in those definitions were—

(1) in the case of a contract to be awarded and performed, or purchase to be made, inside the United States, $200,000; or

(2) in the case of a contract to be awarded and performed, or purchase to be made, outside the United States, $300,000.

(b) Simplified acquisition threshold definitions

In this section, the term "simplified acquisition threshold definitions" means the following:

(1) Section 134 of title 41.

(2) Section 153 of title 41.

(3) Section 3015 of title 10.

(c) Small business reserve

For a procurement carried out pursuant to subsection (a), section 644(j) of title 15 shall be applied as if the maximum anticipated value identified therein is equal to the amounts referred to in subsection (a).

(Pub. L. 107–296, title VIII, §853, Nov. 25, 2002, 116 Stat. 2235; Pub. L. 117–81, div. A, title XVII, §1702(c)(2), Dec. 27, 2021, 135 Stat. 2155.)

EDITORIAL NOTES

AMENDMENTS

2021—Subsec. (b). Pub. L. 117–81 added pars. (1) to (3) and struck out former pars. (1) to (3) which read as follows:

"(1) Section 4(11) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(11)).

"(2) Section 309(d) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 259(d)).

"(3) Section 2302(7) of title 10."

§424. Increased micro-purchase threshold for certain procurements

In the administration of section 1902 of title 41 with respect to a procurement referred to in section 422 of this title, the amount specified in subsections (a), (d), and (e) of such section 1902 shall be deemed to be $7,500.

(Pub. L. 107–296, title VIII, §854, Nov. 25, 2002, 116 Stat. 2236.)

EDITORIAL NOTES

CODIFICATION

In text, "section 1902 of title 41" substituted for "section 32 of the Office of Federal Procurement Policy Act (41 U.S.C. 428)" and "subsections (a), (d), and (e) of such section 1902" substituted for "subsections (c), (d), and (f) of such section 32" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

§425. Application of certain commercial items authorities to certain procurements

(a) Authority

(1) In general

The head of an executive agency may apply the provisions of law listed in paragraph (2) to a procurement referred to in section 422 of this title without regard to whether the property or services are commercial items.

(2) Commercial item laws

The provisions of law referred to in paragraph (1) are as follows:

(A) Sections 1901 and 1906 of title 41.

(B) Section 3205 of title 10.

(C) Section 3305 of title 41.

(b) Inapplicability of limitation on use of simplified acquisition procedures

(1) In general

The $5,000,000 limitation provided in section 1901(a)(2) of title 41, section 3205(a)(2) of title 10, and section 3305(a)(2) of title 41 shall not apply to purchases of property or services to which any of the provisions of law referred to in subsection (a) are applied under the authority of this section.

(2) OMB guidance

The Director of the Office of Management and Budget shall issue guidance and procedures for the use of simplified acquisition procedures for a purchase of property or services in excess of $5,000,000 under the authority of this section.

(c) Continuation of authority for simplified purchase procedures

Authority under a provision of law referred to in subsection (a)(2) that expires under section 4202(e) of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106; 10 U.S.C. 2304 note) shall, notwithstanding such section, continue to apply for use by the head of an executive agency as provided in subsections (a) and (b).

(Pub. L. 107–296, title VIII, §855, Nov. 25, 2002, 116 Stat. 2236; Pub. L. 117–81, div. A, title XVII, §1702(c)(3), Dec. 27, 2021, 135 Stat. 2155.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 4202(e) of the Clinger-Cohen Act of 1996, referred to in subsec. (c), is section 4202(e) of Pub. L. 104–106, which is set out as a note under section 2304 of Title 10, Armed Forces.

AMENDMENTS

2021—Subsec. (a)(2). Pub. L. 117–81, §1702(c)(3)(A), added subpars. (A) to (C) and struck out former subpars. (A) to (C) which read as follows:

"(A) Sections 1901 and 1906 of title 41.

"(B) Section 2304(g) of title 10.

"(C) Section 3305 of title 41."

Subsec. (b)(1). Pub. L. 117–81, §1702(c)(3)(B), substituted "provided in section 1901(a)(2) of title 41, section 3205(a)(2) of title 10, and section 3305(a)(2) of title 41 shall not" for "provided in section 1901(a)(2) of title 41, section 2304(g)(1)(B) of title 10, and section 3305(a)(2) of title 41 shall not".

§426. Use of streamlined procedures

(a) Required use

The head of an executive agency shall, when appropriate, use streamlined acquisition authorities and procedures authorized by law for a procurement referred to in section 422 of this title, including authorities and procedures that are provided under the following provisions of law:

(1) Federal Property and Administrative Services Act of 1949

In division C of subtitle I of title 41:

(A) Paragraphs (1), (2), (6), and (7) of subsection (a) of section 3304 of title 41, relating to use of procedures other than competitive procedures under certain circumstances (subject to subsection (d) of such section).

(B) Section 4106 of title 41, relating to orders under task and delivery order contracts.

(2) Title 10

In part V of subtitle A of title 10:

(A) Paragraphs (1), (2), (6), and (7) of subsection (a) of section 3204, relating to use of procedures other than competitive procedures under certain circumstances (subject to subsection (d) of such section).

(B) Section 3406, relating to orders under task and delivery order contracts.

(3) Office of Federal Procurement Policy Act

Paragraphs (1)(B), (1)(D), and (2)(A) of section 1708(b) of title 41, relating to inapplicability of a requirement for procurement notice.

(b) Waiver of certain small business threshold requirements

Subclause (II) of section 637(a)(1)(D)(i) of title 15 and clause (ii) of section 657a(b)(2)(A) [1] of title 15 shall not apply in the use of streamlined acquisition authorities and procedures referred to in paragraphs (1)(A) and (2)(A) of subsection (a) for a procurement referred to in section 422 of this title.

(Pub. L. 107–296, title VIII, §856, Nov. 25, 2002, 116 Stat. 2237; Pub. L. 117–81, div. A, title XVII, §1702(c)(4), Dec. 27, 2021, 135 Stat. 2155.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Federal Property and Administrative Services Act of 1949, referred to in subsec. (a)(1) heading, is act June 30, 1949, ch. 288, 63 Stat. 377. Title III of the Act was classified generally to subchapter IV (§251 et seq.) of chapter 4 of former Title 41, Public Contracts, and was substantially repealed and restated in division C (§3101 et seq.) of subtitle I of Title 41, Public Contracts, by Pub. L. 111–350, §§3, 7(b), Jan. 4, 2011, 124 Stat. 3677, 3855. For complete classification of this Act to the Code, see Short Title of 1949 Act note set out under section 101 of Title 41 and Tables. For disposition of sections of former Title 41, see Disposition Table preceding section 101 of Title 41.

The Office of Federal Procurement Policy Act, referred to in subsec. (a)(3) heading, is Pub. L. 93–400, Aug. 30, 1974, 88 Stat. 796, which was classified principally to chapter 7 (§401 et seq.) of former Title 41, Public Contracts, and was substantially repealed and restated in division B (§1101 et seq.) of subtitle I of Title 41, Public Contracts, by Pub. L. 111–350, §§3, 7(b), Jan. 4, 2011, 124 Stat. 3677, 3855. For complete classification of this Act to the Code, see Short Title of 1974 Act note set out under section 101 of Title 41 and Tables. For disposition of sections of former Title 41, see Disposition Table preceding section 101 of Title 41.

Subsec. (b) of section 657a of title 15, referred to in subsec. (b), was redesignated subsec. (c) of that section by Pub. L. 115–91, div. A, title XVII, §1701(a)(1), Dec. 12, 2017, 131 Stat. 1795.

AMENDMENTS

2021—Subsec. (a). Pub. L. 117–81 added pars. (1) to (3) and struck out former pars. (1) to (3) which listed provisions in titles 10 and 41 to be followed for procurements.

[1] *See References in Text note below.*

§427. Review and report by Comptroller General

(a) Requirements

Not later than March 31, 2004, the Comptroller General shall—

(1) complete a review of the extent to which procurements of property and services have been made in accordance with this part; and

(2) submit a report on the results of the review to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

(b) Content of report

The report under subsection (a)(2) shall include the following matters:

(1) Assessment

The Comptroller General's assessment of—

(A) the extent to which property and services procured in accordance with this subchapter have contributed to the capacity of the workforce of Federal Government employees within each executive agency to carry out the mission of the executive agency; and

(B) the extent to which Federal Government employees have been trained on the use of technology.

(2) Recommendations

Any recommendations of the Comptroller General resulting from the assessment described in paragraph (1).

(c) Consultation

In preparing for the review under subsection (a)(1), the Comptroller shall consult with the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives on the specific issues and topics to be reviewed. The extent of coverage needed in areas such as technology integration, employee training, and human capital management, as well as the data requirements of the study, shall be included as part of the consultation.

(Pub. L. 107–296, title VIII, §857, Nov. 25, 2002, 116 Stat. 2237.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in subsec. (b)(1)(A), was in the original "this title", meaning title VIII of Pub. L. 107–296, which enacted this subchapter, chapter 97 of Title 5, Government Organization and Employees, and section 8J of the Inspector General Act of 1978, Pub. L. 95–452, formerly set out in the Appendix to Title 5 (see 5 U.S.C. 418), amended section 6 of the Inspector General Act of 1978 (see 5 U.S.C. 406), section 2517 of Title 18, Crimes and Criminal Procedure, Rule 6 of the Federal Rules of Criminal Procedure, set out in the Appendix to Title 18, section 1105 of Title 31, Money and Finance, section 416 of former Title 41, Public Contracts, and sections 1806, 1825, and 3365 of Title 50, War and National Defense, enacted provisions set out as notes under section 101 of this title, section 6 of the Inspector General Act of 1978, and section 1105 of Title 31, amended provisions set out as notes under section 2517 of Title 18, section 40101 of Title 49, Transportation, and section 2301 of Title 50, and repealed provisions set out as a note under section 1113 of Title 31. For complete classification of title VIII to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and

Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§428. Identification of new entrants into the Federal marketplace

The head of each executive agency shall conduct market research on an ongoing basis to identify effectively the capabilities, including the capabilities of small businesses and new entrants into Federal contracting, that are available in the marketplace for meeting the requirements of the executive agency in furtherance of defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack. The head of the executive agency shall, to the maximum extent practicable, take advantage of commercially available market research methods, including use of commercial databases, to carry out the research.

(Pub. L. 107–296, title VIII, §858, Nov. 25, 2002, 116 Stat. 2238.)

PART G—SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES

§441. Administration

(a) In general

The Secretary shall be responsible for the administration of this part.

(b) Designation of qualified anti-terrorism technologies

The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this part in accordance with criteria that shall include, but not be limited to, the following:

(1) Prior United States Government use or demonstrated substantial utility and effectiveness.

(2) Availability of the technology for immediate deployment in public and private settings.

(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.

(4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this part are extended.

(5) Magnitude of risk exposure to the public if such anti-terrorism technology is not deployed.

(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.

(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.

(c) Regulations

The Secretary may issue such regulations, after notice and comment in accordance with section 553 of title 5, as may be necessary to carry out this part.

(Pub. L. 107–296, title VIII, §862, Nov. 25, 2002, 116 Stat. 2238.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

For short title of this part as the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" or the "SAFETY Act", see section 861 of Pub. L. 107–296, set out as a Short Title note under section 101 of this title.

§442. Litigation management

(a) Federal cause of action

(1) In general

There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers [1] that provide qualified anti-terrorism technology to Federal and non-Federal government [2] customers.

(2) Jurisdiction

Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.

(b) Special rules

In an action brought under this section for damages the following provisions apply:

(1) Punitive damages

No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.

(2) Noneconomic damages

(A) In general

Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

(B) Definition

For purposes of subparagraph (A), the term "noneconomic damages" means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

(c) Collateral sources

Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism that result or may result in loss to the Seller.

(d) Government contractor defense

(1) In general

Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the

course of the Secretary's consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.

(2) Exclusive responsibility

The Secretary will be exclusively responsible for the review and approval of anti-terrorism technology for purposes of establishing a government contractor defense in any product liability lawsuit for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. Upon the Seller's submission to the Secretary for approval of anti-terrorism technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.

(3) Certificate

For anti-terrorism technology reviewed and approved by the Secretary, the Secretary will issue a certificate of conformance to the Seller and place the anti-terrorism technology on an Approved Product List for Homeland Security.

(e) Exclusion

Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—

(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from such act of terrorism; or

(2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.

(Pub. L. 107–296, title VIII, §863, Nov. 25, 2002, 116 Stat. 2239.)

[1] So in original. Probably should be "Sellers".

[2] So in original. Probably should be "Government".

§443. Risk management

(a) In general

(1) Liability insurance required

Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers ("Seller") shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(2) Maximum amount

For the total claims related to 1 such act of terrorism, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies.

(3) Scope of coverage

Liability insurance obtained pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture,

qualification, sale, use, or operation of qualified anti-terrorism technologies deployed in defense against or response or recovery from an act of terrorism:

(A) Contractors, subcontractors, suppliers, vendors and customers of the Seller.

(B) Contractors, subcontractors, suppliers, and vendors of the customer.

(4) Third party claims

Such liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.

(b) Reciprocal waiver of claims

The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use or operation of qualified anti-terrorism technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(c) Extent of liability

Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

(Pub. L. 107–296, title VIII, §864, Nov. 25, 2002, 116 Stat. 2240.)

§444. Definitions

For purposes of this part, the following definitions apply:

(1) Qualified anti-terrorism technology

For purposes of this part, the term "qualified anti-terrorism technology" means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.

(2) Act of terrorism

(A) The term "act of terrorism" means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

(B) REQUIREMENTS.—An act meets the requirements of this subparagraph if the act—

(i) is unlawful;

(ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and

(iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

(3) Insurance carrier

The term "insurance carrier" means any corporation, association, society, order, firm, company, mutual,[1] partnership, individual aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial

insurance carrier.

(4) Liability insurance

(A) [2] In general

The term "liability insurance" means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;

(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;

(iii) bodily injury (including) to persons other than the insured or its employees; or

(iv) loss resulting from debt or default of another.

(5) Loss

The term "loss" means death, bodily injury, or loss of or damage to property, including business interruption loss.

(6) Non-Federal Government customers

The term "non-Federal Government customers" means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 [50 U.S.C. 1431 et seq.] to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.

(Pub. L. 107–296, title VIII, §865, Nov. 25, 2002, 116 Stat. 2241.)

EDITORIAL NOTES

REFERENCES IN TEXT

Public Law 85–804, referred to in par. (6), is Pub. L. 85–804, Aug. 28, 1958, 72 Stat. 972, which is classified generally to chapter 29 (§1431 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Tables.

[1] So in original.

[2] So in original. No subpar. (B) has been enacted.

PART H—MISCELLANEOUS PROVISIONS

§451. Advisory committees

(a) In general

The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from chapter 10 of title 5, but the Secretary shall publish notice in the Federal Register announcing the establishment of such a committee and identifying its purpose and membership. Notwithstanding the preceding sentence, members of an advisory committee that is exempted by the Secretary under the preceding sentence who are special Government employees (as that term is defined in section 202 of title 18) shall be eligible for certifications under subsection (b)(3) of section 208 of title 18 for official actions taken as a member of such advisory committee.

(b) Termination

Any advisory committee established by the Secretary shall terminate 2 years after the date of its

establishment, unless the Secretary makes a written determination to extend the advisory committee to a specified date, which shall not be more than 2 years after the date on which such determination is made. The Secretary may make any number of subsequent extensions consistent with this subsection.

(Pub. L. 107–296, title VIII, §871, Nov. 25, 2002, 116 Stat. 2243; Pub. L. 117–286, §4(a)(16), Dec. 27, 2022, 136 Stat. 4307.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–286 substituted "chapter 10 of title 5," for "Public Law 92–463,".

STATUTORY NOTES AND RELATED SUBSIDIARIES

ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY ECONOMIC SECURITY COUNCIL

Pub. L. 117–263, div. G, title LXXI, §7116(a), Dec. 23, 2022, 136 Stat. 3636, provided that:

"(1) DEFINITIONS.—In this subsection:

"(A) COUNCIL.—The term 'Council' means the council established under paragraph (2).

"(B) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

"(C) ECONOMIC SECURITY.—The term 'economic security' has the meaning given such term in section 890B(c)(2) of the Homeland Security Act of 2002 (6 U.S.C. 474(c)(2)).

"(D) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(2) ESTABLISHMENT.—In accordance with the mission of the Department under section 101(b) of the Homeland Security Act of 2002 (6 U.S.C. 111(b)), and in particular paragraph (1)(F) of such section, the Secretary shall establish a standing council of Department component heads or their designees, to carry out the duties described in paragraph (3).

"(3) DUTIES OF THE COUNCIL.—Pursuant to the scope of the mission of the Department as described in paragraph (2), the Council shall provide to the Secretary advice and recommendations on matters of economic security, including relating to the following:

"(A) Identifying concentrated risks for trade and economic security.

"(B) Setting priorities for securing the trade and economic security of the United States.

"(C) Coordinating Department-wide activity on trade and economic security matters.

"(D) With respect to the development of the continuity of the economy plan of the President under section 9603 of the William M. (Mac) Thornberry National Defense Authorization Act of [for] Fiscal Year 2021 (6 U.S.C. 322).

"(E) Proposing statutory and regulatory changes impacting trade and economic security.

"(F) Any other matters the Secretary considers appropriate.

"(4) CHAIR AND VICE CHAIR.—The Under Secretary for Strategy, Policy, and Plans of the Department—

"(A) shall serve as Chair of the Council; and

"(B) may designate a Council member as a Vice Chair.

"(5) MEETINGS.—The Council shall meet not less frequently than quarterly, as well as—

"(A) at the call of the Chair; or

"(B) at the direction of the Secretary.

"(6) BRIEFINGS.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2022] and every 180 days thereafter for four years, the Council shall brief the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Finance of the Senate, the Committee on Ways and Means of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, and Committee on Energy and Commerce of the House of Representatives on the actions and activities of the Council."

[Nothing in section 7116(a) of Pub. L. 117–263, set out above, to be construed to affect or diminish the authority otherwise granted to any other officer of the Department of Homeland Security, see section 7116(c) of Pub. L. 117–263, set out as a note under section 349 of this title.]

§452. Reorganization

(a) Reorganization

The Secretary may allocate or reallocate functions among the officers of the Department, and may establish, consolidate, alter, or discontinue organizational units within the Department, but only—

(1) pursuant to section 542(b) of this title; or

(2) after the expiration of 60 days after providing notice of such action to the appropriate congressional committees, which shall include an explanation of the rationale for the action.

(b) Limitations

(1) In general

Authority under subsection (a)(1) does not extend to the abolition of any agency, entity, organizational unit, program, or function established or required to be maintained by this chapter.

(2) Abolitions

Authority under subsection (a)(2) does not extend to the abolition of any agency, entity, organizational unit, program, or function established or required to be maintained by statute.

(Pub. L. 107–296, title VIII, §872, Nov. 25, 2002, 116 Stat. 2243.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (b)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

TRANSFER OF OFFICE OF BIOMETRIC IDENTITY MANAGEMENT AND FEDERAL PROTECTIVE SERVICE

Pub. L. 115–278, §3, Nov. 16, 2018, 132 Stat. 4184, provided that:

"(a) OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.—The Office of Biometric Identity Management of the Department of Homeland Security located in the National Protection and Programs Directorate of the Department of Homeland Security on the day before the date of enactment of this Act [Nov. 16, 2018] is hereby transferred to the Management Directorate of the Department.

"(b) FEDERAL PROTECTIVE SERVICE.—

"(1) IN GENERAL.—Not later than 90 days after the completion of the Government Accountability Office review of the organizational placement of the Federal Protective Service (authorized under section 1315 of title 40, United States Code), the Secretary of Homeland Security shall determine the appropriate placement of the Service within the Department of Homeland Security and commence the transfer of the Service to such component, directorate, or other office of the Department that the Secretary so determines appropriate.

"(2) EXCEPTION.—If the Secretary of Homeland Security determines pursuant to paragraph (1) that no component, directorate, or other office of the Department of Homeland Security is an appropriate placement for the Federal Protective Service, the Secretary shall—

"(A) provide to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and the Office of Management and Budget a detailed explanation, in writing, of the reason for such determination that includes—

"(i) information on how the Department considered the Government Accountability Office review described in such paragraph;

"(ii) a list of the components, directorates, or other offices of the Department that were considered for such placement; and

"(iii) information on why each such component, directorate, or other office of the Department was determined to not be an appropriate placement for the Service;

"(B) not later than 120 days after the completion of the Government Accountability Office review described in such paragraph, develop and submit to the committees specified in subparagraph (A) and the Office of Management and Budget a plan to coordinate with other appropriate Federal agencies, including the General Services Administration, to determine a more appropriate placement for the Service; and

"(C) not later than 180 days after the completion of such Government Accountability Office review, submit to such committees and the Office of Management and Budget a recommendation regarding the appropriate placement of the Service within the executive branch of the Federal Government."

§453. Use of appropriated funds

(a) Disposal of property

(1) Strict compliance

If specifically authorized to dispose of real property in this chapter or any other Act, the Secretary shall exercise this authority in strict compliance with subchapter IV of chapter 5 of title 40.

(2) Deposit of proceeds

The Secretary shall deposit the proceeds of any exercise of property disposal authority into the miscellaneous receipts of the Treasury in accordance with section 3302(b) of title 31.

(b) Gifts

Except as authorized by section 2601 of title 10, by section 93 [1] of title 14, or by section 321n or 464 of this title, gifts or donations of services or property of or for the Department may not be accepted, used, or disposed of unless specifically permitted in advance in an appropriations Act and only under the conditions and for the purposes specified in such appropriations Act.

(c) Budget request

Under section 1105 of title 31, the President shall submit to Congress a detailed budget request for the Department for fiscal year 2004, and for each subsequent fiscal year.

(Pub. L. 107–296, title VIII, §873, Nov. 25, 2002, 116 Stat. 2243; Pub. L. 108–7, div. L, §103(3), Feb. 20, 2003, 117 Stat. 529; Pub. L. 111–245, §2(a)(2), Sept. 30, 2010, 124 Stat. 2621.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (a)(1), was in the original a reference to this Act, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

Section 93 of title 14, referred to in subsec. (b), was redesignated section 504 of title 14 by Pub. L. 115–282, title I, §105(b), Dec. 4, 2018, 132 Stat. 4200, and references to section 93 of title 14 deemed to refer to such redesignated section, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

CODIFICATION

In subsec. (a)(1), "subchapter IV of chapter 5 of title 40" substituted for "section 204 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 485)" on authority of Pub. L. 107–217, §5(c), Aug. 21, 2002, 116 Stat. 1303, the first section of which enacted Title 40, Public Buildings, Property, and Works.

AMENDMENTS

2010—Subsec. (b). Pub. L. 111–245 substituted "title 10, by section 93 of title 14, or by section 321n or 464 of this title, gifts or donations" for "title 10 and by section 93 of title 14, gifts or donations".

2003—Subsec. (b). Pub. L. 108–7 substituted "Except as authorized by section 2601 of title 10 and by section 93 of title 14, gifts" for "Gifts".

[1] *See References in Text note below.*

§453a. Additional uses of appropriated funds

In fiscal year 2004 and thereafter, unless otherwise provided, funds may be used for purchase of uniforms without regard to the general purchase price limitation for the current fiscal year; purchase of insurance for official motor vehicles operated in foreign countries; entering into contracts with the Department of State to furnish health and medical services to employees and their dependents serving in foreign countries; services authorized by section 3109 of title 5; and the hire and purchase of motor vehicles, as authorized by section 1343 of title 31: *Provided*, That purchase for police-type use of passenger vehicles may be made without regard to the general purchase price limitation for the current fiscal year.

(Pub. L. 108–90, title V, §505, Oct. 1, 2003, 117 Stat. 1153.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§453b. Requirement to buy certain items related to national security interests from American sources; exceptions

(a) Requirement

Except as provided in subsections (c) through (g), funds appropriated or otherwise available to the Department of Homeland Security may not be used for the procurement of an item described in subsection (b) if the item is not grown, reprocessed, reused, or produced in the United States.

(b) Covered items

An item referred to in subsection (a) is any of the following, if the item is directly related to the national security interests of the United States:

(1) [1] An article or item of—

(A) clothing and the materials and components thereof, other than sensors, electronics, or other items added to, and not normally associated with, clothing (and the materials and components thereof);

(B) tents, tarpaulins, covers, textile belts, bags, protective equipment (including but not limited to body armor), sleep systems, load carrying equipment (including but not limited to fieldpacks), textile marine equipment, parachutes, or bandages;

(C) cotton and other natural fiber products, woven silk or woven silk blends, spun silk yarn for cartridge cloth, synthetic fabric or coated synthetic fabric (including all textile fibers and yarns that are for use in such fabrics), canvas products, or wool (whether in the form of fiber or yarn or contained in fabrics, materials, or manufactured articles); or

(D) any item of individual equipment manufactured from or containing such fibers, yarns, fabrics, or materials.

(c) Availability exception

Subsection (a) does not apply to the extent that the Secretary of Homeland Security determines that satisfactory quality and sufficient quantity of any such article or item described in subsection (b)(1) grown, reprocessed, reused, or produced in the United States cannot be procured as and when

needed at United States market prices. This section is not applicable to covered items that are, or include, materials determined to be non-available in accordance with Federal Acquisition Regulation 25.104 Nonavailable Articles.

(d) De minimis exception

Notwithstanding subsection (a), the Secretary of Homeland Security may accept delivery of an item covered by subsection (b) that contains non-compliant fibers if the total value of non-compliant fibers contained in the end item does not exceed 10 percent of the total purchase price of the end item.

(e) Exception for certain procurements outside the United States

Subsection (a) does not apply to the following:

(1) Procurements by vessels in foreign waters.

(2) Emergency procurements.

(f) Exception for small purchases

Subsection (a) does not apply to purchases for amounts not greater than the simplified acquisition threshold referred to in section 3205 of title 10.

(g) Applicability to contracts and subcontracts for procurement of commercial products

This section is applicable to contracts and subcontracts for the procurement of commercial products notwithstanding section 1906 of title 41, with the exception of commercial products listed under subsections (b)(1)(C) and (b)(1)(D) above. For the purposes of this section, "commercial product" shall be as defined in section 103 of title 41.

(h) Geographic coverage

In this section, the term "United States" includes the possessions of the United States.

(i) Notification required within 7 days after contract award if certain exceptions applied

In the case of any contract for the procurement of an item described in subsection (b)(1), if the Secretary of Homeland Security applies an exception set forth in subsection (c) with respect to that contract, the Secretary shall, not later than 7 days after the award of the contract, post a notification that the exception has been applied on the Internet site maintained by the General Services Administration known as FedBizOps.gov (or any successor site).

(j) Training during fiscal year 2009

(1) In general

The Secretary of Homeland Security shall ensure that each member of the acquisition workforce in the Department of Homeland Security who participates personally and substantially in the acquisition of textiles on a regular basis receives training during fiscal year 2009 on the requirements of this section and the regulations implementing this section.

(2) Inclusion of information in new training programs

The Secretary shall ensure that any training program for the acquisition workforce developed or implemented after February 17, 2009, includes comprehensive information on the requirements described in paragraph (1).

(k) Consistency with international agreements

This section shall be applied in a manner consistent with United States obligations under international agreements.

(l) Effective date

This section applies with respect to contracts entered into by the Department of Homeland Security 180 days after February 17, 2009.

(Pub. L. 111–5, div. A, title VI, §604, Feb. 17, 2009, 123 Stat. 165; Pub. L. 115–232, div. A, title VIII, §836(g)(1), Aug. 13, 2018, 132 Stat. 1872; Pub. L. 117–81, div. A, title XVII, §1702(c)(5), Dec. 27, 2021, 135 Stat. 2156.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the American Recovery and Reinvestment Act of 2009, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2021—Subsec. (f). Pub. L. 117–81 substituted "section 3205" for "section 2304(g)".

2018—Subsec. (g). Pub. L. 115–232 substituted "commercial products" for "commercial items" in heading and, in text, substituted "procurement of commercial products notwithstanding section 1906 of title 41, with the exception of commercial products listed" for "procurement of commercial items not withstanding section 34 of the Office of Federal Procurement Policy Act (41 U.S.C. 430), with the exception of commercial items listed" and " 'commercial product' shall be as defined in section 103 of title 41." for " 'commercial' shall be as defined in the Federal Acquisition Regulation—Part 2."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2018 AMENDMENT; SAVINGS PROVISION

Pub. L. 115–232, div. A, title VIII, §836(h), Aug. 13, 2018, 132 Stat. 1874, provided that: "The amendments made by subsections (a) through (g) [see Tables for classification] shall take effect on January 1, 2020. Any provision of law that on the day before such effective date is on a list of provisions of law included in the Federal Acquisition Regulation pursuant to section 1907 of title 41, United States Code, shall be deemed as of that effective date to be on a list of provisions of law included in the Federal Acquisition Regulation pursuant to section 1906 of such title."

[1] So in original. No par. (2) has been enacted.

§453c. Disposition of equines unfit for service

None of the funds made available in this or any other Act for fiscal year 2012 and thereafter may be used to destroy or put out to pasture any horse or other equine belonging to any component or agency of the Department of Homeland Security that has become unfit for service, unless the trainer or handler is first given the option to take possession of the equine through an adoption program that has safeguards against slaughter and inhumane treatment.

(Pub. L. 112–74, div. D, title V, §526, Dec. 23, 2011, 125 Stat. 974.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in text, means div. D of Pub. L. 112–74, Dec. 23, 2011, 125 Stat. 943, known as the Department of Homeland Security Appropriations Act, 2012. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2012, and also as part of the Consolidated Appropriations Act, 2012, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§454. Future Years Homeland Security Program

(a) In general

Each budget request submitted to Congress for the Department under section 1105 of title 31 shall,

at or about the same time, be accompanied by a Future Years Homeland Security Program.

(b) Contents

The Future Years Homeland Security Program under subsection (a) shall—

(1) include the same type of information, organizational structure, and level of detail as the future years defense program submitted to Congress by the Secretary of Defense under section 221 of title 10;

(2) set forth the homeland security strategy of the Department, which shall be developed and updated as appropriate annually by the Secretary, that was used to develop program planning guidance for the Future Years Homeland Security Program; and

(3) include an explanation of how the resource allocations included in the Future Years Homeland Security Program correlate to the homeland security strategy set forth under paragraph (2).

(c) Effective date

This section shall take effect with respect to the preparation and submission of the fiscal year 2005 budget request for the Department and for any subsequent fiscal year, except that the first Future Years Homeland Security Program shall be submitted not later than 90 days after the Department's fiscal year 2005 budget request is submitted to Congress.

(Pub. L. 107–296, title VIII, §874, Nov. 25, 2002, 116 Stat. 2244; Pub. L. 108–330, §5, Oct. 16, 2004, 118 Stat. 1278.)

EDITORIAL NOTES

AMENDMENTS

2004—Subsec. (b). Pub. L. 108–330 added subsec. (b) and struck out heading and text of former subsec. (b). Text read as follows: "The Future Years Homeland Security Program under subsection (a) of this section shall be structured, and include the same type of information and level of detail, as the Future Years Defense Program submitted to Congress by the Department of Defense under section 221 of title 10."

STATUTORY NOTES AND RELATED SUBSIDIARIES

ADMINISTRATIVE PROVISIONS

Pub. L. 115–141, div. F, title I, §101, Mar. 23, 2018, 132 Stat. 606, provided that: "Hereafter, the Secretary of Homeland Security shall submit to the Committees on Appropriations of the Senate and the House of Representatives, at the time the President's budget proposal is submitted pursuant to section 1105(a) of title 31, United States Code, the Future Years Homeland Security Program, as authorized by section 874 of the Homeland Security Act of 2002 (6 U.S.C. 454)."

§455. Miscellaneous authorities

(a) Seal

The Department shall have a seal, whose design is subject to the approval of the President.

(b) Participation of members of the Armed Forces

With respect to the Department, the Secretary shall have the same authorities that the Secretary of Transportation has with respect to the Department of Transportation under section 324 of title 49.

(c) Redelegation of functions

Unless otherwise provided in the delegation or by law, any function delegated under this chapter may be redelegated to any subordinate.

(d) Investigation of certain violent acts, shootings, and mass killings

(1) In general

At the request of an appropriate law enforcement official of a State or political subdivision, the Secretary, through deployment of the Secret Service or United States Immigration and Customs Enforcement, may assist in the investigation of violent acts and shootings occurring in a place of public use, and in the investigation of mass killings and attempted mass killings. Any assistance provided by the Secretary under this subsection shall be presumed to be within the scope of Federal office or employment.

(2) Definitions

For purposes of this subsection—

(A) the term "mass killings" means 3 or more killings in a single incident; and

(B) the term "place of public use" has the meaning given that term under section 2332f(e)(6) of title 18.

(Pub. L. 107–296, title VIII, §875, Nov. 25, 2002, 116 Stat. 2244; Pub. L. 112–265, §2(b), Jan. 14, 2013, 126 Stat. 2435.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (c), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2013—Subsec. (d). Pub. L. 112–265 added subsec (d).

§456. Military activities

Nothing in this chapter shall confer upon the Secretary any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this chapter limit the existing authority of the Department of Defense or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities.

(Pub. L. 107–296, title VIII, §876, Nov. 25, 2002, 116 Stat. 2244.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§457. Regulatory authority and preemption

(a) Regulatory authority

Except as otherwise provided in sections 186(c) and 441(c) of this title and section 1315 of title 40,[1] this chapter vests no new regulatory authority in the Secretary or any other Federal official, and transfers to the Secretary or another Federal official only such regulatory authority as exists on November 25, 2002, within any agency, program, or function transferred to the Department pursuant to this chapter, or that on November 25, 2002, is exercised by another official of the executive branch with respect to such agency, program, or function. Any such transferred authority may not be exercised by an official from whom it is transferred upon transfer of such agency, program, or

function to the Secretary or another Federal official pursuant to this chapter. This chapter may not be construed as altering or diminishing the regulatory authority of any other executive agency, except to the extent that this chapter transfers such authority from the agency.

(b) Preemption of State or local law

Except as otherwise provided in this chapter, this chapter preempts no State or local law, except that any authority to preempt State or local law vested in any Federal agency or official transferred to the Department pursuant to this chapter shall be transferred to the Department effective on the date of the transfer to the Department of that Federal agency or official.

(Pub. L. 107–296, title VIII, §877, Nov. 25, 2002, 116 Stat. 2244.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1315 of title 40, referred to in subsec. (a), was in the original "1706(b)", meaning section 1706(b) of Pub. L. 107–296, which amended generally section 1315 of Title 40, Public Buildings, Property, and Works, and enacted provisions set out as a note under section 1315 of Title 40. For complete classification of section 1706(b) to the Code, see Tables.

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

[1] *See References in Text note below.*

§458. Office of Counternarcotics Enforcement

(a) Office

There is established in the Department an Office of Counternarcotics Enforcement, which shall be headed by a Director appointed by the President.

(b) Assignment of personnel

(1) In general

The Secretary shall assign permanent staff to the Office, consistent with effective management of Department resources.

(2) Liaisons

The Secretary shall designate senior employees from each appropriate subdivision of the Department that has significant counternarcotics responsibilities to act as a liaison between that subdivision and the Office of Counternarcotics Enforcement.

(c) Limitation on concurrent employment

The Director of the Office of Counternarcotics Enforcement shall not be employed by, assigned to, or serve as the head of, any other branch of the Federal Government, any State or local government, or any subdivision of the Department other than the Office of Counternarcotics Enforcement.

(d) Responsibilities

The Secretary shall direct the Director of the Office of Counternarcotics Enforcement—

(1) to coordinate policy and operations within the Department, between the Department and other Federal departments and agencies, and between the Department and State and local agencies with respect to stopping the entry of illegal drugs into the United States;

(2) to ensure the adequacy of resources within the Department for stopping the entry of illegal drugs into the United States;

(3) to recommend the appropriate financial and personnel resources necessary to help the Department better fulfill its responsibility to stop the entry of illegal drugs into the United States;

(4) within the Joint Terrorism Task Force construct to track and sever connections between illegal drug trafficking and terrorism; and

(5) to be a representative of the Department on all task forces, committees, or other entities whose purpose is to coordinate the counternarcotics enforcement activities of the Department and other Federal, State or local agencies.

(e) Savings clause

Nothing in this section shall be construed to authorize direct control of the operations conducted by the Directorate of Border and Transportation Security,[1] the Coast Guard, or joint terrorism task forces.

(f) Reports to Congress

(1) Annual budget review

The Director of the Office of Counternarcotics Enforcement shall, not later than 30 days after the submission by the President to Congress of any request for expenditures for the Department, submit to the Committees on Appropriations and the authorizing committees of jurisdiction of the House of Representatives and the Senate a review and evaluation of such request. The review and evaluation shall—

(A) identify any request or subpart of any request that affects or may affect the counternarcotics activities of the Department or any of its subdivisions, or that affects the ability of the Department or any subdivision of the Department to meet its responsibility to stop the entry of illegal drugs into the United States;

(B) describe with particularity how such requested funds would be or could be expended in furtherance of counternarcotics activities; and

(C) compare such requests with requests for expenditures and amounts appropriated by Congress in the previous fiscal year.

(2) Evaluation of counternarcotics activities

The Director of the Office of Counternarcotics Enforcement shall, not later than February 1 of each year, submit to the Committees on Appropriations and the authorizing committees of jurisdiction of the House of Representatives and the Senate a review and evaluation of the counternarcotics activities of the Department for the previous fiscal year. The review and evaluation shall—

(A) describe the counternarcotics activities of the Department and each subdivision of the Department (whether individually or in cooperation with other subdivisions of the Department, or in cooperation with other branches of the Federal Government or with State or local agencies), including the methods, procedures, and systems (including computer systems) for collecting, analyzing, sharing, and disseminating information concerning narcotics activity within the Department and between the Department and other Federal, State, and local agencies;

(B) describe the results of those activities, using quantifiable data whenever possible;

(C) state whether those activities were sufficient to meet the responsibility of the Department to stop the entry of illegal drugs into the United States, including a description of the performance measures of effectiveness that were used in making that determination; and

(D) recommend, where appropriate, changes to those activities to improve the performance of the Department in meeting its responsibility to stop the entry of illegal drugs into the United States.

(3) Classified or law enforcement sensitive information

Any content of a review and evaluation described in the reports required in this subsection that involves information classified under criteria established by an Executive order, or whose public

disclosure, as determined by the Secretary, would be detrimental to the law enforcement or national security activities of the Department or any other Federal, State, or local agency, shall be presented to Congress separately from the rest of the review and evaluation.

(Pub. L. 107–296, title VIII, §878, Nov. 25, 2002, 116 Stat. 2245; Pub. L. 108–458, title VII, §7407(a), Dec. 17, 2004, 118 Stat. 3851; Pub. L. 109–469, title I, §103(f)(2), Dec. 29, 2006, 120 Stat. 3510; Pub. L. 112–166, §2(f)(3), Aug. 10, 2012, 126 Stat. 1284.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Directorate of Border and Transportation Security, referred to in subsection (e), was abolished by section 802(g)(2) of Pub. L. 114–125, which repealed section 201 of this title. Section 211(a) of this title established U.S. Customs and Border Protection.

AMENDMENTS

2012—Subsec. (a). Pub. L. 112–166 struck out ", by and with the advice and consent of the Senate" before period at end.

2006—Subsec. (c). Pub. L. 109–469, §103(f)(2)(A), substituted "The" for "Except as provided in subsection (d) of this section, the".

Subsecs. (d) to (g). Pub. L. 109–469, §103(f)(2)(B), redesignated subsecs. (e) to (g) as (d) to (f), respectively, and struck out heading and text of former subsec. (d). Text read as follows: "The Director of the Office of Counternarcotics Enforcement may be appointed as the United States Interdiction Coordinator by the Director of the Office of National Drug Control Policy, and shall be the only person at the Department eligible to be so appointed."

2004—Pub. L. 108–458 amended section catchline and text generally. Prior to amendment, text read as follows: "The Secretary shall appoint a senior official in the Department to assume primary responsibility for coordinating policy and operations within the Department and between the Department and other Federal departments and agencies with respect to interdicting the entry of illegal drugs into the United States, and tracking and severing connections between illegal drug trafficking and terrorism. Such official shall—

"(1) ensure the adequacy of resources within the Department for illicit drug interdiction; and

"(2) serve as the United States Interdiction Coordinator for the Director of National Drug Control Policy."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–166 effective 60 days after Aug. 10, 2012, and applicable to appointments made on and after that effective date, including any nomination pending in the Senate on that date, see section 6(a) of Pub. L. 112–166, set out as a note under section 113 of this title.

[1] *See References in Text note below.*

§459. Office of International Affairs

(a) Establishment

There is established within the Office of the Secretary an Office of International Affairs. The Office shall be headed by a Director, who shall be a senior official appointed by the Secretary.

(b) Duties of the Director

The Director shall have the following duties:

(1) To promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security. Such exchange shall include the following:

(A) Exchange of information on research and development on homeland security

technologies.

(B) Joint training exercises of first responders.

(C) Exchange of expertise on terrorism prevention, response, and crisis management.

(2) To identify areas for homeland security information and training exchange where the United States has a demonstrated weakness and another friendly nation or nations have a demonstrated expertise.

(3) To plan and undertake international conferences, exchange programs, and training activities.

(4) To manage international activities within the Department in coordination with other Federal officials with responsibility for counter-terrorism matters.

(Pub. L. 107–296, title VIII, §879, Nov. 25, 2002, 116 Stat. 2245.)

§460. Prohibition of the Terrorism Information and Prevention System

Any and all activities of the Federal Government to implement the proposed component program of the Citizen Corps known as Operation TIPS (Terrorism Information and Prevention System) are hereby prohibited.

(Pub. L. 107–296, title VIII, §880, Nov. 25, 2002, 116 Stat. 2245.)

§461. Review of pay and benefit plans

Notwithstanding any other provision of this chapter, the Secretary shall, in consultation with the Director of the Office of Personnel Management, review the pay and benefit plans of each agency whose functions are transferred under this chapter to the Department and, within 90 days after November 25, 2002, submit a plan to the President of the Senate and the Speaker of the House of Representatives and the appropriate committees and subcommittees of Congress, for ensuring, to the maximum extent practicable, the elimination of disparities in pay and benefits throughout the Department, especially among law enforcement personnel, that are inconsistent with merit system principles set forth in section 2301 of title 5.

(Pub. L. 107–296, title VIII, §881, Nov. 25, 2002, 116 Stat. 2246.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§462. Office of National Capital Region Coordination

(a) Establishment

(1) In general

There is established within the Office of the Secretary the Office of National Capital Region Coordination, to oversee and coordinate Federal programs for and relationships with State, local, and regional authorities in the National Capital Region, as defined under section 2674(f)(2) of title 10.

(2) Director

The Office established under paragraph (1) shall be headed by a Director, who shall be appointed by the Secretary.

(3) Cooperation

The Secretary shall cooperate with the Mayor of the District of Columbia, the Governors of Maryland and Virginia, and other State, local, and regional officers in the National Capital Region to integrate the District of Columbia, Maryland, and Virginia into the planning, coordination, and execution of the activities of the Federal Government for the enhancement of domestic preparedness against the consequences of terrorist attacks.

(b) Responsibilities

The Office established under subsection (a)(1) shall—

(1) coordinate the activities of the Department relating to the National Capital Region, including cooperation with the Office for State and Local Government Coordination;

(2) assess, and advocate for, the resources needed by State, local, and regional authorities in the National Capital Region to implement efforts to secure the homeland;

(3) provide State, local, and regional authorities in the National Capital Region with regular information, research, and technical support to assist the efforts of State, local, and regional authorities in the National Capital Region in securing the homeland;

(4) develop a process for receiving meaningful input from State, local, and regional authorities and the private sector in the National Capital Region to assist in the development of the homeland security plans and activities of the Federal Government;

(5) coordinate with Federal agencies in the National Capital Region on terrorism preparedness, to ensure adequate planning, information sharing, training, and execution of the Federal role in domestic preparedness activities;

(6) coordinate with Federal, State, local, and regional agencies, and the private sector in the National Capital Region on terrorism preparedness to ensure adequate planning, information sharing, training, and execution of domestic preparedness activities among these agencies and entities; and

(7) serve as a liaison between the Federal Government and State, local, and regional authorities, and private sector entities in the National Capital Region to facilitate access to Federal grants and other programs.

(c) Annual report

The Office established under subsection (a) shall submit an annual report to Congress that includes—

(1) the identification of the resources required to fully implement homeland security efforts in the National Capital Region;

(2) an assessment of the progress made by the National Capital Region in implementing homeland security efforts; and

(3) recommendations to Congress regarding the additional resources needed to fully implement homeland security efforts in the National Capital Region.

(d) Limitation

Nothing contained in this section shall be construed as limiting the power of State and local governments.

(Pub. L. 107–296, title VIII, §882, Nov. 25, 2002, 116 Stat. 2246.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

INCORPORATION OF GOVERNORS OF WEST VIRGINIA AND PENNSYLVANIA INTO MASS EVACUATION PLANNING

Pub. L. 113–6, div. D, title III, Mar. 26, 2013, 127 Stat. 357, provided in part: "That for fiscal year 2013 and thereafter, for purposes of planning, coordination, execution, and decision making related to mass evacuation during a disaster, the Governors of the State of West Virginia and the Commonwealth of

Pennsylvania, or their designees, shall be incorporated into efforts to integrate the activities of Federal, State, and local governments in the National Capital Region, as defined in section 882 of the Homeland Security Act of 2002 (Public Law 107–296) [6 U.S.C. 462]".

§463. Requirement to comply with laws protecting equal employment opportunity and providing whistleblower protections

Nothing in this chapter shall be construed as exempting the Department from requirements applicable with respect to executive agencies—

(1) to provide equal employment protection for employees of the Department (including pursuant to the provisions in section 2302(b)(1) of title 5 and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (Public Law 107–174)); or

(2) to provide whistleblower protections for employees of the Department (including pursuant to the provisions in section 2302(b)(8) and (9) of such title and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002).

(Pub. L. 107–296, title VIII, §883, Nov. 25, 2002, 116 Stat. 2247.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in introductory provisions, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002, referred to in pars. (1) and (2), is Pub. L. 107–174, May 15, 2002, 116 Stat. 566, which is set out as a note under section 2301 of Title 5, Government Organization and Employees. For complete classification of this Act to the Code, see Tables.

§464. Federal Law Enforcement Training Centers

(a) Establishment

The Secretary shall maintain in the Department the Federal Law Enforcement Training Centers (FLETC), headed by a Director, who shall report to the Secretary.

(b) Position

The Director shall occupy a career-reserved position within the Senior Executive Service.

(c) Functions of the Director

The Director shall—

(1) develop training goals and establish strategic and tactical organizational program plan and priorities;

(2) provide direction and management for FLETC's training facilities, programs, and support activities while ensuring that organizational program goals and priorities are executed in an effective and efficient manner;

(3) develop homeland security and law enforcement training curricula, including curricula related to domestic preparedness and response to threats or acts of terrorism, for Federal, State, local, tribal, territorial, and international law enforcement and security agencies and private sector security agencies;

(4) monitor progress toward strategic and tactical FLETC plans regarding training curricula, including curricula related to domestic preparedness and response to threats or acts of terrorism, and facilities;

(5) ensure the timely dissemination of homeland security information as necessary to Federal,

State, local, tribal, territorial, and international law enforcement and security agencies and the private sector to achieve the training goals for such entities, in accordance with paragraph (1);

(6) carry out delegated acquisition responsibilities in a manner that—

(A) fully complies with—

(i) Federal law;

(ii) the Federal Acquisition Regulation, including requirements regarding agency obligations to contract only with responsible prospective contractors; and

(iii) Department acquisition management directives; and

(B) maximizes opportunities for small business participation;

(7) coordinate and share information with the heads of relevant components and offices on digital learning and training resources, as appropriate;

(8) advise the Secretary on matters relating to executive level policy and program administration of Federal, State, local, tribal, territorial, and international law enforcement and security training activities and private sector security agency training activities, including training activities related to domestic preparedness and response to threats or acts of terrorism;

(9) collaborate with the Secretary and relevant officials at other Federal departments and agencies, as appropriate, to improve international instructional development, training, and technical assistance provided by the Federal Government to foreign law enforcement; and

(10) carry out such other functions as the Secretary determines are appropriate.

(d) Training responsibilities

(1) In general

The Director is authorized to provide training to employees of Federal agencies who are engaged, directly or indirectly, in homeland security operations or Federal law enforcement activities, including such operations or activities related to domestic preparedness and response to threats or acts of terrorism. In carrying out such training, the Director shall—

(A) evaluate best practices of law enforcement training methods and curriculum content to maintain state-of-the-art expertise in adult learning methodology;

(B) provide expertise and technical assistance, including on domestic preparedness and response to threats or acts of terrorism, to Federal, State, local, tribal, territorial, and international law enforcement and security agencies and private sector security agencies; and

(C) maintain a performance evaluation process for students.

(2) Relationship with law enforcement agencies

The Director shall consult with relevant law enforcement and security agencies in the development and delivery of FLETC's training programs.

(3) Training delivery locations

The training required under paragraph (1) may be conducted at FLETC facilities, at appropriate off-site locations, or by distributed learning.

(4) Strategic partnerships

(A) In general

The Director may—

(i) execute strategic partnerships with State and local law enforcement to provide such law enforcement with specific training, including maritime law enforcement training; and

(ii) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency and with private sector stakeholders, including critical infrastructure owners and operators, to provide training pertinent to improving coordination, security, and resiliency of critical infrastructure.

(B) Provision of information

The Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, upon request, information on activities undertaken in the previous year pursuant to subparagraph (A).

(5) FLETC details to DHS

The Director may detail employees of FLETC to positions throughout the Department in furtherance of improving the effectiveness and quality of training provided by the Department and, as appropriate, the development of critical departmental programs and initiatives.

(6) Detail of instructors to FLETC

Partner organizations that wish to participate in FLETC training programs shall assign non-reimbursable detailed instructors to FLETC for designated time periods to support all training programs at FLETC, as appropriate. The Director shall determine the number of detailed instructors that is proportional to the number of training hours requested by each partner organization scheduled by FLETC for each fiscal year. If a partner organization is unable to provide a proportional number of detailed instructors, such partner organization shall reimburse FLETC for the salary equivalent for such detailed instructors, as appropriate.

(7) Partner organization expenses requirements

(A) In general

Partner organizations shall be responsible for the following expenses:

(i) Salaries, travel expenses, lodging expenses, and miscellaneous per diem allowances of their personnel attending training courses at FLETC.

(ii) Salaries and travel expenses of instructors and support personnel involved in conducting advanced training at FLETC for partner organization personnel and the cost of expendable supplies and special equipment for such training, unless such supplies and equipment are common to FLETC-conducted training and have been included in FLETC's budget for the applicable fiscal year.

(B) Excess basic and advanced Federal training

All hours of advanced training and hours of basic training provided in excess of the training for which appropriations were made available shall be paid by the partner organizations and provided to FLETC on a reimbursable basis in accordance with section 4104 of title 5.

(8) Provision of non-Federal training

(A) In general

The Director is authorized to charge and retain fees that would pay for its actual costs of the training for the following:

(i) State, local, tribal, and territorial law enforcement personnel.

(ii) Foreign law enforcement officials, including provision of such training at the International Law Enforcement Academies wherever established.

(iii) Private sector security officers, participants in the Federal Flight Deck Officer program under section 44921 of title 49, and other appropriate private sector individuals.

(B) Waiver

The Director may waive the requirement for reimbursement of any cost under this section and shall maintain records regarding the reasons for any requirements so waived.

(9) Reimbursement

The Director is authorized to reimburse travel or other expenses for non-Federal personnel who attend activities related to training sponsored by FLETC, at travel and per diem rates established by the General Services Administration.

(10) Student support

In furtherance of its training mission, the Director is authorized to provide the following support

to students:

(A) Athletic and related activities.

(B) Short-term medical services.

(C) Chaplain services.

(11) Authority to hire Federal annuitants

(A) In general

Notwithstanding any other provision of law, the Director is authorized to appoint and maintain, as necessary, Federal annuitants who have expert knowledge and experience to meet the training responsibilities under this subsection.

(B) No reduction in retirement pay

A Federal annuitant employed pursuant to this paragraph shall not be subject to any reduction in pay for annuity allocable to the period of actual employment under the provisions of section 8344 or 8468 of title 5 or similar provision of any other retirement system for employees.

(C) Re-employed annuitants

A Federal annuitant employed pursuant to this paragraph shall not be considered an employee for purposes of subchapter III of chapter 83 or chapter 84 of title 5 or such other retirement system (referred to in subparagraph (B)) as may apply.

(D) Counting

Federal annuitants shall be counted on a full time equivalent basis.

(E) Limitation

No appointment under this paragraph may be made which would result in the displacement of any employee.

(12) Travel for intermittent employees

The Director is authorized to reimburse intermittent Federal employees traveling from outside a commuting distance (to be predetermined by the Director) for travel expenses.

(e) On-FLETC housing

Notwithstanding any other provision of law, individuals attending training at any FLETC facility shall, to the extent practicable and in accordance with FLETC policy, reside in on-FLETC or FLETC-provided housing.

(f) Additional fiscal authorities

In order to further the goals and objectives of FLETC, the Director is authorized to—

(1) expend funds for public awareness and to enhance community support of law enforcement training, including the advertisement of available law enforcement training programs;

(2) accept and use gifts of property, both real and personal, and to accept gifts of services, for purposes that promote the functions of the Director pursuant to subsection (c) and the training responsibilities of the Director under subsection (d);

(3) accept reimbursement from other Federal agencies for the construction or renovation of training and support facilities and the use of equipment and technology on government owned-property; [1]

(4) obligate funds in anticipation of reimbursements from agencies receiving training at FLETC, except that total obligations at the end of a fiscal year may not exceed total budgetary resources available at the end of such fiscal year;

(5) in accordance with the purchasing authority provided under section 453a of this title—

(A) purchase employee and student uniforms; and

(B) purchase and lease passenger motor vehicles, including vehicles for police-type use;

(6) provide room and board for student interns; and

(7) expend funds each fiscal year to honor and memorialize FLETC graduates who have died in

the line of duty.

(g) Definitions

In this section:

(1) Basic training

The term "basic training" means the entry-level training required to instill in new Federal law enforcement personnel fundamental knowledge of criminal laws, law enforcement and investigative techniques, laws and rules of evidence, rules of criminal procedure, constitutional rights, search and seizure, and related issues.

(2) Detailed instructors

The term "detailed instructors" means personnel who are assigned to the Federal Law Enforcement Training Centers for a period of time to serve as instructors for the purpose of conducting basic and advanced training.

(3) Director

The term "Director" means the Director of the Federal Law Enforcement Training Centers.

(4) Distributed learning

The term "distributed learning" means education in which students take academic courses by accessing information and communicating with the instructor, from various locations, on an individual basis, over a computer network or via other technologies.

(5) Employee

The term "employee" has the meaning given such term in section 2105 of title 5.

(6) Federal agency

The term "Federal agency" means—

(A) an Executive Department as defined in section 101 of title 5;
(B) an independent establishment as defined in section 104 of title 5;
(C) a Government corporation as defined in section 9101 of title 31;
(D) the Government Printing Office;
(E) the United States Capitol Police;
(F) the United States Supreme Court Police; and
(G) Government agencies with law enforcement related duties.

(7) Law enforcement personnel

The term "law enforcement personnel" means an individual, including criminal investigators (commonly known as "agents") and uniformed police (commonly known as "officers"), who has statutory authority to search, seize, make arrests, or to carry firearms.

(8) Local

The term "local" means—

(A) of or pertaining to any county, parish, municipality, city, town, township, rural community, unincorporated town or village, local public authority, educational institution, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, any agency or instrumentality of a local government, or any other political subdivision of a State; and

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation.

(9) Partner organization

The term "partner organization" means any Federal agency participating in FLETC's training programs under a formal memorandum of understanding.

(10) State

The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(11) Student intern

The term "student intern" means any eligible baccalaureate or graduate degree student participating in FLETC's College Intern Program.

(h) Prohibition on new funding

No funds are authorized to carry out this section. This section shall be carried out using amounts otherwise appropriated or made available for such purpose.

(Pub. L. 107–296, title VIII, §884, Nov. 25, 2002, 116 Stat. 2247; Pub. L. 111–245, §2(a)(3), Sept. 30, 2010, 124 Stat. 2621; Pub. L. 114–285, §2(a), Dec. 16, 2016, 130 Stat. 1453; Pub. L. 115–278, §2(g)(5)(A), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 117–263, div. G, title LXXI, §7143(c)(2), Dec. 23, 2022, 136 Stat. 3662.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (d)(4)(A)(ii). Pub. L. 117–263 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security".

2018—Subsec. (d)(4)(A)(ii). Pub. L. 115–278 substituted "Director of Cybersecurity and Infrastructure Security" for "Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department".

2016—Pub. L. 114–285 amended section generally. Prior to amendment, section related to the Federal Law Enforcement Training Center.

2010—Subsec. (c). Pub. L. 111–245 added subsec. (c).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Government Printing Office redesignated Government Publishing Office. See section 1301(b) of Pub. L. 113–235, set out as a note preceding section 301 of Title 44, Public Printing and Documents.

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out in a note under section 650 of this title.

STANDARDS FOR MEASURING AND ASSESSING THE QUALITY AND EFFECTIVENESS OF FEDERAL LAW ENFORCEMENT TRAINING

Pub. L. 108–334, title V, §506, Oct. 18, 2004, 118 Stat. 1316, provided that: "The Federal Law Enforcement Training Center shall establish an accrediting body, to include representatives from the Federal law enforcement community and non-Federal accreditation experts involved in law enforcement training, to establish standards for measuring and assessing the quality and effectiveness of Federal law enforcement training programs, facilities, and instructors."

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 108–90, title V, §509, Oct. 1, 2003, 117 Stat. 1154.

Pub. L. 108–7, div. J, title I, §122, Feb. 20, 2003, 117 Stat. 439.

ANNUAL OUTSTANDING STUDENT AWARD

Pub. L. 108–7, div. J, title I, Feb. 20, 2003, 117 Stat. 431, provided in part: "That the [Federal Law Enforcement Training] Center is authorized to accept and use gifts of property, both real and personal, and to accept services, for authorized purposes, including funding of a gift of intrinsic value which shall be awarded

annually by the Director of the Center to the outstanding student who graduated from a basic training program at the Center during the previous fiscal year, which shall be funded only by gifts received through the Center's gift authority".

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 107–67, title I, Nov. 12, 2001, 115 Stat. 516.
Pub. L. 106–554, §1(a)(3) [title I], Dec. 21, 2000, 114 Stat. 2763, 2763A–127.
Pub. L. 106–58, title I, Sept. 29, 1999, 113 Stat. 432.
Pub. L. 105–277, div. A, §101(h) [title I], Oct. 21, 1998, 112 Stat. 2681–480, 2681–483.
Pub. L. 105–61, title I, Oct. 10, 1997, 111 Stat. 1275.
Pub. L. 104–208, div. A, title I, §101(f) [title I], Sept. 30, 1996, 110 Stat. 3009–314, 3009–317.
Pub. L. 104–52, title I, Nov. 19, 1995, 109 Stat. 470.
Pub. L. 103–329, title I, Sept. 30, 1994, 108 Stat. 2383.
Pub. L. 103–123, title I, Oct. 28, 1993, 107 Stat. 1227.
Pub. L. 102–393, title I, Oct. 6, 1992, 106 Stat. 1730.
Pub. L. 102–141, title I, Oct. 28, 1991, 105 Stat. 835.
Pub. L. 101–509, title I, Nov. 5, 1990, 104 Stat. 1390.
Pub. L. 101–136, title I, Nov. 3, 1989, 103 Stat. 784.

[1] So in original. Probably should be "Government-owned property;".

§464a. Repealed. Pub. L. 111–245, §2(b)(2), Sept. 30, 2010, 124 Stat. 2621

Section, Pub. L. 108–90, title IV, Oct. 1, 2003, 117 Stat. 1150, related to Federal Law Enforcement Training Center's acceptance and use of gifts. See section 464(f)(2) of this title.

§464b. Staffing accreditation function

In fiscal year 2004 and thereafter, the Center is authorized to accept detailees from other Federal agencies, on a non-reimbursable basis, to staff the accreditation function.

(Pub. L. 108–90, title IV, Oct. 1, 2003, 117 Stat. 1150.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Center, referred to in text, means the Federal Law Enforcement Training Center.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PRIOR PROVISIONS

Similar provisions were contained in the following prior appropriation act:
Pub. L. 108–7, div. J, title I, Feb. 20, 2003, 117 Stat. 431.

§464c. Student housing

In fiscal year 2004 and thereafter, students attending training at any Center site shall reside in on-Center or Center-provided housing, insofar as available and in accordance with Center policy.

(Pub. L. 108–90, title IV, Oct. 1, 2003, 117 Stat. 1151.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Center, referred to in text, means the Federal Law Enforcement Training Center.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PRIOR PROVISIONS

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 108–7, div. J, title I, Feb. 20, 2003, 117 Stat. 431.
Pub. L. 107–67, title I, Nov. 12, 2001, 115 Stat. 517.
Pub. L. 106–554, §1(a)(3) [title I], Dec. 21, 2000, 114 Stat. 2763, 2763A–127.
Pub. L. 106–58, title I, Sept. 29, 1999, 113 Stat. 432.
Pub. L. 105–277, div. A, §101(h) [title I], Oct. 21, 1998, 112 Stat. 2681–480, 2681–483.
Pub. L. 105–61, title I, Oct. 10, 1997, 111 Stat. 1275.
Pub. L. 104–208, div. A, title I, §101(f) [title I], Sept. 30, 1996, 110 Stat. 3009–314, 3009–317.
Pub. L. 104–52, title I, Nov. 19, 1995, 109 Stat. 470.
Pub. L. 103–329, title I, Sept. 30, 1994, 108 Stat. 2383.
Pub. L. 103–123, title I, Oct. 28, 1993, 107 Stat. 1227.
Pub. L. 102–393, title I, Oct. 6, 1992, 106 Stat. 1730.
Pub. L. 102–141, title I, Oct. 28, 1991, 105 Stat. 835.
Pub. L. 101–509, title I, Nov. 5, 1990, 104 Stat. 1390.
Pub. L. 101–136, title I, Nov. 3, 1989, 103 Stat. 784.

§464d. Additional funds for training

In fiscal year 2004 and thereafter, funds appropriated in this account shall be available, at the discretion of the Director, for the following: training United States Postal Service law enforcement personnel and Postal police officers; State and local government law enforcement training on a space-available basis; training of foreign law enforcement officials on a space-available basis with reimbursement of actual costs to this appropriation, except that reimbursement may be waived by the Secretary for law enforcement training activities in foreign countries undertaken under section 801 of the Antiterrorism and Effective Death Penalty Act of 1996 (28 U.S.C. 509 note); training of private sector security officials on a space-available basis with reimbursement of actual costs to this appropriation; and travel expenses of non-Federal personnel to attend course development meetings and training sponsored by the Center.

(Pub. L. 108–90, title IV, Oct. 1, 2003, 117 Stat. 1151.)

EDITORIAL NOTES

REFERENCES IN TEXT

"Funds appropriated in this account", and "this appropriation", referred to in text, mean funds appropriated under the headings "FEDERAL LAW ENFORCEMENT TRAINING CENTER" and "SALARIES AND EXPENSES" of title IV of the Department of Homeland Security Appropriations Act, 2004, Pub. L. 108–90.

Section 801 of the Antiterrorism and Effective Death Penalty Act of 1996, referred to in text, is section 801 of Pub. L. 104–132, which is set out as a note under section 509 of Title 28, Judiciary and Judicial Procedure.

The Center, referred to in text, means the Federal Law Enforcement Training Center.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PRIOR PROVISIONS

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 108–7, div. J, title I, Feb. 20, 2003, 117 Stat. 431.
Pub. L. 107–67, title I, Nov. 12, 2001, 115 Stat. 516.
Pub. L. 106–554, §1(a)(3) [title I], Dec. 21, 2000, 114 Stat. 2763, 2763A–127.

Pub. L. 106–58, title I, Sept. 29, 1999, 113 Stat. 432.
Pub. L. 105–277, div. A, §101(h) [title I], Oct. 21, 1998, 112 Stat. 2681–480, 2681–483.
Pub. L. 105–61, title I, Oct. 10, 1997, 111 Stat. 1276.
Pub. L. 104–208, div. A, title I, §101(f) [title I], Sept. 30, 1996, 110 Stat. 3009–314, 3009–317.
Pub. L. 104–52, title I, Nov. 19, 1995, 109 Stat. 470.
Pub. L. 103–329, title I, Sept. 30, 1994, 108 Stat. 2383.

§464e. Short-term medical services for students

In fiscal year 2004 and thereafter, the Center is authorized to provide short-term medical services for students undergoing training at the Center.

(Pub. L. 108–90, title IV, Oct. 1, 2003, 117 Stat. 1151.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Center, referred to in text, means the Federal Law Enforcement Training Center.

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PRIOR PROVISIONS

Similar provisions were contained in the following prior appropriation acts:
Pub. L. 108–7, div. J, title I, Feb. 20, 2003, 117 Stat. 431.
Pub. L. 107–67, title I, Nov. 12, 2001, 115 Stat. 517.
Pub. L. 106–554, §1(a)(3) [title I], Dec. 21, 2000, 114 Stat. 2763, 2763A–127.
Pub. L. 106–58, title I, Sept. 29, 1999, 113 Stat. 433.
Pub. L. 105–277, div. A, §101(h) [title I], Oct. 21, 1998, 112 Stat. 2681–480, 2681–483.
Pub. L. 105–61, title I, Oct. 10, 1997, 111 Stat. 1276.
Pub. L. 104–208, div. A, title I, §101(f) [title I], Sept. 30, 1996, 110 Stat. 3009–314, 3009–318.
Pub. L. 104–52, title I, Nov. 19, 1995, 109 Stat. 470.
Pub. L. 103–329, title I, Sept. 30, 1994, 108 Stat. 2384.
Pub. L. 103–123, title I, Oct. 28, 1993, 107 Stat. 1228.
Pub. L. 102–393, title I, Oct. 6, 1992, 106 Stat. 1730.

§465. Joint Interagency Task Force

(a) Establishment

The Secretary may establish and operate a permanent Joint Interagency Homeland Security Task Force composed of representatives from military and civilian agencies of the United States Government for the purposes of anticipating terrorist threats against the United States and taking appropriate actions to prevent harm to the United States.

(b) Structure

It is the sense of Congress that the Secretary should model the Joint Interagency Homeland Security Task Force on the approach taken by the Joint Interagency Task Forces for drug interdiction at Key West, Florida and Alameda, California, to the maximum extent feasible and appropriate.

(Pub. L. 107–296, title VIII, §885, Nov. 25, 2002, 116 Stat. 2247.)

§466. Sense of Congress reaffirming the continued importance and applicability of the Posse Comitatus Act

(a) Findings

Congress finds the following:

(1) Section 1385 of title 18 (commonly known as the "Posse Comitatus Act") prohibits the use of the Armed Forces as a posse comitatus to execute the laws except in cases and under circumstances expressly authorized by the Constitution or Act of Congress.

(2) Enacted in 1878, the Posse Comitatus Act was expressly intended to prevent United States Marshals, on their own initiative, from calling on the Army for assistance in enforcing Federal law.

(3) The Posse Comitatus Act has served the Nation well in limiting the use of the Armed Forces to enforce the law.

(4) Nevertheless, by its express terms, the Posse Comitatus Act is not a complete barrier to the use of the Armed Forces for a range of domestic purposes, including law enforcement functions, when the use of the Armed Forces is authorized by Act of Congress or the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection, or other serious emergency.

(5) Existing laws, including chapter 13 of title 10 (commonly known as the "Insurrection Act"), and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.), grant the President broad powers that may be invoked in the event of domestic emergencies, including an attack against the Nation using weapons of mass destruction, and these laws specifically authorize the President to use the Armed Forces to help restore public order.

(b) Sense of Congress

Congress reaffirms the continued importance of section 1385 of title 18, and it is the sense of Congress that nothing in this chapter should be construed to alter the applicability of such section to any use of the Armed Forces as a posse comitatus to execute the laws.

(Pub. L. 107–296, title VIII, §886, Nov. 25, 2002, 116 Stat. 2248; Pub. L. 115–232, div. A, title XII, §1204(a)(1), Aug. 13, 2018, 132 Stat. 2017.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a)(5), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

This chapter, referred to in subsec. (b), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2018—Subsec. (a)(5). Pub. L. 115–232 substituted "chapter 13" for "chapter 15".

§467. Coordination with the Department of Health and Human Services under the Public Health Service Act

(a) In general

The annual Federal response plan developed by the Department shall be consistent with section 319 of the Public Health Service Act (42 U.S.C. 247d).

(b) Disclosures among relevant agencies

(1) In general

Full disclosure among relevant agencies shall be made in accordance with this subsection.

(2) Public health emergency

During the period in which the Secretary of Health and Human Services has declared the existence of a public health emergency under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)), the Secretary of Health and Human Services shall keep relevant agencies, including the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation, fully and currently informed.

(3) Potential public health emergency

In cases involving, or potentially involving, a public health emergency, but in which no determination of an emergency by the Secretary of Health and Human Services under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)), has been made, all relevant agencies, including the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigation, shall keep the Secretary of Health and Human Services and the Director of the Centers for Disease Control and Prevention fully and currently informed.

(Pub. L. 107–296, title VIII, §887, Nov. 25, 2002, 116 Stat. 2248.)

§468. Preserving Coast Guard mission performance

(a) Transferred

(b) Transfer

There are transferred to the Department the authorities, functions, personnel, and assets of the Coast Guard, which shall be maintained as a distinct entity within the Department, including the authorities and functions of the Secretary of Transportation relating thereto.

(c) Maintenance of status of functions and assets

Notwithstanding any other provision of this chapter, the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts.

(d) Certain transfers prohibited

No mission, function, or asset (including for purposes of this subsection any ship, aircraft, or helicopter) of the Coast Guard may be diverted to the principal and continuing use of any other organization, unit, or entity of the Department, except for details or assignments that do not reduce the Coast Guard's capability to perform its missions.

(e) Changes to missions

(1) Prohibition

The Secretary may not substantially or significantly reduce the missions of the Coast Guard or the Coast Guard's capability to perform those missions, except as specified in subsequent Acts.

(2) Waiver

The Secretary may waive the restrictions under paragraph (1) for a period of not to exceed 90 days upon a declaration and certification by the Secretary to Congress that a clear, compelling, and immediate need exists for such a waiver. A certification under this paragraph shall include a detailed justification for the declaration and certification, including the reasons and specific information that demonstrate that the Nation and the Coast Guard cannot respond effectively if the restrictions under paragraph (1) are not waived.

(f) Direct reporting to Secretary

Upon the transfer of the Coast Guard to the Department, the Commandant shall report directly to the Secretary without being required to report through any other official of the Department.

(g) Operation as a service in the Navy

None of the conditions and restrictions in this section shall apply when the Coast Guard operates

as a service in the Navy under section 3 [1] of title 14.

(Pub. L. 107–296, title VIII, §888, Nov. 25, 2002, 116 Stat. 2249; Pub. L. 113–284, §2(b), Dec. 18, 2014, 128 Stat. 3089; Pub. L. 115–282, title VIII, §801, Dec. 4, 2018, 132 Stat. 4299; Pub. L. 119–60, div. G, title LXXII, §7201(j)(2), Dec. 18, 2025, 139 Stat. 1686.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsec. (c), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

Section 3 of title 14, referred to in subsec. (g), was redesignated section 103 of title 14 by Pub. L. 115–282, title I, §103(b), Dec. 4, 2018, 132 Stat. 4195, and references to section 3 of title 14 deemed to refer to such redesignated section, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

AMENDMENTS

2025—Subsec. (a). Pub. L. 119–60 transferred subsec. (a) of this section defining "non-homeland security missions" and "homeland security missions" to section 102 of Title 14, Coast Guard.

2018—Subsec. (h). Pub. L. 115–282 struck out subsec. (h). Text read as follows: "Not later than 90 days after November 25, 2002, the Secretary, in consultation with the Commandant of the Coast Guard, shall submit a report to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Transportation and Infrastructure of the House of Representatives, and the Committees on Appropriations of the Senate and the House of Representatives that—

"(1) analyzes the feasibility of accelerating the rate of procurement in the Coast Guard's Integrated Deepwater System from 20 years to 10 years;

"(2) includes an estimate of additional resources required;

"(3) describes the resulting increased capabilities;

"(4) outlines any increases in the Coast Guard's homeland security readiness;

"(5) describes any increases in operational efficiencies; and

"(6) provides a revised asset phase-in time line."

2014—Subsecs. (f) to (i). Pub. L. 113–284 redesignated subsecs. (g) to (i) as (f) to (h), respectively, and struck out former subsec. (f) which related to annual review.

[1] *See References in Text note below.*

§469. Fees for credentialing and background investigations in transportation

(a) Fees

For fiscal year 2004 and thereafter, the Secretary of Homeland Security shall charge reasonable fees for providing credentialing and background investigations in the field of transportation: *Provided*, That the establishment and collection of fees shall be subject to the following requirements:

(1) such fees, in the aggregate, shall not exceed the costs incurred by the Department of Homeland Security associated with providing the credential or performing the background record checks;

(2) the Secretary shall charge fees in amounts that are reasonably related to the costs of providing services in connection with the activity or item for which the fee is charged;

(3) a fee may not be collected except to the extent such fee will be expended to pay for the costs of conducting or obtaining a criminal history record check and a review of available law enforcement databases and commercial databases and records of other governmental and international agencies; reviewing and adjudicating requests for waiver and appeals of agency decisions with respect to providing the credential, performing the background record check, and

denying requests for waiver and appeals; and any other costs related to providing the credential or performing the background record check; and

(4) any fee collected shall be available for expenditure only to pay the costs incurred in providing services in connection with the activity or item for which the fee is charged and shall remain available until expended.

(b) Recurrent training of aliens in operation of aircraft

(1) Process for reviewing threat assessments

Notwithstanding section 44939(e) of title 49, the Secretary shall establish a process to ensure that an alien (as defined in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)) applying for recurrent training in the operation of any aircraft is properly identified and has not, since the time of any prior threat assessment conducted pursuant to section 44939(a) of such title, become a risk to aviation or national security.

(2) Interruption of training

If the Secretary determines, in carrying out the process established under paragraph (1), that an alien is a present risk to aviation or national security, the Secretary shall immediately notify the person providing the training of the determination and that person shall not provide the training or if such training has commenced that person shall immediately terminate the training.

(3) Fees

The Secretary may charge reasonable fees under subsection (a) for providing credentialing and background investigations for aliens in connection with the process for recurrent training established under paragraph (1). Such fees shall be promulgated by notice in the Federal Register.

(Pub. L. 108–90, title V, §520, Oct. 1, 2003, 117 Stat. 1156; Pub. L. 110–329, div. D, title V, §543, Sept. 30, 2008, 122 Stat. 3689.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2008—Pub. L. 110–329 designated existing provisions as subsec. (a), inserted heading, and added subsec. (b).

§469a. Collection of fees from non-Federal participants in meetings

For fiscal year 2010 and thereafter, the Secretary of Homeland Security may collect fees from any non-Federal participant in a conference, seminar, exhibition, symposium, or similar meeting conducted by the Department of Homeland Security in advance of the conference, either directly or by contract, and those fees shall be credited to the appropriation or account from which the costs of the conference, seminar, exhibition, symposium, or similar meeting are paid and shall be available to pay the costs of the Department of Homeland Security with respect to the conference or to reimburse the Department for costs incurred with respect to the conference: *Provided*, That in the event the total amount of fees collected with respect to a conference exceeds the actual costs of the Department of Homeland Security with respect to the conference, the amount of such excess shall be deposited into the Treasury as miscellaneous receipts: *Provided further*, That the Secretary shall provide a report to the Committees on Appropriations of the Senate and the House of Representatives not later than January 5, 2011, providing the level of collections and a summary by agency of the purposes and levels of expenditures for the prior fiscal year,.[1]

(Pub. L. 111–83, title V, §554, Oct. 28, 2009, 123 Stat. 2179; Pub. L. 114–113, div. F, title V,

§510(c), Dec. 18, 2015, 129 Stat. 2514.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2010, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2015—Pub. L. 114–113 struck out "and shall report annually thereafter" before period at end.

[1] *So in original.*

§470. Disclosures regarding homeland security grants

(a) Definitions

In this section:

(1) Homeland security grant

The term "homeland security grant" means any grant made or administered by the Department, including—

(A) the State Homeland Security Grant Program;
(B) the Urban Area Security Initiative Grant Program;
(C) the Law Enforcement Terrorism Prevention Program;
(D) the Citizen Corps; and
(E) the Metropolitan Medical Response System.

(2) Local government

The term "local government" has the meaning given the term in section 101 of this title.

(b) Required disclosures

Each State or local government that receives a homeland security grant shall, not later than 12 months after the later of October 13, 2006, and the date of receipt of such grant, and every 12 months thereafter until all funds provided under such grant are expended, submit a report to the Secretary that contains a list of all expenditures made by such State or local government using funds from such grant.

(Pub. L. 109–347, title VII, §702, Oct. 13, 2006, 120 Stat. 1943.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of "Department" and "Secretary" as used in this section, see section 901 of this title.

§471. Annual ammunition report

(a) The Secretary of Homeland Security shall submit to Congress, 180 days after January 17, 2014, and annually thereafter beginning with the submission of the President's budget proposal for

fiscal year 2016 pursuant to section 1105(a) of title 31, a comprehensive report on the purchase and usage of ammunition, subdivided by ammunition type. The report shall include—

(1) the quantity of ammunition in inventory at the end of the preceding calendar year, and the amount of ammunition expended and purchased, subdivided by ammunition type, during the year for each relevant component or agency in the Department of Homeland Security;

(2) a description of how such quantity, usage, and purchase aligns to each component or agency's mission requirements for certification, qualification, training, and operations; and

(3) details on all contracting practices applied by the Department of Homeland Security, including comparative details regarding other contracting options with respect to cost and availability.

(b) The reports required by subsection (a) shall be submitted in an appropriate format in order to ensure the safety of law enforcement personnel.

(Pub. L. 113–76, div. F, title V, §569, Jan. 17, 2014, 128 Stat. 286.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the appropriation act cited in the credit of this section, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§472. Annual weaponry report

(a) The Secretary of Homeland Security shall submit to the Congress, not later than 180 days after March 4, 2015, and annually thereafter, beginning at the time the President's budget proposal for fiscal year 2017 is submitted pursuant to section 1105(a) of title 31, a comprehensive report on the purchase and usage of weapons, subdivided by weapon type. The report shall include—

(1) the quantity of weapons in inventory at the end of the preceding calendar year, and the amount of weapons, subdivided by weapon type, included in the budget request for each relevant component or agency in the Department of Homeland Security;

(2) a description of how such quantity and purchase aligns to each component or agency's mission requirements for certification, qualification, training, and operations; and

(3) details on all contracting practices applied by the Department of Homeland Security, including comparative details regarding other contracting options with respect to cost and availability.

(b) The reports required by subsection (a) shall be submitted in an appropriate format in order to ensure the safety of law enforcement personnel.

(Pub. L. 114–4, title V, §562, Mar. 4, 2015, 129 Stat. 72.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the appropriation act cited in the credit of this section, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§473. Cyber Crimes Center, Child Exploitation Investigations Unit, Computer Forensics Unit, and Cyber Crimes Unit

(a) Cyber Crimes Center

(1) In general

The Secretary shall operate, within United States Immigration and Customs Enforcement, Homeland Security Investigations, a Cyber Crimes Center (referred to in this section as the "Center").

(2) Purpose

The Center shall provide investigative assistance, training, and equipment to support domestic and international investigations of cyber-related crimes by the Department.

(b) Child Exploitation Investigations Unit

(1) In general

The Secretary shall operate, within the Center, a Child Exploitation Investigations Unit (referred to in this subsection as the "CEIU").

(2) Functions

The CEIU—

(A) shall coordinate all United States Immigration and Customs Enforcement child exploitation initiatives, including investigations into—

(i) child exploitation;
(ii) child pornography;
(iii) child victim identification;
(iv) traveling child sex offenders; and
(v) forced child labor, including the sexual exploitation of minors;

(B) shall, among other things, focus on—

(i) child exploitation prevention;
(ii) investigative capacity building;
(iii) enforcement operations; and
(iv) training for Federal, State, local, tribal, and foreign law enforcement agency personnel, upon request;

(C) shall provide training, technical expertise, support, or coordination of child exploitation investigations, as needed, to cooperating law enforcement agencies and personnel, which shall include participating in training for Homeland Security Investigations personnel conducted by Internet Crimes Against Children Task Forces;

(D) shall provide psychological support and counseling services for United States Immigration and Customs Enforcement personnel engaged in child exploitation prevention initiatives, including making available other existing services to assist employees who are exposed to child exploitation material during investigations;

(E) is authorized to collaborate with the Department of Defense and the National Association to Protect Children for the purpose of the recruiting, training, equipping and hiring of wounded, ill, and injured veterans and transitioning service members, through the Human Exploitation Rescue Operative (HERO) Child Rescue Corps program [1]; and

(F) shall collaborate with other governmental, nongovernmental, and nonprofit entities approved by the Secretary for the sponsorship of, and participation in, outreach and training activities.

(3) Data collection

The CEIU shall collect and maintain data concerning—

(A) the total number of suspects identified by United States Immigration and Customs Enforcement;

(B) the number of arrests by United States Immigration and Customs Enforcement in child exploitation investigations, disaggregated by type, including—

(i) the number of child victims identified through investigations carried out by United States Immigration and Customs Enforcement; and

(ii) the number of suspects arrested who were in positions of trust or authority over children;

(C) the number of child exploitation cases opened for investigation by United States Immigration and Customs Enforcement; and

(D) the number of child exploitation cases resulting in a Federal, State, foreign, or military prosecution.

(4) Availability of data to Congress

In addition to submitting the reports required under paragraph (7), the CEIU shall make the data collected and maintained under paragraph (3) available to the committees of Congress described in paragraph (7).

(5) Cooperative agreements

The CEIU is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraphs (2) and (3).

(6) Acceptance of gifts

(A) In general

The Secretary is authorized to accept monies and in-kind donations from the Virtual Global Taskforce, national laboratories, Federal agencies, not-for-profit organizations, and educational institutions to create and expand public awareness campaigns in support of the functions of the CEIU.

(B) Exemption from Federal Acquisition Regulation

Gifts authorized under subparagraph (A) shall not be subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in such subparagraph are donated or of minimal cost to the Department.

(7) Reports

Not later than 1 year after May 29, 2015, and annually for the following 4 years, the CEIU shall—

(A) submit a report containing a summary of the data collected pursuant to paragraph (3) during the previous year to—

(i) the Committee on Homeland Security and Governmental Affairs of the Senate;
(ii) the Committee on the Judiciary of the Senate;
(iii) the Committee on Appropriations of the Senate;
(iv) the Committee on Homeland Security of the House of Representatives;
(v) the Committee on the Judiciary of the House of Representatives; and
(vi) the Committee on Appropriations of the House of Representatives; and

(B) make a copy of each report submitted under subparagraph (A) publicly available on the website of the Department.

(c) Computer Forensics Unit

(1) In general

The Secretary shall operate, within the Center, a Computer Forensics Unit (referred to in this subsection as the "CFU").

(2) Functions

The CFU—

(A) shall provide training and technical support in digital forensics and administer the Digital Forensics and Document and Media Exploitation program to—

(i) United States Immigration and Customs Enforcement personnel; and
(ii) Federal, State, local, tribal, military, and foreign law enforcement agency personnel

engaged in the investigation of crimes within their respective jurisdictions, upon request and subject to the availability of funds;

(B) shall provide computer hardware, software, and forensic licenses for all computer forensics personnel within United States Immigration and Customs Enforcement;

(C) shall participate in research and development in the area of digital forensics and emerging technologies, in coordination with appropriate components of the Department; and

(D) is authorized to collaborate with the Department of Defense, the National Association to Protect Children, and other governmental entities for the purpose of recruiting, training, equipping, and hiring wounded, ill, and injured veterans and transitioning service members, through the Human Exploitation Rescue Operative (HERO) Child Rescue Corps program [1].

(3) Cooperative agreements

The CFU is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(4) Acceptance of gifts

(A) In general

The Secretary is authorized to accept monies and in-kind donations from the Virtual Global Task Force, national laboratories, Federal agencies, not-for-profit organizations, and educational institutions to create and expand public awareness campaigns in support of the functions of the CFU.

(B) Exemption from Federal Acquisition Regulation

Gifts authorized under subparagraph (A) shall not be subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in such subparagraph are donated or of minimal cost to the Department.

(d) Cyber Crimes Unit

(1) In general

The Secretary shall operate, within the Center, a Cyber Crimes Unit (referred to in this subsection as the "CCU").

(2) Functions

The CCU—

(A) shall oversee the cyber security strategy and cyber-related operations and programs for United States Immigration and Customs Enforcement;

(B) shall enhance United States Immigration and Customs Enforcement's ability to combat criminal enterprises operating on or through the Internet, with specific focus in the areas of—

(i) cyber economic crime;

(ii) digital theft of intellectual property;

(iii) illicit e-commerce (including hidden marketplaces);

(iv) Internet-facilitated proliferation of arms and strategic technology; and

(v) cyber-enabled smuggling and money laundering;

(C) shall provide training and technical support in cyber investigations to—

(i) United States Immigration and Customs Enforcement personnel; and

(ii) Federal, State, local, tribal, military, and foreign law enforcement agency personnel engaged in the investigation of crimes within their respective jurisdictions, upon request and subject to the availability of funds;

(D) shall participate in research and development in the area of cyber investigations, in coordination with appropriate components of the Department; and

(E) is authorized to recruit participants of the Human Exploitation Rescue Operative (HERO)

Child Rescue Corps program [1] for investigative and forensic positions in support of the functions of the CCU.

(3) Cooperative agreements

The CCU is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(e) HERO Child-Rescue Corps [2]

(1) Establishment

(A) In general

There is established within the Center a Human Exploitation Rescue Operation [3] Child-Rescue Corps Program (referred to in this section as the "HERO Child-Rescue Corps Program"), which shall be a Department-wide program, in collaboration with the Department of Defense and the National Association to Protect Children.

(B) Private sector collaboration

As part of the HERO Child-Rescue Corps Program, the National Association to Protect Children shall provide logistical support for program participants.

(2) Purpose

The purpose of the HERO Child-Rescue Corps Program shall be to recruit, train, equip, and employ members of the Armed Forces on active duty and wounded, ill, and injured veterans to combat and prevent child exploitation, including in investigative, intelligence, analyst, inspection, and forensic positions or any other positions determined appropriate by the employing agency.

(3) Functions

The HERO Child-Rescue Program shall—

(A) provide, recruit, train, and equip participants of the Program in the areas of digital forensics, investigation, analysis, intelligence, and victim identification, as determined by the Center and the needs of the Department; and

(B) ensure that during the internship period, participants of the Program are assigned to investigate and analyze—

(i) child exploitation;
(ii) child pornography;
(iii) unidentified child victims;
(iv) human trafficking;
(v) traveling child sex offenders; and
(vi) forced child labor, including the sexual exploitation of minors.

(f) Paid internship and hiring program

(1) In general

The Secretary shall establish a paid internship and hiring program for the purpose of placing participants of the HERO Child-Rescue Corps Program (in this subsection referred to as "participants") into paid internship positions, for the subsequent appointment of the participants to permanent positions, as described in the guidelines promulgated under paragraph (3).

(2) Internship positions

Under the paid internship and hiring program required to be established under paragraph (1), the Secretary shall assign or detail participants to positions within United States Immigration and Customs Enforcement or any other Federal agency in accordance with the guidelines promulgated under paragraph (3).

(3) Placement

(A) In general

The Secretary shall promulgate guidelines for assigning or detailing participants to positions within United States Immigration and Customs Enforcement and other Federal agencies, which shall include requirements for internship duties and agreements regarding the subsequent appointment of the participants to permanent positions.

(B) Preference

The Secretary shall give a preference to Homeland Security Investigations in assignments or details under the guidelines promulgated under subparagraph (A).

(4) Term of internship

An appointment to an internship position under this subsection shall be for a term not to exceed 12 months.

(5) Rate and term of pay

After completion of initial group training and upon beginning work at an assigned office, a participant appointed to an internship position under this subsection who is not receiving monthly basic pay as a member of the Armed Forces on active duty shall receive compensation at a rate that is—

(A) not less than the minimum rate of basic pay payable for a position at level GS–5 of the General Schedule; and

(B) not more than the maximum rate of basic pay payable for a position at level GS–7 of the General Schedule.

(6) Eligibility

In establishing the paid internship and hiring program required under paragraph (1), the Secretary shall ensure that the eligibility requirements for participation in the internship program are the same as the eligibility requirements for participation in the HERO Child-Rescue Corps Program.

(7) Hero Corps hiring

The Secretary shall establish within Homeland Security Investigations positions, which shall be in addition to any positions in existence on December 21, 2019, for the hiring and permanent employment of graduates of the paid internship program required to be established under paragraph (1).

(g) Authorization of appropriations

(1) In general

There are authorized to be appropriated to the Secretary such sums as are necessary to carry out this section.

(2) Allocation

Of the amount made available pursuant to paragraph (1) in each of fiscal years 2022 through 2027, not more than $10,000,000 shall be used to carry out subsection (e) and not less than $2,000,000 shall be used to carry out subsection (f).

(Pub. L. 107–296, title VIII, §890A, as added Pub. L. 114–22, title III, §302(b)(1), May 29, 2015, 129 Stat. 251; amended Pub. L. 115–392, §23(a), (b), Dec. 21, 2018, 132 Stat. 5261, 5262; Pub. L. 117–347, title I, §105(b), Jan. 5, 2023, 136 Stat. 6203.)

EDITORIAL NOTES

AMENDMENTS

2023—Subsec. (g)(2). Pub. L. 117–347 substituted "2022 through 2027" for "2019 through 2022".

2018—Subsec. (a)(1). Pub. L. 115–392, §23(a)(1)(A), inserted "Homeland Security Investigations," after "Customs Enforcement,".

Subsec. (a)(2). Pub. L. 115–392, §23(a)(1)(B), added par. (2) and struck out former par. (2). Prior to amendment, text read as follows: "The purpose of the Center shall be to provide investigative assistance,

training, and equipment to support United States Immigration and Customs Enforcement's domestic and international investigations of cyber-related crimes."

Subsec. (b)(2)(C). Pub. L. 115–392, §23(a)(2)(A), inserted ", which shall include participating in training for Homeland Security Investigations personnel conducted by Internet Crimes Against Children Task Forces" after "agencies and personnel".

Subsec. (b)(3)(B). Pub. L. 115–392, §23(a)(2)(B)(i)(I), inserted "in child exploitation investigations" after "Enforcement" in introductory provisions.

Subsec. (b)(3)(B)(i). Pub. L. 115–392, §23(a)(2)(B)(i)(II), inserted "child" before "victims".

Subsec. (b)(3)(C), (D). Pub. L. 115–392, §23(a)(2)(B)(ii), (iii), inserted "child exploitation" after "number of".

Subsec. (c)(2)(A). Pub. L. 115–392, §23(a)(3)(A), inserted "and administer the Digital Forensics and Document and Media Exploitation program" after "forensics" in introductory provisions.

Subsec. (c)(2)(C). Pub. L. 115–392, §23(a)(3)(B), inserted "and emerging technologies" after "forensics".

Subsec. (c)(2)(D). Pub. L. 115–392, §23(a)(3)(C), substituted ", the National Association to Protect Children, and other governmental entities" for "and the National Association to Protect Children".

Subsecs. (e), (f). Pub. L. 115–392, §23(b)(2), added subsecs. (e) and (f). Former subsec. (e) redesignated (g).

Subsec. (g). Pub. L. 115–392, §23(b)(1), (3), redesignated subsec. (e) as (g), inserted par. (1) designation and heading, and added par. (2).

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 114–22, title III, §302(a), May 29, 2015, 129 Stat. 251, provided that: "Congress finds the following:

> "(1) The illegal market for the production and distribution of child abuse imagery is a growing threat to children in the United States. International demand for this material creates a powerful incentive for the rape, abuse, and torture of children within the United States.
>
> "(2) The targeting of United States children by international criminal networks is a threat to the homeland security of the United States. This threat must be fought with trained personnel and highly specialized counter-child-exploitation strategies and technologies.
>
> "(3) The United States Immigration and Customs Enforcement of the Department of Homeland Security serves a critical national security role in protecting the United States from the growing international threat of child exploitation and human trafficking.
>
> "(4) The Cyber Crimes Center of the United States Immigration and Customs Enforcement is a vital national resource in the effort to combat international child exploitation, providing advanced expertise and assistance in investigations, computer forensics, and victim identification.
>
> "(5) The returning military heroes of the United States possess unique and valuable skills that can assist law enforcement in combating global sexual and child exploitation, and the Department of Homeland Security should use this national resource to the maximum extent possible.
>
> "(6) Through the Human Exploitation Rescue Operative (HERO) Child Rescue Corps program, the returning military heroes of the United States are trained and hired to investigate crimes of child exploitation in order to target predators and rescue children from sexual abuse and slavery."

[1] *So in original. Probably should be "Program".*

[2] *So in original. "Program" probably should be inserted at end of heading.*

[3] *So in original. Probably should be "Operative".*

§474. Homeland security critical domain research and development

(a) In general

(1) Research and development

The Secretary is authorized to conduct research and development to—

(A) identify United States critical domains for economic security and homeland security; and

(B) evaluate the extent to which disruption, corruption, exploitation, or dysfunction of any of such domain poses a substantial threat to homeland security.

(2) Requirements

(A) Risk analysis of critical domains

The research under paragraph (1) shall include a risk analysis of each identified United States critical domain for economic security to determine the degree to which there exists a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such domain. Such research shall consider, to the extent possible, the following:

(i) The vulnerability and resilience of relevant supply chains.

(ii) Foreign production, processing, and manufacturing methods.

(iii) Influence of malign economic actors.

(iv) Asset ownership.

(v) Relationships within the supply chains of such domains.

(vi) The degree to which the conditions referred to in clauses (i) through (v) would place such a domain at risk of disruption, corruption, exploitation, or dysfunction.

(B) Additional research into high-risk critical domains

Based on the identification and risk analysis of United States critical domains for economic security pursuant to paragraph (1) and subparagraph (A) of this paragraph, respectively, the Secretary may conduct additional research into those critical domains, or specific elements thereof, with respect to which there exists the highest degree of a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such a domain. For each such high-risk domain, or element thereof, such research shall—

(i) describe the underlying infrastructure and processes;

(ii) analyze present and projected performance of industries that comprise or support such domain;

(iii) examine the extent to which the supply chain of a product or service necessary to such domain is concentrated, either through a small number of sources, or if multiple sources are concentrated in one geographic area;

(iv) examine the extent to which the demand for supplies of goods and services of such industries can be fulfilled by present and projected performance of other industries, identify strategies, plans, and potential barriers to expand the supplier industrial base, and identify the barriers to the participation of such other industries;

(v) consider each such domain's performance capacities in stable economic environments, adversarial supply conditions, and under crisis economic constraints;

(vi) identify and define needs and requirements to establish supply resiliency within each such domain; and

(vii) consider the effects of sector consolidation, including foreign consolidation, either through mergers or acquisitions, or due to recent geographic realignment, on such industries' performances.

(3) Consultation

In conducting the research under paragraph (1) and subparagraph (B) of paragraph (2), the Secretary may consult with appropriate Federal agencies, State agencies, and private sector stakeholders.

(4) Publication

Beginning one year after December 27, 2021, the Secretary shall publish a report containing information relating to the research under paragraph (1) and subparagraph (B) of paragraph (2), including findings, evidence, analysis, and recommendations. Such report shall be updated annually through 2026.

(b) Submission to Congress

Not later than 90 days after the publication of each report required under paragraph (4) of subsection (a), the Secretary shall transmit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate each such report, together with a description of actions the Secretary, in consultation with appropriate Federal agencies, will undertake or has undertaken in response to each such report.

(c) Definitions

In this section:

(1) United states critical domains for economic security

The term "United States critical domains for economic security" means the critical infrastructure and other associated industries, technologies, and intellectual property, or any combination thereof, that are essential to the economic security of the United States.

(2) Economic security

The term "economic security" means the condition of having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values.

(d) Authorization of appropriations

There is authorized to be appropriated $1,000,000 for each of fiscal years 2022 through 2026 to carry out this section.

(Pub. L. 107–296, title VIII, §890B, as added Pub. L. 117–81, div. F, title LXIV, §6409(a), Dec. 27, 2021, 135 Stat. 2406.)

§475. Transnational Criminal Investigative Units

(a) In general

The Secretary, with the concurrence of the Secretary of State, shall operate Transnational Criminal Investigative Units within Homeland Security Investigations.

(b) Composition

Each Transnational Criminal Investigative Unit shall be composed of trained foreign law enforcement officials who shall collaborate with Homeland Security Investigations to investigate and prosecute individuals involved in transnational criminal activity.

(c) Vetting requirement

(1) In general

Before entry into a Transnational Criminal Investigative Unit, and at periodic intervals while serving in such a unit, foreign law enforcement officials shall be required to pass certain security evaluations, which may include a background check, a polygraph examination, a urinalysis test, or other measures that the Secretary determines to be appropriate.

(2) Leahy vetting required

No member of a foreign law enforcement unit may join a Transnational Criminal Investigative Unit if the Secretary, in coordination with the Secretary of State, has credible information that such foreign law enforcement unit has committed a gross violation of human rights, consistent with the limitations set forth in section 2378d of title 22.

(3) Approval and concurrence

The establishment and continued support of the Transnational Criminal Investigative Units who are assigned under paragraph (1)—

(A) shall be performed with the approval of the chief of mission to the foreign country to which the personnel are assigned;

(B) shall be consistent with the duties and powers of the Secretary of State and the chief of mission for a foreign country under section 4802 of title 22 and section 3927 of title 22, respectively; and

(C) shall not be established without the concurrence of the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs.

(4) Report

The Executive Associate Director of Homeland Security Investigations shall submit a report to the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on the Judiciary of the House of Representatives that describes—

(A) the procedures used for vetting Transnational Criminal Investigative Unit members to include compliance with the vetting required under this subsection; and

(B) any additional measures that should be implemented to prevent personnel in vetted units from being compromised by criminal organizations.

(d) Monetary stipend

The Executive Associate Director of Homeland Security Investigations is authorized to pay vetted members of a Transnational Criminal Investigative Unit a monetary stipend in an amount associated with their duties dedicated to unit activities.

(e) Annual briefing

The Executive Associate Director of Homeland Security Investigations, during the 5-year period beginning on December 23, 2022, shall provide an annual unclassified briefing to the congressional committees referred to in subsection (c)(4), which may include a classified session, if necessary, that identifies—

(1) the number of vetted members of Transnational Criminal Investigative Unit in each country;

(2) the amount paid in stipends to such members, disaggregated by country;

(3) relevant enforcement statistics, such as arrests and progress made on joint investigations, in each such country; and

(4) whether any vetted members of the Transnational Criminal Investigative Unit in each country were involved in any unlawful activity, including human rights abuses or significant acts of corruption.

(Pub. L. 107–296, title VIII, §890C, as added Pub. L. 117–263, div. G, title LXXI, §7105(b)(1), Dec. 23, 2022, 136 Stat. 3623.)

§475a. Mentor-protégé program

(a) Establishment

There is established in the Department a mentor-protégé program (in this section referred to as the "Program") under which a mentor firm enters into an agreement with a protégé firm for the purpose of assisting the protégé firm to compete for prime contracts and subcontracts of the Department.

(b) Eligibility

The Secretary shall establish criteria for mentor firms and protégé firms to be eligible to participate in the Program, including a requirement that a firm is not included on any list maintained by the Federal Government of contractors that have been suspended or debarred.

(c) Program application and approval

(1) Application

The Secretary, acting through the Office of Small and Disadvantaged Business Utilization of the Department, shall establish a process for submission of an application jointly by a mentor firm

and the protégé firm selected by the mentor firm. The application shall include each of the following:

(A) A description of the assistance to be provided by the mentor firm, including, to the extent available, the number and a brief description of each anticipated subcontract to be awarded to the protégé firm.

(B) A schedule with milestones for achieving the assistance to be provided over the period of participation in the Program.

(C) An estimate of the costs to be incurred by the mentor firm for providing assistance under the Program.

(D) Attestations that Program participants will submit to the Secretary reports at times specified by the Secretary to assist the Secretary in evaluating the protégé firm's developmental progress.

(E) Attestations that Program participants will inform the Secretary in the event of a change in eligibility or voluntary withdrawal from the Program.

(2) Approval

Not later than 60 days after receipt of an application pursuant to paragraph (1), the head of the Office of Small and Disadvantaged Business Utilization shall notify applicants of approval or, in the case of disapproval, the process for resubmitting an application for reconsideration.

(3) Rescission

The head of the Office of Small and Disadvantaged Business Utilization may rescind the approval of an application under this subsection if it determines that such action is in the best interest of the Department.

(d) Program duration

A mentor firm and protégé firm approved under subsection (c) shall enter into an agreement to participate in the Program for a period of not less than 36 months.

(e) Program benefits

A mentor firm and protégé firm that enter into an agreement under subsection (d) may receive the following Program benefits:

(1) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive evaluation credit for participating in the Program.

(2) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive credit for a protégé firm performing as a first tier subcontractor or a subcontractor at any tier in an amount equal to the total dollar value of any subcontracts awarded to such protégé firm.

(3) A protégé firm may receive technical, managerial, financial, or any other mutually agreed upon benefit from a mentor firm, including a subcontract award.

(f) Reporting

Not later than one year after December 23, 2022, and annually thereafter, the head of the Office of Small and Disadvantaged Business Utilization shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Homeland Security and the Committee on Small Business of the House of Representatives a report that—

(1) identifies each agreement between a mentor firm and a protégé firm entered into under this section, including the number of protégé firm participants that are—

(A) small business concerns;

(B) small business concerns owned and controlled by veterans;

(C) small business concerns owned and controlled by service-disabled veterans;

(D) qualified HUBZone small business concerns;

(E) small business concerns owned and controlled by socially and economically disadvantaged individuals;

(F) small business concerns owned and controlled by women;
(G) historically Black colleges and universities; and
(H) minority-serving institutions;

(2) describes the type of assistance provided by mentor firms to protégé firms;
(3) identifies contracts within the Department in which a mentor firm serving as the prime contractor provided subcontracts to a protégé firm under the Program; and
(4) assesses the degree to which there has been—
(A) an increase in the technical capabilities of protégé firms; and
(B) an increase in the quantity and estimated value of prime contract and subcontract awards to protégé firms for the period covered by the report.

(g) Rule of construction

Nothing in this section may be construed to limit, diminish, impair, or otherwise affect the authority of the Department to participate in any program carried out by or requiring approval of the Small Business Administration or adopt or follow any regulation or policy that the Administrator of the Small Business Administration may promulgate, except that, to the extent that any provision of this section (including subsection (h)) conflicts with any other provision of law, regulation, or policy, this section shall control.

(h) Definitions

In this section:

(1) Historically Black college or university

The term "historically Black college or university" has the meaning given the term "part B institution" in section 1061 of title 20.

(2) Mentor firm

The term "mentor firm" means a for-profit business concern that is not a small business concern that—
(A) has the ability to assist and commits to assisting a protégé to compete for Federal prime contracts and subcontracts; and
(B) satisfies any other requirements imposed by the Secretary.

(3) Minority-serving institution

The term "minority-serving institution" means an institution of higher education described in section 1067q(a) of title 20.[1]

(4) Protégé firm

The term "protégé firm" means a small business concern, a historically Black college or university, or a minority-serving institution that—
(A) is eligible to enter into a prime contract or subcontract with the Department; and
(B) satisfies any other requirements imposed by the Secretary.

(5) Small Business Act definitions

The terms "small business concern", "small business concern owned and controlled by veterans", "small business concern owned and controlled by service-disabled veterans", "qualified HUBZone small business concern", "and small [2] business concern owned and controlled by women" have the meanings given such terms, respectively, under section 632 of title 15. The term "small business concern owned and controlled by socially and economically disadvantaged individuals" has the meaning given such term in section 637(d)(3)(C) of title 15.

(Pub. L. 107–296, title VIII, §890D, as added Pub. L. 117–263, div. G, title LXXI, §7115(a), Dec. 23, 2022, 136 Stat. 3634.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1067q(a) of title 20, referrred to in subsec. (h)(3), was in the original "section 317 of the Higher Education Act of 1965 (20 U.S.C. 1067q(a))" and was translated as reading "section 371(a) of the Higher Education Act of 1965", to reflect the probable intent of Congress.

[1] See References in Text note below.

[2] So in original. The opening quotation marks preceding "and" probably should precede "small".

PART I—INFORMATION SHARING

§481. Short title; findings; and sense of Congress

(a) Short title

This part may be cited as the "Homeland Security Information Sharing Act".

(b) Findings

Congress finds the following:

(1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.

(2) The Federal Government relies on State and local personnel to protect against terrorist attack.

(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.

(4) Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information.

(6) Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.

(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) Increased efforts to share homeland security information should avoid duplicating existing information systems.

(c) Sense of Congress

It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and

rural communities.

(Pub. L. 107–296, title VIII, §891, Nov. 25, 2002, 116 Stat. 2252.)

EDITORIAL NOTES

REFERENCES IN TEXT

This part, referred to in subsec. (a), was in the original "This subtitle", meaning subtitle I (§§891–899) of title VIII of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2252, which enacted this part, amended section 2517 of Title 18, Crimes and Criminal Procedure, Rule 6 of the Federal Rules of Criminal Procedure, set out in the Appendix to Title 18, and sections 1806, 1825, and 3365 of Title 50, War and National Defense, and amended provisions set out as a note under section 2517 of Title 18. For complete classification of subtitle I to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

REPORTS TO CONGRESS

Pub. L. 110–28, title III, May 25, 2007, 121 Stat. 139, provided in part: "That starting July 1, 2007, the Secretary of Homeland Security shall submit quarterly reports to the Committees on Appropriations of the Senate and the House of Representatives detailing the information required in House Report 110–107."

§482. Facilitating homeland security information sharing procedures

(a) Procedures for determining extent of sharing of homeland security information

(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) Procedures for sharing of homeland security information

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.

(2) Each information sharing system through which information is shared under paragraph (1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.

(c) Sharing of classified information and sensitive but unclassified information with State and local personnel

(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a).

(2) It is the sense of Congress that such procedures may include 1 or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph (B) in order to assist such officials in—

(i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;

(ii) reporting information relating to such potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;

(iii) assuring that all reported information is systematically submitted to and passed on by the

Department for use by appropriate Federal agencies; and

(iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.

(B) The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.

(C) The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107–56; 28 U.S.C. 509 note).

(D) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.

(d) Responsible officials

For each affected Federal agency, the head of such agency shall designate an official to administer this chapter with respect to such agency.

(e) Federal control of information

Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.

(f) Definitions

As used in this section:

(1) The term "homeland security information" means any information possessed by a Federal, State, or local agency that—

(A) relates to the threat of terrorist activity;

(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;

(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or

(D) would improve the response to a terrorist act.

(2) The term "intelligence community" has the meaning given such term in section 3003(4) of title 50.

(3) The term "State and local personnel" means any of the following persons involved in prevention, preparation, or response for terrorist attack:

(A) State Governors, mayors, and other locally elected officials.

(B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.

(E) Other appropriate emergency response agency personnel.

(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.

(4) The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.

(g) Construction

Nothing in this chapter shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this

chapter to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

(Pub. L. 107–296, title VIII, §892, Nov. 25, 2002, 116 Stat. 2253; Pub. L. 108–177, title III, §316(a), Dec. 13, 2003, 117 Stat. 2610.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsecs. (d) and (g), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2003—Subsec. (c)(3). Pub. L. 108–177 added par. (3).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13311. HOMELAND SECURITY INFORMATION SHARING

Ex. Ord. No. 13311, July 29, 2003, 68 F.R. 45149, as amended by Ex. Ord. No. 13388, §8(a), Oct. 25, 2005, 70 F.R. 62025, provided:

By the authority vested in me by the Constitution and the laws of the United States, including sections 892 and 893 of the Homeland Security Act of 2002 (the "Act") (6 U.S.C. 482 and 483) and section 301 of title 3, United States Code, it is hereby ordered as follows:

SECTION 1. *Assignment of Functions*. (a) The functions of the President under section 892 of the Act are assigned to the Secretary of Homeland Security (the "Secretary"), except the functions of the President under subsections 892(a)(2) and 892(b)(7).

(b) Subject to section 2(b) of this order, the function of the President under section 893 of the Act is assigned to the Secretary.

(c) Procedures issued by the Secretary in the performance of the function of the President under section 892(a)(1) of the Act shall apply to all agencies of the Federal Government. Such procedures shall specify that the President may make, or may authorize another officer of the United States to make, exceptions to the procedures.

(d) The function of the President under section 892(b)(7) of the Act is delegated to the Attorney General and the Director of National Intelligence, to be exercised jointly.

(e) In performing the functions assigned to the Secretary by subsection (a) of this section, the Secretary shall coordinate with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Director of the Office of Management and Budget, the Director of National Intelligence, the Archivist of the United States, and as the Secretary deems appropriate, other officers of the United States.

(f) A determination, under the procedures issued by the Secretary in the performance of the function of the President under section 892(a)(1) of the Act, as to whether, or to what extent, an individual who falls within the category of "State and local personnel" as defined in sections 892(f)(3) and (f)(4) of the Act shall have access to information classified pursuant to [former] Executive Order 12958 of April 17, 1995, as amended, is a discretionary determination and shall be conclusive and not subject to review or appeal.

SEC. 2. *Rules of Construction*. Nothing in this order shall be construed to impair or otherwise affect:

(a) the authority of the Director of National Intelligence under section 102A(i)(1) [now 102A(h)(1)] of the National Security Act of 1947, as amended (50 U.S.C. 403–3(c)(7) [sic]) [now 50 U.S.C. 3024(h)(1)], to protect intelligence sources and methods from unauthorized disclosure;

(b) the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals; or

(c) the provisions of Executive Orders 12958 of April 17, 1995 [former 50 U.S.C. 435 note], as amended, and 12968 of August 2, 1995 [50 U.S.C. 3161 note], as amended.

SEC. 3. *General Provision*. This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH.

§483. Report

(a) Report required

Not later than 12 months after November 25, 2002, the President shall submit to the congressional committees specified in subsection (b) a report on the implementation of section 482 of this title. The report shall include any recommendations for additional measures or appropriation requests, beyond the requirements of section 482 of this title, to increase the effectiveness of sharing of information between and among Federal, State, and local entities.

(b) Specified congressional committees

The congressional committees referred to in subsection (a) are the following committees:

(1) The Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

(2) The Select Committee on Intelligence and the Committee on the Judiciary of the Senate.

(Pub. L. 107–296, title VIII, §893, Nov. 25, 2002, 116 Stat. 2255.)

EXECUTIVE DOCUMENTS

DELEGATION OF FUNCTIONS

For assignment of function of President under this section, subject to certain limitations, to Secretary of Homeland Security, see Ex. Ord. No. 13311, §1(b), July 29, 2003, 68 F.R. 45149, set out as a note under section 482 of this title.

§484. Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out section 482 of this title.

(Pub. L. 107–296, title VIII, §894, Nov. 25, 2002, 116 Stat. 2256.)

§484a. Reciprocal information sharing

Acting in accordance with a bilateral or multilateral arrangement, the Secretary, in the Secretary's discretion and on the basis of reciprocity, may provide information from the National Sex Offender Registry relating to a conviction for a sex offense against a minor (as such terms are defined in section 20911 of title 34) to a foreign government upon the request of the foreign government, and may receive comparable information from the foreign government.

(Pub. L. 107–296, title VIII, §895, as added Pub. L. 117–347, title III, §323(a)(1)(B), Jan. 5, 2023, 136 Stat. 6207.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 895 of Pub. L. 107–296 amended Rule 6 of the Federal Rules of Criminal Procedure, set out in the Appendix to Title 18, Crimes and Criminal Procedure, prior to repeal by Pub. L. 117–347, title III, §323(a)(1)(A), Jan. 5, 2023, 136 Stat. 6206.

§485. Information sharing

(a) Definitions

In this section:

(1) Homeland security information

The term "homeland security information" has the meaning given that term in section 482(f) of this title.

(2) Information Sharing Council

The term "Information Sharing Council" means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

(3) Information sharing environment

The terms "information sharing environment" and "ISE" mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.

(4) Program manager

The term "program manager" means the program manager designated under subsection (f).

(5) Terrorism information

The term "terrorism information"—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(iii) communications of or by such groups or individuals; or

(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.

(6) Weapons of mass destruction information

The term "weapons of mass destruction information" means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

(b) Information sharing environment

(1) Establishment

The President shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) Attributes

The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;

(J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;

(K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as "collective and noncollective collaboration"), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

(3) Delegation

(A) In general

Subject to subparagraph (B), the President may delegate responsibility for carrying out this subsection.

(B) Limitation

The President may not delegate responsibility for carrying out this subsection to the Director of National Intelligence.

(c) Preliminary report

Not later than 180 days after December 17, 2004, the program manager shall, in consultation with the Information Sharing Council—

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) Guidelines and requirements

As soon as possible, but in no event later than 270 days after December 17, 2004, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) Implementation plan report

Not later than one year after December 17, 2004, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to

operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with—

(A) the authority of the Director of National Intelligence under this title,[1] and the amendments made by this title,[1] to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Department of Justice, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) Program manager

(1) Designation

Not later than 120 days after December 17, 2004, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. Beginning on December 20, 2019, each individual designated as the program manager shall be appointed by the Director of National Intelligence. The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) Duties and responsibilities

(A) In general

The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) Content of policies, procedures, guidelines, rules, and standards

The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) Information Sharing Council

(1) Establishment

There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

(2) Specific duties

In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles,[2] and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) Consultation

In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) Inapplicability of chapter 10 of title 5

The Information Sharing Council (including any subsidiary group of the Information Sharing Council) shall not be subject to the requirements of chapter 10 of title 5.

(5) Detailees

Upon a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).

(h) Agency responsibilities

The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(i) Report on the information sharing environment

(1) In general

Not later than 180 days after August 3, 2007, the President shall report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Homeland Security of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives on the feasibility of—

(A) eliminating the use of any marking or process (including "Originator Control") intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, between and among participants in the information sharing environment, unless the President has—

(i) specifically exempted categories of information from such elimination; and

(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph; and

(B) continuing to use Federal agency standards in effect on August 3, 2007, for the collection, sharing, and access to information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;

(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an "authorized use" standard); and

(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which—

(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and

(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information.

(2) Definition

In this subsection, the term "anonymized data" means data in which the individual to whom the data pertains is not identifiable with reasonable efforts, including information that has been

encrypted or hidden through the use of other technology.

(j) Additional positions

The program manager is authorized to hire not more than 40 full-time employees to assist the program manager in—

(1) activities associated with the implementation of the information sharing environment, including—

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (f)(2)(A)(iv).

(k) Authorization of appropriations

There is authorized to be appropriated to carry out this section $30,000,000 for each of fiscal years 2008 and 2009.

(Pub. L. 108–458, title I, §1016, Dec. 17, 2004, 118 Stat. 3664; Pub. L. 110–53, title V, §504, Aug. 3, 2007, 121 Stat. 313; Pub. L. 111–259, title VIII, §806(a)(1), Oct. 7, 2010, 124 Stat. 2748; Pub. L. 116–92, div. E, title LXIV, §6402, Dec. 20, 2019, 133 Stat. 2196; Pub. L. 116–260, div. W, title III, §307, Dec. 27, 2020, 134 Stat. 2368; Pub. L. 117–263, div. F, title LXVIII, §6811(c)(1), Dec. 23, 2022, 136 Stat. 3600; Pub. L. 117–286, §4(a)(17), Dec. 27, 2022, 136 Stat. 4307.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order 13356, referred to in subsec. (a)(2), which was formerly set out as a note below, was revoked by Ex. Ord. No. 13388, set out as a note below, which established an Information Sharing Council consistent with subsec. (g) of this section.

This title, referred to in subsec. (e)(10)(A), is title I of Pub. L. 108–458, Dec. 17, 2004, 118 Stat. 3643, known as the National Security Intelligence Reform Act of 2004. For complete classification of title I to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the National Security Intelligence Reform Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2022—Subsec. (g)(4). Pub. L. 117–286 substituted "chapter 10 of title 5" for "Federal Advisory Committee Act" in heading and "chapter 10 of title 5." for "the Federal Advisory Committee Act (5 U.S.C. App.)." in text.

Subsecs. (h) to (l). Pub. L. 117–263 redesignated subsecs. (i) to (l) as (h) to (k), respectively, and struck out former subsec. (h) which related to performance management reports.

2020—Subsec. (b)(1). Pub. L. 116–260, §307(1), substituted "President" for "Director of National Intelligence" in introductory provisions.

Subsec. (b)(2). Pub. L. 116–260, §307(2), substituted "President" for "Director of National Intelligence" in two places in introductory provisions.

Subsec. (b)(3). Pub. L. 116–260, §307(3), added par. (3).

2019—Subsec. (b)(1). Pub. L. 116–92, §6402(a)(1), substituted "Director of National Intelligence" for "President" in introductory provisions.

Subsec. (b)(2). Pub. L. 116–92, §6402(a)(2), substituted "Director of National Intelligence" for "President" in two places in introductory provisions.

Subsec. (f)(1). Pub. L. 116–92, §6402(b), substituted "Beginning on December 20, 2019, each individual designated as the program manager shall be appointed by the Director of National Intelligence." for "The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President's sole discretion)."

2010—Subsec. (e)(10)(B). Pub. L. 111–259 substituted "Department of Justice" for "Attorney General".

2007—Subsec. (a)(1), (2). Pub. L. 110–53, §504(1)(A), (B), added par. (1) and redesignated former par. (1) as (2). Former par. (2) redesignated (3).

Subsec. (a)(3). Pub. L. 110–53, §504(1)(C), added par. (3) and struck out heading and text of former par. (3). Text read as follows: "The terms 'information sharing environment' and 'ISE' mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section."

Pub. L. 110–53, §504(1)(A), redesignated par. (2) as (3). Former par. (3) redesignated (4).

Subsec. (a)(4). Pub. L. 110–53, §504(1)(A), redesignated par. (3) as (4). Former par. (4) redesignated (5).

Subsec. (a)(5). Pub. L. 110–53, §504(1)(D), added par. (5) and struck out heading and text of former par (5). Text read as follows: "The term 'terrorism information' means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

"(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

"(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

"(C) communications of or by such groups or individuals; or

"(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals."

Pub. L. 110–53, §504(1)(A), redesignated par. (4) as (5).

Subsec. (a)(6). Pub. L. 110–53, §504(1)(E), added par. (6).

Subsec. (b)(2)(J) to (O). Pub. L. 110–53, §504(2), added subpars. (J) to (O).

Subsec. (f)(1). Pub. L. 110–53, §504(3)(A), substituted "until removed from service or replaced" for "during the two-year period beginning on the date of designation under this paragraph unless sooner removed from service and replaced" and "The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law" for "The program manager shall have and exercise governmentwide authority".

Subsec. (f)(2)(A)(ii) to (v). Pub. L. 110–53, §504(3)(B), added cls. (ii) to (iv), redesignated former cl. (iii) as (v), and struck out former cl. (ii) which read as follows: "assist in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and".

Subsec. (g)(1). Pub. L. 110–53, §504(4)(A), substituted "until removed from service or replaced" for "during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1) of this section, unless sooner removed from service and replaced".

Subsec. (g)(2)(G) to (I). Pub. L. 110–53, §504(4)(B), added subpars. (G) and (H) and redesignated former subpar. (G) as (I).

Subsec. (g)(4). Pub. L. 110–53, §504(4)(C), inserted "(including any subsidiary group of the Information Sharing Council)" before "shall not be subject".

Subsec. (g)(5). Pub. L. 110–53, §504(4)(D), added par. (5).

Subsec. (h)(1). Pub. L. 110–53, §504(5), substituted "and not later than June 30 of each year thereafter" for "and annually thereafter".

Subsecs. (j) to (l). Pub. L. 110–53, §504(6), added subsecs. (j) to (l) and struck out heading and text of former subsec. (j). Text read as follows: "There is authorized to be appropriated to carry out this section $20,000,000 for each of fiscal years 2005 and 2006."

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

For determination by President that section takes effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of Title 50, War and National Defense.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see

section 1097(a) of Pub. L. 108–458, set out as an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of Title 50, War and National Defense.

PROCEDURES TO CLEAR INDIVIDUALS FROM TERRORIST DATABASE LISTS

Pub. L. 109–295, title V, §556, Oct. 4, 2006, 120 Stat. 1391, provided that: "Not later than six months after the date of enactment of this Act [Oct. 4, 2006], the Secretary of Homeland Security shall establish revised procedures for expeditiously clearing individuals whose names have been mistakenly placed on a terrorist database list or who have names identical or similar to individuals on a terrorist database list. The Secretary shall advise Congress of the procedures established."

EXECUTIVE DOCUMENTS

EXECUTIVE ORDER NO. 13356

Ex. Ord. No. 13356, Aug. 27, 2004, 69 F.R. 53599, which provided for strengthening the sharing of terrorism information to protect Americans, was revoked by Ex. Ord. No. 13388, §8(b), Oct. 25, 2005, 70 F.R. 62025, set out below.

EX. ORD. NO. 13388. FURTHER STRENGTHENING THE SHARING OF TERRORISM INFORMATION TO PROTECT AMERICANS

Ex. Ord. No. 13388, Oct. 25, 2005, 70 F.R. 62023, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458) [6 U.S.C. 485], and in order to further strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

SECTION 1. *Policy*. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and

(b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).

SEC. 2. *Duties of Heads of Agencies Possessing or Acquiring Terrorism Information*. To implement the policy set forth in section 1 of this order, the head of each agency that possesses or acquires terrorism information:

(a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency, unless otherwise directed by the President, and consistent with (i) the statutory responsibilities of the agencies providing and receiving the information; (ii) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of this order; and (iii) other applicable law, including sections 102A(g) and (i) [now 102A(f), (h)] of the National Security Act of 1947 [50 U.S.C. 3024(f), (h)], section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 [6 U.S.C. 485] (including any policies, procedures, guidelines, rules, and standards issued pursuant thereto), sections 202 and 892 of the Homeland Security Act of 2002 [6 U.S.C. 122, 482], [former] Executive Order 12958 of April 17, 1995, as amended, and Executive Order 13311 of July 29, 2003 [6 U.S.C. 482 note]; and

(b) shall cooperate in and facilitate production of reports based on terrorism information with contents and formats that permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States.

SEC. 3. *Preparing Terrorism Information for Maximum Distribution*. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the common standards for the sharing of terrorism information established pursuant to section 3 of Executive Order 13356 of August 27, 2004 [formerly set out above], shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 4. *Requirements for Collection of Terrorism Information Inside the United States*. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the

recommendations regarding the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information collected within the United States made pursuant to section 4 of Executive Order 13356 [formerly set out above] shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 5. *Establishment and Functions of Information Sharing Council*. (a) Consistent with section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004, there is hereby established an Information Sharing Council (Council), chaired by the Program Manager to whom section 1016 of such Act refers, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center; and such other heads of departments or agencies as the Director of National Intelligence may designate.

(b) The mission of the Council is to (i) provide advice and information concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of this order; and (ii) perform the duties set forth in section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004.

(c) To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the plan for establishment of a proposed interoperable terrorism information sharing environment reported under section 5(c) of Executive Order 13356 [formerly set out above] shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 6. *Definitions*. As used in this order:

(a) the term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office; and

(b) the term "terrorism information" has the meaning set forth for such term in section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 7. *General Provisions*. (a) This order:

(i) shall be implemented in a manner consistent with applicable law, including Federal law protecting the information privacy and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the authority of the principal officers of agencies as heads of their respective agencies, including under section 199 of the Revised Statutes (22 U.S.C. 2651), section 201 of the Department of Energy Organization Act (42 U.S.C. 7131), section 103 of the National Security Act of 1947 (50 U.S.C. 403–3) [now 50 U.S.C. 3025], section 102(a) of the Homeland Security Act of 2002 (6 U.S.C. 112(a)), and sections 301 of title 5, 113(b) and 162(b) of title 10, 1501 of title 15, 503 of title 28, and 301(b) of title 31, United States Code;

(iii) shall be implemented consistent with the Presidential Memorandum of June 2, 2005, on "Strengthening Information Sharing, Access, and Integration—Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment;" [not set out in the Code]

(iv) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(v) shall be implemented in a manner consistent with section 102A of the National Security Act of 1947 [50 U.S.C. 3024].

(b) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

SEC. 8. *Amendments and Revocation*. (a) [Amended Ex. Ord. No. 13311, set out as a note under section 482 of this title.]

(b) Executive Order 13356 of August 27, 2004 [formerly set out above], is hereby revoked.

GEORGE W. BUSH.

ASSIGNMENT OF CERTAIN FUNCTIONS UNDER THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

Memorandum of President of the United States, Nov. 14, 2006, 71 F.R. 67029, provided:

Memorandum for the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States, including section 301 of title 3, United States Code, the reporting function of the President under section 1016(e) of the

Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458, 118 Stat. 3638) is hereby assigned to the Director of National Intelligence (Director).

The Director shall perform such function in a manner consistent with the President's constitutional authority to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties.

Any reference in this memorandum to the provision of any Act shall be deemed to include references to any hereafter-enacted provision of law that is the same or substantially the same as such provision.

You are authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

Memorandum of President of the United States, Apr. 10, 2007, 72 F.R. 18561, provided:

Memorandum for the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States of America, including section 301 of title 3, United States Code, the functions of the President under section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458) (the "Act") are hereby assigned to the Director of National Intelligence (Director).

The Director shall perform such functions in a manner consistent with direction and guidance issued by the President, including (1) the Memorandum for the Heads of Executive Departments and Agencies of June 2, 2005, entitled "Strengthening Information Sharing, Access, and Integration—Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment," and (2) the Memorandum for the Heads of Executive Departments and Agencies of December 16, 2005, entitled "Guidelines and Requirements in Support of the Information Sharing Environment;" provided that the Director shall ensure that the official within the Office of the Director of National Intelligence previously designated as the program manager responsible for information sharing across the Federal Government pursuant to the Act shall be the assistant to the Director in carrying out the functions delegated by this memorandum.

You are authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

[Pub. L. 116–92, div. E, title LXIV, §6402(a), Dec. 20, 2019, 133 Stat. 2196, amended subsec. (b) of this section by substituting "Director of National Intelligence" for "President", thereby making the assignment of functions in the memorandum above moot.]

Memorandum of President of the United States, Sept. 8, 2007, 72 F.R. 52279, provided:

Memorandum for the Secretary of State[,] the Secretary of Defense[,] the Attorney General[,] the Secretary of Energy[,] the Secretary of Homeland Security[, and] the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States, including section 301 of title 3, United States Code, the reporting functions of the President under subsections (h) and (j) of section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53) (IRTPA), are hereby assigned to the Director of National Intelligence (Director). The Director shall consult the Secretaries of State, Defense, Energy, Homeland Security, and the Attorney General in performing such functions.

Heads of departments and agencies shall, to the extent permitted by law, furnish to the Director information that the Director requests to perform such functions, in the format and on the schedule specified by the Director.

The Director shall perform such functions in a manner consistent with the President's constitutional authority to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, and the performance of the Executive's constitutional duties.

Any reference in this memorandum to the provision of IRTPA shall be deemed to include references to any hereafter-enacted provision of law that is the same or substantially the same as such provision.

The Director is authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

[1] *See References in Text note below.*

[2] *So in original. Probably should be "rules,".*

§486. Limitation of liability

A person who has completed a security awareness training course approved by or operated under a cooperative agreement with the Department of Homeland Security using funds made available in fiscal year 2006 and thereafter or in any prior appropriations Acts, who is enrolled in a program recognized or acknowledged by an Information Sharing and Analysis Center, and who reports a situation, activity or incident pursuant to that program to an appropriate authority, shall not be liable for damages in any action brought in a Federal or State court which result from any act or omission unless such person is guilty of gross negligence or willful misconduct.

(Pub. L. 109–90, title V, §541, Oct. 18, 2005, 119 Stat. 2089.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2006, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PART J—SECURE HANDLING OF AMMONIUM NITRATE

§488. Definitions

In this part:

(1) Ammonium nitrate

The term "ammonium nitrate" means—

(A) solid ammonium nitrate that is chiefly the ammonium salt of nitric acid and contains not less than 33 percent nitrogen by weight; and

(B) any mixture containing a percentage of ammonium nitrate that is equal to or greater than the percentage determined by the Secretary under section 488a(b) of this title.

(2) Ammonium nitrate facility

The term "ammonium nitrate facility" means any entity that produces, sells or otherwise transfers ownership of, or provides application services for ammonium nitrate.

(3) Ammonium nitrate purchaser

The term "ammonium nitrate purchaser" means any person who purchases ammonium nitrate from an ammonium nitrate facility.

(Pub. L. 107–296, title VIII, §899A, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2083.)

§488a. Regulation of the sale and transfer of ammonium nitrate

(a) In general

The Secretary shall regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility in accordance with this part to prevent the misappropriation or use of ammonium nitrate in an act of terrorism. Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.

(b) Ammonium nitrate mixtures

Not later than 90 days after December 26, 2007, the Secretary, in consultation with the heads of appropriate Federal departments and agencies (including the Secretary of Agriculture), shall, after

notice and an opportunity for comment, establish a threshold percentage for ammonium nitrate in a substance.

(c) Registration of owners of ammonium nitrate facilities

(1) Registration

The Secretary shall establish a process by which any person that—

(A) owns an ammonium nitrate facility is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this part.

(2) Registration information

Any person applying to register under paragraph (1) shall submit to the Secretary—

(A) the name, address, and telephone number of each ammonium nitrate facility owned by that person;

(B) the name of the person designated by that person as the point of contact for each such facility, for purposes of this part; and

(C) such other information as the Secretary may determine is appropriate.

(d) Registration of ammonium nitrate purchasers

(1) Registration

The Secretary shall establish a process by which any person that—

(A) intends to be an ammonium nitrate purchaser is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this part.

(2) Registration information

Any person applying to register under paragraph (1) as an ammonium nitrate purchaser shall submit to the Secretary—

(A) the name, address, and telephone number of the applicant; and

(B) the intended use of ammonium nitrate to be purchased by the applicant.

(e) Records

(1) Maintenance of records

The owner of an ammonium nitrate facility shall—

(A) maintain a record of each sale or transfer of ammonium nitrate, during the two-year period beginning on the date of that sale or transfer; and

(B) include in such record the information described in paragraph (2).

(2) Specific information required

For each sale or transfer of ammonium nitrate, the owner of an ammonium nitrate facility shall—

(A) record the name, address, telephone number, and registration number issued under subsection (c) or (d) of each person that purchases ammonium nitrate, in a manner prescribed by the Secretary;

(B) if applicable, record the name, address, and telephone number of an agent acting on behalf of the person described in subparagraph (A), at the point of sale;

(C) record the date and quantity of ammonium nitrate sold or transferred; and

(D) verify the identity of the persons described in subparagraphs (A) and (B), as applicable, in accordance with a procedure established by the Secretary.

(3) Protection of information

In maintaining records in accordance with paragraph (1), the owner of an ammonium nitrate facility shall take reasonable actions to ensure the protection of the information included in such records.

(f) Exemption for explosive purposes

The Secretary may exempt from this part a person producing, selling, or purchasing ammonium nitrate exclusively for use in the production of an explosive under a license or permit issued under chapter 40 of title 18.

(g) Consultation

In carrying out this section, the Secretary shall consult with the Secretary of Agriculture, States, and appropriate private sector entities, to ensure that the access of agricultural producers to ammonium nitrate is not unduly burdened.

(h) Data confidentiality

(1) In general

Notwithstanding section 552 of title 5 or the USA PATRIOT ACT (Public Law 107–56; 115 Stat. 272), and except as provided in paragraph (2), the Secretary may not disclose to any person any information obtained under this part.

(2) Exception

The Secretary may disclose any information obtained by the Secretary under this part to—

(A) an officer or employee of the United States, or a person that has entered into a contract with the United States, who has a need to know the information to perform the duties of the officer, employee, or person; or

(B) to a State agency under section 488c of this title, under appropriate arrangements to ensure the protection of the information.

(i) Registration procedures and check of terrorist screening database

(1) Registration procedures

(A) Generally

The Secretary shall establish procedures to efficiently receive applications for registration numbers under this part, conduct the checks required under paragraph (2), and promptly issue or deny a registration number.

(B) Initial six-month registration period

The Secretary shall take steps to maximize the number of registration applications that are submitted and processed during the six-month period described in section 488e(e) of this title.

(2) Check of terrorist screening database

(A) Check required

The Secretary shall conduct a check of appropriate identifying information of any person seeking to register with the Department under subsection (c) or (d) against identifying information that appears in the terrorist screening database of the Department.

(B) Authority to deny registration number

If the identifying information of a person seeking to register with the Department under subsection (c) or (d) appears in the terrorist screening database of the Department, the Secretary may deny issuance of a registration number under this part.

(3) Expedited review of applications

(A) In general

Following the six-month period described in section 488e(e) of this title, the Secretary shall, to the extent practicable, issue or deny registration numbers under this part not later than 72 hours after the time the Secretary receives a complete registration application, unless the Secretary determines, in the interest of national security, that additional time is necessary to review an application.

(B) Notice of application status

In all cases, the Secretary shall notify a person seeking to register with the Department under

subsection (c) or (d) of the status of the application of that person not later than 72 hours after the time the Secretary receives a complete registration application.

(4) Expedited appeals process

(A) Requirement

(i) Appeals process

The Secretary shall establish an expedited appeals process for persons denied a registration number under this part.

(ii) Time period for resolution

The Secretary shall, to the extent practicable, resolve appeals not later than 72 hours after receiving a complete request for appeal unless the Secretary determines, in the interest of national security, that additional time is necessary to resolve an appeal.

(B) Consultation

The Secretary, in developing the appeals process under subparagraph (A), shall consult with appropriate stakeholders.

(C) Guidance

The Secretary shall provide guidance regarding the procedures and information required for an appeal under subparagraph (A) to any person denied a registration number under this part.

(5) Restrictions on use and maintenance of information

(A) In general

Any information constituting grounds for denial of a registration number under this section shall be maintained confidentially by the Secretary and may be used only for making determinations under this section.

(B) Sharing of information

Notwithstanding any other provision of this part, the Secretary may share any such information with Federal, State, local, and tribal law enforcement agencies, as appropriate.

(6) Registration information

(A) Authority to require information

The Secretary may require a person applying for a registration number under this part to submit such information as may be necessary to carry out the requirements of this section.

(B) Requirement to update information

The Secretary may require persons issued a registration under this part to update registration information submitted to the Secretary under this part, as appropriate.

(7) Re-checks against terrorist screening database

(A) Re-checks

The Secretary shall, as appropriate, recheck persons provided a registration number pursuant to this part against the terrorist screening database of the Department, and may revoke such registration number if the Secretary determines such person may pose a threat to national security.

(B) Notice of revocation

The Secretary shall, as appropriate, provide prior notice to a person whose registration number is revoked under this section and such person shall have an opportunity to appeal, as provided in paragraph (4).

(Pub. L. 107–296, title VIII, §899B, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2084; amended Pub. L. 115–278, §2(g)(5)(B), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

REFERENCES IN TEXT

The USA PATRIOT ACT, referred to in subsec. (h)(1), is Pub. L. 107–56, Oct. 26, 2001, 115 Stat. 272, also known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. For complete classification of this Act to the Code, see Short Title of 2001 Amendment note set out under section 1 of Title 18, Crimes and Criminal Procedure, and Tables.

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278 inserted at end "Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency."

§488b. Inspection and auditing of records

The Secretary shall establish a process for the periodic inspection and auditing of the records maintained by owners of ammonium nitrate facilities for the purpose of monitoring compliance with this part or for the purpose of deterring or preventing the misappropriation or use of ammonium nitrate in an act of terrorism.

(Pub. L. 107–296, title VIII, §899C, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2087.)

§488c. Administrative provisions

(a) Cooperative agreements

The Secretary—

(1) may enter into a cooperative agreement with the Secretary of Agriculture, or the head of any State department of agriculture or its designee involved in agricultural regulation, in consultation with the State agency responsible for homeland security, to carry out the provisions of this part; and

(2) wherever possible, shall seek to cooperate with State agencies or their designees that oversee ammonium nitrate facility operations when seeking cooperative agreements to implement the registration and enforcement provisions of this part.

(b) Delegation

(1) Authority

The Secretary may delegate to a State the authority to assist the Secretary in the administration and enforcement of this part.

(2) Delegation required

At the request of a Governor of a State, the Secretary shall delegate to that State the authority to carry out functions under sections 488a and 488b of this title, if the Secretary determines that the State is capable of satisfactorily carrying out such functions.

(3) Funding

Subject to the availability of appropriations, if the Secretary delegates functions to a State under this subsection, the Secretary shall provide to that State sufficient funds to carry out the delegated functions.

(c) Provision of guidance and notification materials to ammonium nitrate facilities

(1) Guidance

The Secretary shall make available to each owner of an ammonium nitrate facility registered under section 488a(c)(1) of this title guidance on—

(A) the identification of suspicious ammonium nitrate purchases or transfers or attempted

purchases or transfers;

(B) the appropriate course of action to be taken by the ammonium nitrate facility owner with respect to such a purchase or transfer or attempted purchase or transfer, including—

(i) exercising the right of the owner of the ammonium nitrate facility to decline sale of ammonium nitrate; and

(ii) notifying appropriate law enforcement entities; and

(C) additional subjects determined appropriate to prevent the misappropriation or use of ammonium nitrate in an act of terrorism.

(2) Use of materials and programs

In providing guidance under this subsection, the Secretary shall, to the extent practicable, leverage any relevant materials and programs.

(3) Notification materials

(A) In general

The Secretary shall make available materials suitable for posting at locations where ammonium nitrate is sold.

(B) Design of materials

Materials made available under subparagraph (A) shall be designed to notify prospective ammonium nitrate purchasers of—

(i) the record-keeping requirements under section 488a of this title; and

(ii) the penalties for violating such requirements.

(Pub. L. 107–296, title VIII, §899D, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2087.)

§488d. Theft reporting requirement

Any person who is required to comply with section 488a(e) of this title who has knowledge of the theft or unexplained loss of ammonium nitrate shall report such theft or loss to the appropriate Federal law enforcement authorities not later than 1 calendar day of the date on which the person becomes aware of such theft or loss. Upon receipt of such report, the relevant Federal authorities shall inform State, local, and tribal law enforcement entities, as appropriate.

(Pub. L. 107–296, title VIII, §899E, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2088.)

§488e. Prohibitions and penalty

(a) Prohibitions

(1) Taking possession

No person shall purchase ammonium nitrate from an ammonium nitrate facility unless such person is registered under subsection (c) or (d) of section 488a of this title, or is an agent of a person registered under subsection (c) or (d) of that section.

(2) Transferring possession

An owner of an ammonium nitrate facility shall not transfer possession of ammonium nitrate from the ammonium nitrate facility to any ammonium nitrate purchaser who is not registered under subsection (c) or (d) of section 488a of this title, or to any agent acting on behalf of an ammonium nitrate purchaser when such purchaser is not registered under subsection (c) or (d) of section 488a of this title.

(3) Other prohibitions

No person shall—

(A) purchase ammonium nitrate without a registration number required under subsection (c) or (d) of section 488a of this title;

(B) own or operate an ammonium nitrate facility without a registration number required under section 488a(c) of this title; or

(C) fail to comply with any requirement or violate any other prohibition under this part.

(b) Civil penalty

A person that violates this part may be assessed a civil penalty by the Secretary of not more than $50,000 per violation.

(c) Penalty considerations

In determining the amount of a civil penalty under this section, the Secretary shall consider—

(1) the nature and circumstances of the violation;

(2) with respect to the person who commits the violation, any history of prior violations, the ability to pay the penalty, and any effect the penalty is likely to have on the ability of such person to do business; and

(3) any other matter that the Secretary determines that justice requires.

(d) Notice and opportunity for a hearing

No civil penalty may be assessed under this part unless the person liable for the penalty has been given notice and an opportunity for a hearing on the violation for which the penalty is to be assessed in the county, parish, or incorporated city of residence of that person.

(e) Delay in application of prohibition

Paragraphs (1) and (2) of subsection (a) shall apply on and after the date that is 6 months after the date that the Secretary issues a final rule implementing this part.

(Pub. L. 107–296, title VIII, §899F, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2088.)

§488f. Protection from civil liability

(a) In general

Notwithstanding any other provision of law, an owner of an ammonium nitrate facility that in good faith refuses to sell or transfer ammonium nitrate to any person, or that in good faith discloses to the Department or to appropriate law enforcement authorities an actual or attempted purchase or transfer of ammonium nitrate, based upon a reasonable belief that the person seeking purchase or transfer of ammonium nitrate may use the ammonium nitrate to create an explosive device to be employed in an act of terrorism (as defined in section 3077 of title 18), or to use ammonium nitrate for any other unlawful purpose, shall not be liable in any civil action relating to that refusal to sell ammonium nitrate or that disclosure.

(b) Reasonable belief

A reasonable belief that a person may use ammonium nitrate to create an explosive device to be employed in an act of terrorism under subsection (a) may not solely be based on the race, sex, national origin, creed, religion, status as a veteran, or status as a member of the Armed Forces of the United States of that person.

(Pub. L. 107–296, title VIII, §899G, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2089.)

§488g. Preemption of other laws

(a) Other Federal regulations

Except as provided in section 488f of this title, nothing in this part affects any regulation issued by any agency other than an agency of the Department.

(b) State law

Subject to section 488f of this title, this part preempts the laws of any State to the extent that such laws are inconsistent with this part, except that this part shall not preempt any State law that provides additional protection against the acquisition of ammonium nitrate by terrorists or the use of ammonium nitrate in explosives in acts of terrorism or for other illicit purposes, as determined by the Secretary.

(Pub. L. 107–296, title VIII, §899H, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2089.)

§488h. Deadlines for regulations

The Secretary—

(1) shall issue a proposed rule implementing this part not later than 6 months after December 26, 2007; and

(2) issue a final rule implementing this part not later than 1 year after December 26, 2007.

(Pub. L. 107–296, title VIII, §899I, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2089.)

§488i. Authorization of appropriations

There are authorized to be appropriated to the Secretary—

(1) $2,000,000 for fiscal year 2008; and

(2) $10,750,000 for each of fiscal years 2009 through 2012.

(Pub. L. 107–296, title VIII, §899J, as added Pub. L. 110–161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2090.)

SUBCHAPTER IX—NATIONAL HOMELAND SECURITY COUNCIL

§491. National Homeland Security Council

There is established within the Executive Office of the President a council to be known as the "Homeland Security Council" (in this subchapter referred to as the "Council").

(Pub. L. 107–296, title IX, §901, Nov. 25, 2002, 116 Stat. 2258.)

§492. Function

The function of the Council shall be to advise the President on homeland security matters.

(Pub. L. 107–296, title IX, §902, Nov. 25, 2002, 116 Stat. 2258.)

§493. Membership

(a) Members

The members of the Council shall be the following:

(1) The President.

(2) The Vice President.
(3) The Secretary of Homeland Security.
(4) The Attorney General.
(5) The Secretary of Defense.
(6) Such other individuals as may be designated by the President.

(b) Attendance of Chairman of Joint Chiefs of Staff at meetings

The Chairman of the Joint Chiefs of Staff (or, in the absence of the Chairman, the Vice Chairman of the Joint Chiefs of Staff) may, in the role of the Chairman of the Joint Chiefs of Staff as principal military adviser to the Council and subject to the direction of the President, attend and participate in meetings of the Council.

(Pub. L. 107–296, title IX, §903, Nov. 25, 2002, 116 Stat. 2258; Pub. L. 109–163, div. A, title IX, §908(b), Jan. 6, 2006, 119 Stat. 3404.)

EDITORIAL NOTES

AMENDMENTS

2006—Pub. L. 109–163 designated existing provisions as subsec. (a), inserted heading, and added subsec. (b).

§494. Other functions and activities

For the purpose of more effectively coordinating the policies and functions of the United States Government relating to homeland security, the Council shall—

(1) assess the objectives, commitments, and risks of the United States in the interest of homeland security and to [1] make resulting recommendations to the President;

(2) oversee and review homeland security policies of the Federal Government and to [1] make resulting recommendations to the President; and

(3) perform such other functions as the President may direct.

(Pub. L. 107–296, title IX, §904, Nov. 25, 2002, 116 Stat. 2259.)

[1] So in original. The word "to" probably should not appear.

§495. Staff composition

The Council shall have a staff, the head of which shall be a civilian Executive Secretary, who shall be appointed by the President. The President is authorized to fix the pay of the Executive Secretary at a rate not to exceed the rate of pay payable to the Executive Secretary of the National Security Council.

(Pub. L. 107–296, title IX, §905, Nov. 25, 2002, 116 Stat. 2259.)

§496. Relation to the National Security Council

The President may convene joint meetings of the Homeland Security Council and the National Security Council with participation by members of either Council or as the President may otherwise direct.

(Pub. L. 107–296, title IX, §906, Nov. 25, 2002, 116 Stat. 2259.)

SUBCHAPTER X—CONSTRUCTION

§511. Information security responsibilities of certain agencies

(1) National security responsibilities

(A) Nothing in this chapter (including any amendment made by this chapter) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3552(b)(5) [1] of title 44.

(B) Omitted

(2) Atomic Energy Act of 1954

Nothing in this chapter shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

(Pub. L. 107–296, title X, §1001(c), Nov. 25, 2002, 116 Stat. 2267; Pub. L. 113–283, §2(e)(3)(B), Dec. 18, 2014, 128 Stat. 3087.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Tables.

The Atomic Energy Act of 1954, referred to in par. (2), is act Aug. 1, 1946, ch. 724, as added by act Aug. 30, 1954, ch. 1073, §1, 68 Stat. 919, which is classified principally to chapter 23 (§2011 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 42 and Tables.

CODIFICATION

Section is comprised of section 1001(c) of Pub. L. 107–296. Par. (1)(B) of section 1001(c) of Pub. L. 107–296 amended section 2224 of Title 10, Armed Forces.

AMENDMENTS

2014—Par. (1)(A). Pub. L. 113–283 substituted "section 3552(b)(5)" for "section 3532(3)".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

SHORT TITLE

For short title of title X of Pub. L. 107–296, which enacted this subchapter, as the "Federal Information Security Management Act of 2002", see section 1001(a) of Pub. L. 107–296, set out as a note under section 101 of this title.

[1] *So in original. Probably should be "3552(b)(6)".*

§512. Construction

Nothing in this chapter, or the amendments made by this chapter, affects the authority of the National Institute of Standards and Technology or the Department of Commerce relating to the development and promulgation of standards or guidelines under paragraphs (1) and (2) of section 278g–3(a) of title 15.

(Pub. L. 107–296, title X, §1006, Nov. 25, 2002, 116 Stat. 2273.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Tables.

§513. Federal air marshal program

(1) Sense of Congress

It is the sense of Congress that the Federal air marshal program is critical to aviation security.

(2) Limitation on statutory construction

Nothing in this chapter, including any amendment made by this chapter, shall be construed as preventing the Under Secretary of Transportation for Security from implementing and training Federal air marshals.

(Pub. L. 107–296, title XIV, §1402(c), Nov. 25, 2002, 116 Stat. 2305.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in par. (2), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to Under Secretary of Transportation for Security deemed to refer to Administrator of the Transportation Security Administration, see section 1994 of Pub. L. 115–254, set out as a note under section 114 of Title 49, Transportation.

SUBCHAPTER XI—DEPARTMENT OF JUSTICE DIVISIONS

PART A—EXECUTIVE OFFICE FOR IMMIGRATION REVIEW

§521. Legal status of EOIR

(a) [1] Existence of EOIR

There is in the Department of Justice the Executive Office for Immigration Review, which shall be subject to the direction and regulation of the Attorney General under section 1103(g) of title 8.

(Pub. L. 107–296, title XI, §1101, Nov. 25, 2002, 116 Stat. 2273.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Pub. L. 107–296, title XI, §1104, as added by Pub. L. 108–7, div. L, §105(a)(3), Feb. 20, 2003, 117 Stat. 531, provided that: "The provisions of this subtitle [subtitle A (§§1101–1104) of title XI of Pub. L. 107–296, enacting this part and amending section 1103 of Title 8, Aliens and Nationality] shall take effect on the date of the transfer of functions from the Commissioner of Immigration and Naturalization to officials of the Department of Homeland Security [functions transferred Mar. 1, 2003]".

[1] *So in original. No subsec. (b) has been enacted.*

§522. Statutory construction

Nothing in this chapter, any amendment made by this chapter, or in section 1103 of title 8, shall be construed to limit judicial deference to regulations, adjudications, interpretations, orders, decisions, judgments, or any other actions of the Secretary of Homeland Security or the Attorney General.

(Pub. L. 107–296, title XI, §1103, Nov. 25, 2002, 116 Stat. 2274.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE

Section effective on the date of the transfer of functions from the Commissioner of Immigration and Naturalization to officials of the Department of Homeland Security (Mar. 1, 2003), see section 1104 of Pub. L. 107–296, as added by Pub. L. 108–7, set out as a note under section 521 of this title.

PART B—TRANSFER OF THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS TO THE DEPARTMENT OF JUSTICE

§531. Bureau of Alcohol, Tobacco, Firearms, and Explosives

(a), (b) Transferred

(c) Transfer of authorities, functions, personnel, and assets to the Department of Justice

(1) Transferred

(2) Administration and revenue collection functions

There shall be retained within the Department of the Treasury the authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms relating to the administration and enforcement of chapters 51 and 52 of title 26, sections 4181 and 4182 of title

26, and title 27.

(3) Transferred

(d) Tax and Trade Bureau

(1) Establishment

There is established within the Department of the Treasury the Tax and Trade Bureau.

(2) Administrator

The Tax and Trade Bureau shall be headed by an Administrator, who shall perform such duties as assigned by the Under Secretary for Enforcement of the Department of the Treasury. The Administrator shall occupy a career-reserved position within the Senior Executive Service.

(3) Responsibilities

The authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms that are not transferred to the Department of Justice under this section shall be retained and administered by the Tax and Trade Bureau.

(Pub. L. 107–296, title XI, §1111, Nov. 25, 2002, 116 Stat. 2274; Pub. L. 109–162, title XI, §1187(b), Jan. 5, 2006, 119 Stat. 3127.)

EDITORIAL NOTES

AMENDMENTS

2006—Pub. L. 109–162 transferred section catchline and subsecs. (a)–(c)(1), (3), to section 599A of Title 28, Judiciary and Judicial Procedure.

§532. Explosives Training and Research Facility

(a) Establishment

There is established within the Bureau an Explosives Training and Research Facility at Fort AP Hill, Fredericksburg, Virginia.

(b) Purpose

The facility established under subsection (a) shall be utilized to train Federal, State, and local law enforcement officers to—

(1) investigate bombings and explosions;
(2) properly handle, utilize, and dispose of explosive materials and devices;
(3) train canines on explosive detection; and
(4) conduct research on explosives.

(c) Authorization of appropriations

(1) In general

There are authorized to be appropriated such sums as may be necessary to establish and maintain the facility established under subsection (a).

(2) Availability of funds

Any amounts appropriated pursuant to paragraph (1) shall remain available until expended.

(Pub. L. 107–296, title XI, §1114, Nov. 25, 2002, 116 Stat. 2280.)

§533. Transferred

EDITORIAL NOTES

CODIFICATION

Section, Pub. L. 107–296, title XI, §1115, Nov. 25, 2002, 116 Stat. 2280, which related to a Personnel Management Demonstration Project, was transferred to section 599B of Title 28, Judiciary and Judicial Procedure, by Pub. L. 109–162, title XI, §1187(b), (c)(2), Jan. 5, 2006, 119 Stat. 3127, 3128.

SUBCHAPTER XII—TRANSITION

PART A—REORGANIZATION PLAN

§541. Definitions

For purposes of this subchapter:

(1) The term "agency" includes any entity, organizational unit, program, or function.

(2) The term "transition period" means the 12-month period beginning on the effective date of this chapter.

(Pub. L. 107–296, title XV, §1501, Nov. 25, 2002, 116 Stat. 2307.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in par. (2), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

§542. Reorganization plan

(a) Submission of plan

Not later than 60 days after November 25, 2002, the President shall transmit to the appropriate congressional committees a reorganization plan regarding the following:

(1) The transfer of agencies, personnel, assets, and obligations to the Department pursuant to this chapter.

(2) Any consolidation, reorganization, or streamlining of agencies transferred to the Department pursuant to this chapter.

(b) Plan elements

The plan transmitted under subsection (a) shall contain, consistent with this chapter, such elements as the President deems appropriate, including the following:

(1) Identification of any functions of agencies transferred to the Department pursuant to this chapter that will not be transferred to the Department under the plan.

(2) Specification of the steps to be taken by the Secretary to organize the Department, including the delegation or assignment of functions transferred to the Department among officers of the Department in order to permit the Department to carry out the functions transferred under the plan.

(3) Specification of the funds available to each agency that will be transferred to the Department as a result of transfers under the plan.

(4) Specification of the proposed allocations within the Department of unexpended funds transferred in connection with transfers under the plan.

(5) Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations of agencies transferred under the plan.

(6) Specification of the proposed allocations within the Department of the functions of the

agencies and subdivisions that are not related directly to securing the homeland.

(c) Modification of plan

The President may, on the basis of consultations with the appropriate congressional committees, modify or revise any part of the plan until that part of the plan becomes effective in accordance with subsection (d).

(d) Effective date

(1) In general

The reorganization plan described in this section, including any modifications or revisions of the plan under subsection (d), shall become effective for an agency on the earlier of—

(A) the date specified in the plan (or the plan as modified pursuant to subsection (d)), except that such date may not be earlier than 90 days after the date the President has transmitted the reorganization plan to the appropriate congressional committees pursuant to subsection (a); or

(B) the end of the transition period.

(2) Statutory construction

Nothing in this subsection may be construed to require the transfer of functions, personnel, records, balances of appropriations, or other assets of an agency on a single date.

(3) Supersedes existing law

Paragraph (1) shall apply notwithstanding section 905(b) of title 5.

(Pub. L. 107–296, title XV, §1502, Nov. 25, 2002, 116 Stat. 2308.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in subsecs. (a) and (b), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

EXECUTIVE DOCUMENTS

DEPARTMENT OF HOMELAND SECURITY

REORGANIZATION PLAN

NOVEMBER 25, 2002

H. DOC. NO. 108–16, 108TH CONGRESS, 1ST SESSION, PROVIDED:

INTRODUCTION

This Reorganization Plan is submitted pursuant to Section 1502 of the Department [sic] of Homeland Security Act of 2002 [6 U.S.C. 542] ("the Act"), which requires submission, not later than 60 days after enactment [Nov. 25, 2002], of a reorganization plan regarding two categories of information concerning plans for the Department of Homeland Security ("the Department" or "DHS"):

(1) The transfer of agencies, personnel, assets, and obligations to the Department pursuant to this Act [Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135].

(2) Any consolidation, reorganization, or streamlining of agencies transferred to the Department pursuant to this Act. Section 1502(a).

Section 1502(b) of the Act identifies six elements, together with other elements "as the President deems appropriate," as among those for discussion in the plan. Each of the elements set out in the statute is identified *verbatim* below, followed by a discussion of current plans with respect to that element.

This plan is subject to modification pursuant to Section 1502(d) of the Act, which provides that on the basis of consultations with appropriate congressional committees the President may modify or revise any part of the plan until that part of the plan becomes effective. Additional details concerning the process for establishing

the Department will become available in the coming weeks and months, and the President will work closely with Congress to modify this plan consistent with the Act.

PLAN ELEMENTS

(1) Identification of any functions of agencies transferred to the Department pursuant to this Act that will not be transferred to the Department under the plan.

Except as otherwise directed in the Act, all functions of agencies that are to be transferred to the Department pursuant to the Act will be transferred to the Department under the plan. The functions of agencies being transferred to the Department which the Act directs are not to be transferred are the following:

- Pursuant to Section 201(g)(1) of the Act [6 U.S.C. 121(g)(1)], the Computer Investigations and Operations Section ("CIOS") of the National Infrastructure Protection Center ("NIPC") of the Federal Bureau of Investigation ("FBI") will not transfer to the Department with the rest of NIPC. CIOS is the FBI headquarters entity responsible for managing all FBI computer intrusion field office cases (whether law enforcement or national security related).
- Pursuant to Sections 421(c) & (d) of the Act [6 U.S.C. 231(c), (d)], the regulatory responsibilities and quarantine activities relating to agricultural import and entry inspection activities of the United States Department of Agriculture ("the USDA") Animal and Plant Health Inspection Service ("APHIS") will remain with the USDA, as will the Secretary of Agriculture's authority to issue regulations, policies, and procedures regarding the functions transferred pursuant to Sections 421(a) & (b) of the Act.
- Pursuant to Subtitle B of Title IV of the Act [6 U.S.C. 211 et seq.], the authorities of the Secretary of the Treasury related to Customs revenue functions, as defined in the statute, will not transfer to the Department.
- Functions under the immigration laws of the United States with respect to the care of unaccompanied alien children will not transfer from the Department of Justice to DHS, but will instead transfer to the Department of Health and Human Services pursuant to Section 462 of the Act [6 U.S.C. 279].

(2) Specification of the steps to be taken by the Secretary to organize the Department, including the delegation or assignment of functions transferred to the Department among officers of the Department in order to permit the Department to carry out the functions transferred under the plan.

A. *Steps to be taken by the Secretary to organize the Department*. The President intends that the Secretary will carry out the following actions on the dates specified. All of the following transfers shall be deemed to be made to DHS, and all offices and positions to be established and all officers and officials to be appointed or named shall be deemed to be established, appointed, or named within DHS.

January 24, 2003 (effective date of the Act pursuant to Section 4 [6 U.S.C. 101 note]):

- Establish the Office of the Secretary.
- Begin to appoint, upon confirmation by the Senate, or transfer pursuant to the transfer provisions of the Act, as many of the following officers as may be possible:
  - (1) Deputy Secretary of Homeland Security
  - (2) Under Secretary for Information Analysis and Infrastructure Protection
  - (3) Under Secretary for Science and Technology
  - (4) Under Secretary for Border and Transportation Security
  - (5) Under Secretary for Emergency Preparedness and Response
  - (6) Director of the Bureau of Citizenship and Immigration Services
  - (7) Under Secretary for Management
  - (8) Not more than 12 Assistant Secretaries
  - (9) General Counsel
  - (10) Inspector General
  - (11) Commissioner of Customs
- Name, as soon as may be possible, officers to fill the following offices created by the Act:
  - (1) Assistant Secretary for Information Analysis
  - (2) Assistant Secretary for Infrastructure Protection
  - (3) Privacy Officer
  - (4) Director of the Secret Service
  - (5) Chief Information Officer
  - (6) Chief Human Capital Officer
  - (7) Chief Financial Officer

(8) Officer for Civil Rights and Civil Liberties
(9) Director of Shared Services
(10) Citizenship and Immigration Ombudsman
(11) Director of the Homeland Security Advanced Research Projects Agency

• Establish, within the Office of the Secretary, the Office for State and Local Government Coordination, the Office of International Affairs, and the Office of National Capital Region Coordination.

• Establish the Homeland Security Advanced Research Projects Agency and the Acceleration Fund for Research and Development of Homeland Security Technologies.

• Establish within the Directorate of Science and Technology the Office for National Laboratories.

• Establish the Bureau of Border Security [now Bureau of Immigration and Customs Enforcement], the Bureau of Citizenship and Immigration Services, and the Director of Shared Services.

• Establish the Transportation Security Oversight Board with the Secretary of Homeland Security as its Chair.

March 1, 2003:

• Transfer the Critical Infrastructure Assurance Office ("CIAO") of the Department of Commerce, the National Communications System ("the NCS"), the NIPC of the FBI (other than the CIOS), the National Infrastructure Simulation and Analysis Center ("NISAC"), the Energy Assurance Office ("EAO") of the Department of Energy, and the Federal Computer Incident Response Center of the General Services Administration ("FedCIRC").

• Transfer the Coast Guard.

• Transfer the Customs Service, the Transportation Security Administration ("the TSA"), functions of the Immigration and Naturalization Service ("the INS"), the Federal Protective Service ("the FPS"), the Office of Domestic Preparedness ("the ODP"), and the Federal Law Enforcement Training Center ("the FLETC").

• Transfer the functions of the Secretary of Agriculture relating to agricultural import and entry inspection activities under the laws specified in Section 421(b) of the Act [6 U.S.C. 231(b)] from the Animal and Plant Health Inspection Service.

• Transfer the United States Secret Service.

• Transfer the following programs and activities to the Directorate of Science and Technology:

º The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program of the Department of Energy.

º The life sciences activities related to microbial pathogens of the Biological and Environmental Research Program of the Department of Energy.

º The National Bio-Weapons Defense Analysis Center of the Department of Defense.

º The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program of the Department of Energy.

º The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program of the Department of Energy and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory of the Department of Energy.

º The Environmental Measurements Laboratory of the Department of Energy.

• Transfer the Federal Emergency Management Agency ("FEMA").

• Transfer the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, which shall be renamed "FIRESTAT."

• Transfer the National Domestic Preparedness Office of the FBI, including the functions of the Attorney General relating thereto.

• Transfer the Domestic Emergency Support Team of the Department of Justice, including the functions of the Attorney General relating thereto.

• Transfer the Metropolitan Medical Response System of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer the National Disaster Medical System of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer the Office of Emergency Preparedness and the Strategic National Stockpile of the Department of Health and Human Services, including the functions of the Secretary of Health and Human Services and Assistant Secretary for Public Health Emergency Preparedness relating thereto.

• Transfer to the Secretary the authority (in connection with an actual or threatened terrorist attack,

major disaster, or other emergency in the United States) to direct the Nuclear Incident Response Team of the Department of Energy to operate as an organizational unit.

June 1, 2003:

• Transfer the Plum Island Animal Disease Center of USDA.

• Establish the Homeland Security Science and Technology Advisory Committee.

By September 30, 2003:

• Complete any incidental transfers, pursuant to Section 1516 of the Act [6 U.S.C. 556], of personnel, assets, and liabilities held, used, arising from, available, or to be made available, in connection with the functions transferred by the Act.

B. *Delegation or Assignment Among Officers of Functions Transferred to the Department*. The President intends that the Secretary will delegate or assign transferred functions within the Department as follows:

1. Information Analysis and Infrastructure Protection

a. *Under Secretary for Information Analysis and Infrastructure Protection ("IA and IP"):* Will be responsible for oversight of functions of NIPC, NCS, CIAO, NISAC, EAO, and FedCIRC transferred by the Act, the management of the Directorate's Information Analysis and Infrastructure Protection duties, and the administration of the Homeland Security Advisory System.

b. *Assistant Secretary for Information Analysis:* Will oversee the following Information Analysis functions:

• Identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States; and, understand such threats in light of actual and potential vulnerabilities of the homeland.

• In coordination with the Assistant Secretary for Infrastructure Protection, integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

• Ensure the timely and efficient access by the Department to all information necessary to discharge the responsibilities under Section 201 of the Act [6 U.S.C. 121], including obtaining such information from other agencies of the Federal Government.

• Review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities.

• Disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

• Consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

• Consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

• Ensure that—

1. Any material received pursuant to the Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and
2. Any intelligence information under the Act is shared, retained, and disseminated consistent with the authority of the Director of Central Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. Section 401, et seq.) [now 50 U.S.C. 3001 et seq.] and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

• Request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States,

or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

• Establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of statutory responsibilities, and to disseminate information acquired and analyzed by the Department, as appropriate.

• Ensure, in conjunction with the Chief Information Officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

1. Are compatible with one another and with relevant information databases of other agencies of the Federal Government; and
2. Treat information in such databases in a manner that complies with applicable Federal law on privacy.

• Coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

• Coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

• Provide intelligence and information analysis and support to other elements of the Department.

c. *Assistant Secretary for Infrastructure Protection:* Will oversee the following Infrastructure Protection functions:

• Carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

• In coordination with the Assistant Secretary for Information Analysis, integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

• Develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

• Recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

• In coordination with the Under Secretary for Emergency Preparedness and Response, provide to State and local government entities, and upon request to private entities that own or operate critical information systems, crisis management support in response to threats to, or attacks on, critical information systems.

• Provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

• Coordinate with other agencies of the Federal Government to provide specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public.

2. Science and Technology

Under Secretary for Science and Technology: Will be responsible for performing the functions set forth in Section 302 of the Act [6 U.S.C. 182], including the following:

• Advise the Secretary regarding research and development efforts and priorities in support of the Department's missions.

• Develop, in consultation with other appropriate executive agencies, a national policy and

strategic plan for identifying priorities, goals, objectives, and policies for, and coordinating the Federal Government's civilian efforts with respect to, identifying and developing countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts.

• Support the Under Secretary for Information Analysis and Infrastructure Protection by assessing and testing homeland security vulnerabilities and possible threats.

• Conduct basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities.

• Establish priorities for directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

1. preventing the importation of chemical, biological, radiological, nuclear, and related weapons and material; and
2. detecting, preventing, protecting against, and responding to terrorist attacks.

• Establish a system for transferring homeland security developments or technologies to Federal, State, and local governments, and to private sector entities.

• Enter into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities.

• Collaborate with the Secretary of Agriculture and the Attorney General as provided in Section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. §8401), as amended by Section 1709(b) of the Act.

• Collaborate with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as "select agents" in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to Section 351A of the Public Health Service Act (42 U.S.C. §262a).

• Support United States leadership in science and technology.

• Establish and administer the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department.

• Coordinate and integrate all research, development, demonstration, testing, and evaluation activities of the Department.

• Coordinate with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs.

• Develop and oversee the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

3. Border and Transportation Security

The Directorate of Border and Transportation Security ("BTS") will include the following: the Bureau of Border Security [now Bureau of Immigration and Customs Enforcement]; the Office for Domestic Preparedness; the Customs Service [renamed Bureau of Customs and Border Protection]; the Transportation Security Administration; FLETC; and FPS.

The BTS Directorate will also have in place the key leaders of the new Directorate to include:

a. *Under Secretary for BTS:* Will be responsible for oversight of all responsibilities set forth in Section 402 of the Act [6 U.S.C. 202], including the following:

• Prevent the entry of terrorists and the instruments of terrorism into the United States.

• Secure the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.

• Establish and administer rules, in accordance with Section 428 of the Act [6 U.S.C. 236], governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States.

• Establish national immigration enforcement policies and priorities.

• Administer the customs laws of the United States, except as otherwise provided in the Act.

• Conduct the inspection and related administrative functions of the USDA transferred to the Secretary of Homeland Security under Section 421 of the Act [6 U.S.C. 231].

• In carrying out the foregoing responsibilities, ensure the speedy, orderly, and efficient flow of lawful traffic and commerce.

• Carry out the immigration enforcement functions specified under Section 441 of the Act [6 U.S.C. 251] that were vested by statute in, or performed by, the Commissioner of the INS (or any officer, employee, or component of the INS) immediately before the date on which the transfer of functions takes place.

b. *Assistant Secretary for Border Security:* Will report directly to the Under Secretary for Border and Transportation Security, and whose responsibilities will include the following:

• Establish and oversee the administration of the policies for performing such functions as are—

1. transferred to the Under Secretary for Border and Transportation Security by Section 441 of the Act and delegated to the Assistant Secretary by the Under Secretary for Border and Transportation Security; or
2. otherwise vested in the Assistant Secretary by law.

• Advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of the Bureau of Border Security [now Bureau of Immigration and Customs Enforcement] that may affect the Bureau of Citizenship and Immigration.

c. *Director of the Office for Domestic Preparedness*—Will report directly to the Under Secretary for Border and Transportation Security and will have the primary responsibility within the Executive Branch of the Federal Government for the preparedness of the United States for acts of terrorism, including the following responsibilities:

• Coordinate preparedness efforts at the Federal level, and work with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support.

• Coordinate or, as appropriate, consolidate communications and systems of communications relating to homeland security at all levels of government.

• Direct and supervise terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers.

• Incorporate homeland security priorities into planning guidance on an agency level for the preparedness efforts of the Office for Domestic Preparedness.

• Provide agency-specific training for agents and analysts within the Department, other agencies, and State and local agencies, and international entities.

• As the lead executive branch agency for preparedness of the United States for acts of terrorism, cooperate closely with the FEMA, which shall have the primary responsibility within the executive branch to prepare for and mitigate the effects of nonterrorist-related disasters in the United States.

• Assist and support the Secretary, in coordination with other Directorates and entities outside the Department, in conducting appropriate risk analysis and risk management activities of State, local, and tribal governments consistent with the mission and functions of the Directorate.

• Supervise those elements of the Office of National Preparedness of FEMA that relate to terrorism, which shall be consolidated within the Department in the ODP established pursuant to Section 430 of the Act [6 U.S.C. 238].

4. Emergency Preparedness and Response

The Emergency Preparedness and Response Directorate will be headed by the Under Secretary for Emergency Preparedness and Response.

Under Secretary for EP&R: Will be responsible for all of those functions included within Section 502 [now 504] of the Act [6 U.S.C. 314], including:

• Helping to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies.

• With respect to the Nuclear Incident Response Team (regardless of whether it is operating as an organizational unit of the Department pursuant to the Act):

1. Establishing standards and certifying when those standards have been met;
2. Conducting joint and other exercises and training and evaluating performance; and,
3. Providing funds to the Department of Energy and the Environmental Protection Agency, as appropriate,

for homeland security planning, exercises and training, and equipment.

• Providing the Federal Government's response to terrorist attacks and major disasters, including:

1. Managing such response;
2. Directing the Domestic Emergency Support Team, the Strategic National Stockpile, the National Disaster Medical System, and (when operating as an organizational unit of the Department pursuant to the Act) the Nuclear Incident Response Team;
3. Overseeing the Metropolitan Medical Response System; and
4. Coordinating other Federal response resources in the event of a terrorist attack or major disaster.

• Aiding the recovery from terrorist attacks and major disasters;

• Building a comprehensive national incident management system with Federal, State, and local government personnel, agencies, and authorities, to respond to such attacks and disasters.

• Consolidating existing Federal Government emergency response plans into a single, coordinated national response plan; and

• Developing comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology.

5. Other Officers and Functions

a. *Director of the Bureau of Citizenship and Immigration Services:* Will report directly to the Deputy Secretary; and will be responsible for the following:

• Establishing the policies for performing such functions as are transferred to the Director by Section 451 of the Act [6 U.S.C. 271] or otherwise vested in the Director by law.

• Oversight of the administration of such policies.

• Advising the Deputy Secretary with respect to any policy or operation of the Bureau of Citizenship and Immigration Services that may affect the Bureau of Border Security [now Bureau of Immigration and Customs Enforcement] of the Department, including potentially conflicting policies or operations.

• Establishing national immigration services policies and priorities.

• Meeting regularly with the Ombudsman described in Section 452 of the Act [6 U.S.C. 272] to correct serious service problems identified by the Ombudsman.

• Establishing procedures requiring a formal response to any recommendations submitted in the Ombudsman's annual report to Congress within three months after its submission to Congress.

b. *Citizenship and Immigration Services Ombudsman:* Will report directly to the Deputy Secretary; and will be responsible for the following:

• Assisting individuals and employers in resolving problems with the Bureau of Citizenship and Immigration Services;

• Identifying areas in which individuals and employers have problems in dealing with the Bureau of Citizenship and Immigration Services; and

• Proposing changes in the administrative practices of the Bureau of Citizenship and Immigration Services to mitigate identified problems.

(3) Specification of the funds available to each agency that will be transferred to the Department as a result of transfers under the plan.

• The attached tables [not set out in the Code] provide estimates of the funds available to the agencies and entities that will be transferred to the Department by operation of the Act. The two tables include total funding (mandatory and discretionary including fees) and discretionary funding net of fees. The tables provide the enacted levels for 2002 and 2002 supplementals, and the President's requested levels for 2003.

Because of the current state of the 2003 budget process, information concerning the funds that will be available to each transferring agency on the date of the proposed transfers is not currently available and will not likely be available during the time period in which the President is to submit this Reorganization Plan. As additional information becomes available, it will be provided as may be required in accordance with the procedures under the Act for modification of this Plan or other applicable law.

(4) Specification of the proposed allocations within the Department of unexpended funds transferred in connection with transfers under the plan.

• The attached tables [not set out in the Code] provide estimates of the unobligated balances as of

September 30, 2002, for the agencies and programs that will be transferred to the Department. The first table provides estimates of unobligated balances for the accounts that are moving to the Department in whole. The second table provides estimates of the unobligated balances in the accounts of which only a portion will be transferring to the new Department. These latter estimates, however, are of the unobligated balances for the full account, only a portion of which are associated with the activities that will be transferred to the Department. In addition, these unobligated balances are based on the Department of Treasury's estimates as of September 30, 2002, which are the latest available figures. Since October 1, 2002, Departments and agencies (except the Department of Defense) have been operating under continuing resolutions, and, as such, have been spending these balances to maintain current operations.

Authority to reallocate unexpended funds of agencies transferred under this Plan is found in H.J. Res. 124 [Pub. L. 107–294, Nov. 23, 2002, 116 Stat. 2062], the continuing resolution in effect currently and until January 11, 2003. The resolution provides authority for the Office of Management and Budget to transfer an amount not to exceed $140,000,000 from unobligated balances of appropriations enacted before October 1, 2002 "for organizations and entities that will be transferred to the new Department and for salaries and expenses associated with the initiation of the Department." Such authority may be exercised upon providing 15 days' notice to the Appropriations Committees. We anticipate that it may be necessary to provide funding through such transfers both for transferring entities and for salaries and expenses associated with the initiation of the Department, including, for example, those associated with establishing the Office of the Secretary and other new offices provided for in the Act. Any plan to use such funding will follow the procedures required under the continuing resolution, including the provision of at least 15 days' notice to the Appropriations Committees.

(5) Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations of agencies transferred under the plan.

• There is no intention to dispose of property, facility, contracts, records, and other assets and obligations of agencies transferred under the plan. All of such assets and obligations will transfer with each agency pursuant to Section 1511(d)(1) of the Act [6 U.S.C. 551(d)(1)].

• Prior to and during the transition period (as defined by Section 1501(a)(2) of the Act [6 U.S.C. 541(a)(2)]), the Department may identify property, facilities, contracts, records, and other assets and obligations of agencies transferred that would be candidates for disposition due to duplication, non-use, obsolescence, and the like. If and when any such proposed dispositions are identified, we will follow provisions of the Act relating to modification of this plan or further notification of Congress.

(6) Specification of the proposed allocations within the Department of the functions of the agencies and subdivisions that are not related directly to securing the homeland.

• As agencies and subdivisions are transferred into the Department, any functions of those entities that are not directly related to securing the homeland will continue to be allocated to the agencies and subdivisions in which they are currently incorporated.

[Bureau of Border Security renamed Bureau of Immigration and Customs Enforcement, and Customs Service renamed Bureau of Customs and Border Protection, by Reorganization Plan Modification for the Department of Homeland Security, H. Doc. No. 108–32, 108th Congress, 1st Session, set out below.]

[For transfer of functions of Strategic National Stockpile to Secretary of Health and Human Services, with certain exceptions, see section 3(c)(1), (2) of Pub. L. 108–276, set out as a note under section 247d–6b of Title 42, The Public Health and Welfare.]

MESSAGE OF THE PRESIDENT

38 Weekly Compilation of Presidential Documents 2095, Dec. 2, 2002; H. Doc. No. 108–16, provided:

THE WHITE HOUSE, *Washington, November 25, 2002.*

Dear Mr. Speaker: (Dear Mr. President:) [1]

Pursuant to section 1502 of the Homeland Security Act of 2002 [6 U.S.C. 542], I submit herewith the enclosed Reorganization Plan for the Department of Homeland Security. The Reorganization Plan provides information concerning the elements identified in section 1502(b), and is subject to modification pursuant to section 1502(d) of the Act. In accordance with section 1502(a) of the Act, please transmit this Reorganization Plan to the appropriate congressional committees.

The details of this Plan are set forth in the enclosed letter from the Director of the Office of Management and Budget. I concur with his comments and observations.

Sincerely,

GEORGE W. BUSH.

[1] **Editorial note**. This is the text of identical letters addressed to the Speaker of the House of Representatives and the President of the Senate.

Enclosure.

REORGANIZATION PLAN MODIFICATION FOR THE DEPARTMENT OF HOMELAND SECURITY

JANUARY 30, 2003

H. DOC. NO. 108–32, 108TH CONGRESS, 1ST SESSION, PROVIDED:

INTRODUCTION

This Reorganization Plan Modification is submitted pursuant to the Homeland Security Act ("the Act") of 2002 [Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135]. All elements of the Department of Homeland Security Reorganization Plan of November 25, 2002 ("the Plan") [set out above] remain as submitted except for those modifications addressed herein.

PURPOSE OF MODIFICATION

This modification of the Plan is to establish and specify organizational units within the Border and Transportation Security Directorate. This modification presents a structural change, but does not consolidate, discontinue, or diminish transferred agencies' current operations in the field.

PLAN MODIFICATIONS

(a) *Rename the "Bureau of Border Security" the "Bureau of Immigration and Customs Enforcement."* As required by the Act, this Bureau will be headed by an Assistant Secretary who will report directly to the Undersecretary for Border and Transportation Security.

This Bureau will comprise Immigration Naturalization Service (INS) interior enforcement functions, including the detention and removal program, the intelligence program, and the investigations program. At the same time, pursuant to this modification, the interior enforcement resources and missions of the Customs Service and the Federal Protective Service will be added to this Bureau. The mission of the Bureau is:

1. To enforce the full range of immigration and customs laws within the interior of the United States; and,

2. To protect specified federal buildings.

The Assistant Secretary will:

1. Establish and oversee the administration of the policies for performing the detention and removal program, the intelligence program, and the investigation program functions as are—

(a) transferred to the Under Secretary for Border and Transportation Security by Section 441 of the Act [6 U.S.C. 251] and delegated to the Assistant Secretary by the Under Secretary for Border and Transportation Security; or

(b) otherwise vested in the Assistant Secretary by law.

2. Advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of the Bureau that may affect the Bureau of Citizenship and Immigration Services established under subtitle E of the Act [probably means subtitle E of title IV of the Act, 6 U.S.C. 271 et seq.], including potentially conflicting policies and operations.

(b) *Rename the "Customs Service" the "Bureau of Customs and Border Protection."* This Bureau will be headed by the Commissioner of Customs and will report to the Under Secretary for Border and Transportation Security.

The Bureau will contain the resources and missions relating to borders and ports of entry of the Customs Service, the INS, including the Border Patrol and the inspections program, and the agricultural inspections function of the Agricultural Quarantine Inspection program.

The Commissioner will:

1. Establish and oversee the administration of the policies for performing the Border Patrol and inspections program functions as are—

(a) transferred to the Under Secretary for Border and Transportation Security by Section 441 of

the Act [6 U.S.C. 251] and delegated to the Commissioner by the Under Secretary for Border and Transportation Security; or

(b) otherwise vested in the Assistant Secretary [probably should be "Commissioner"] by law.

2. Advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of the Bureau that may affect the Bureau of Citizenship and Immigration Services established under subtitle E of the Act [probably means subtitle E of title IV of the Act, 6 U.S.C. 271 et seq.], including potentially conflicting policies and operations.

IMPLEMENTATION DATE

March 1, 2003

ELEMENTS REQUIRED BY THE ACT TO BE SUBMITTED WITH MODIFIED PLAN

(1) *Identification of any functions of agencies transferred to the Department pursuant to this Act that will not be transferred to the Department under the plan.*

None.

(2) *Specification of the steps to be taken by the Secretary to organize the Department, including the delegation or assignment of functions transferred to the Department among officers of the Department in order to permit the Department to carry out the functions transferred under the plan.*

See plan modifications above.

(3) *Specification of the funds available to each agency that will be transferred to the Department as a result of transfers under the plan.*

The table attached at Tab A [not set out in the Code] provides estimates of the funds available to the agencies affected by this modification that will be transferred to the Department by operation of the Act. The table includes total funding (mandatory and discretionary including fees) and discretionary funding net of fees. The table provides the President's requested levels for 2003.

Because of the current state of the 2003 budget process, information concerning the funds that will be available to each transferring agency on the date of the proposed transfers is not currently available. As additional information becomes available, it will be provided as may be required in accordance with the procedures under the Act for modification of this Plan or other applicable law.

(4) *Specification of the proposed allocations within the Department of unexpended funds transferred in connection with transfers under the plan.*

The table attached at Tab B [not set out in the Code] provides updated estimates of the unobligated balances as of September 30, 2002, for the agencies affected by this modification that will be transferred to the Department. Since October 1, 2002, these agencies have been operating under continuing resolutions, and, as such, have been spending these balances to maintain current operations. As additional information becomes available, it will be provided as may be required in accordance with the procedures under the Act for modification of this Plan or other applicable law.

(5) *Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations of agencies transferred under the plan.*

There is no intention to dispose of property, facilities, contracts, records, and other assets and obligations of agencies transferred under this modification. All such assets and obligations will transfer with each agency pursuant to Section 1511(d)(1) of the Act [6 U.S.C. 551(d)(1)].

(6) *Specification of the proposed allocations within the Department of the functions of the agencies and subdivisions that are not related directly to securing the homeland.*

The functions of the agencies affected by this modification that are not directly related to securing the homeland will continue to be performed by the bureaus formed by this planned reorganization.

MESSAGE OF THE PRESIDENT

39 Weekly Compilation of Presidential Documents 136, Feb. 3, 2003; H. Doc. No. 108–32, provided:

THE WHITE HOUSE, *Washington, January 30, 2003.*

Dear Mr. Speaker: (Dear Mr. President:) [1]

Pursuant to section 1502 of the Homeland Security Act of 2002 [6 U.S.C. 542] (Public Law 107–296) (the "Act"), I submit herewith the enclosed Reorganization Plan Modification for the Department of Homeland Security (DHS), which represents a modification of certain aspects of the DHS Reorganization Plan [set out above] I submitted to you on November 25, 2002. The modification involves organizational units within the DHS Border and Transportation Security Directorate. The enclosed Reorganization Plan Modification provides information concerning the elements identified in section 1502(b), and is itself subject to modification pursuant to section 1502(d) of the Act. In accordance with section 1502(a) of the Act, please transmit this Reorganization Plan Modification to the appropriate congressional committees.

Sincerely,

GEORGE W. BUSH.

[1] **Editorial note**. This is the text of identical letters addressed to the Speaker of the House of Representatives and the President of the Senate.

§543. Review of congressional committee structures

It is the sense of Congress that each House of Congress should review its committee structure in light of the reorganization of responsibilities within the executive branch by the establishment of the Department.

(Pub. L. 107–296, title XV, §1503, Nov. 25, 2002, 116 Stat. 2309.)

PART B—TRANSITIONAL PROVISIONS

§551. Transitional authorities

(a) Provision of assistance by officials

Until the transfer of an agency to the Department, any official having authority over or functions relating to the agency immediately before the effective date of this chapter shall provide to the Secretary such assistance, including the use of personnel and assets, as the Secretary may request in preparing for the transfer and integration of the agency into the Department.

(b) Services and personnel

During the transition period, upon the request of the Secretary, the head of any executive agency may, on a reimbursable basis, provide services or detail personnel to assist with the transition.

(c) Acting officials

(1) During the transition period, pending the advice and consent of the Senate to the appointment of an officer required by this chapter to be appointed by and with such advice and consent, the President may designate any officer whose appointment was required to be made by and with such advice and consent and who was such an officer immediately before the effective date of this chapter (and who continues in office) or immediately before such designation, to act in such office until the same is filled as provided in this chapter. While so acting, such officers shall receive compensation at the higher of—

(A) the rates provided by this chapter for the respective offices in which they act; or

(B) the rates provided for the offices held at the time of designation.

(2) Nothing in this chapter shall be understood to require the advice and consent of the Senate to the appointment by the President to a position in the Department of any officer whose agency is transferred to the Department pursuant to this chapter and whose duties following such transfer are germane to those performed before such transfer.

(d) Transfer of personnel, assets, obligations, and functions

Upon the transfer of an agency to the Department—

(1) the personnel, assets, and obligations held by or available in connection with the agency shall be transferred to the Secretary for appropriate allocation, subject to the approval of the Director of the Office of Management and Budget and in accordance with the provisions of section 1531(a)(2) of title 31; and

(2) the Secretary shall have all functions relating to the agency that any other official could by

law exercise in relation to the agency immediately before such transfer, and shall have in addition all functions vested in the Secretary by this chapter or other law.

(e) Prohibition on use of transportation trust funds

(1) In general

Notwithstanding any other provision of this chapter, no funds derived from the Highway Trust Fund, Airport and Airway Trust Fund, Inland Waterway Trust Fund, or Harbor Maintenance Trust Fund, may be transferred to, made available to, or obligated by the Secretary or any other official in the Department.

(2) Limitation

This subsection shall not apply to security-related funds provided to the Federal Aviation Administration for fiscal years preceding fiscal year 2003 for (A) operations, (B) facilities and equipment, or (C) research, engineering, and development, and to any funds provided to the Coast Guard from the Sport Fish Restoration and Boating Trust Fund for boating safety programs.

(Pub. L. 107–296, title XV, §1511, Nov. 25, 2002, 116 Stat. 2309; Pub. L. 108–7, div. L, §103(4), Feb. 20, 2003, 117 Stat. 529; Pub. L. 109–59, title XI, §11115(b)(2)(F), Aug. 10, 2005, 119 Stat. 1950.)

EDITORIAL NOTES

REFERENCES IN TEXT

The effective date of this chapter, referred to in subsecs. (a) and (c)(1), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

This chapter, referred to in subsecs. (c), (d)(2), and (e)(1), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2005—Subsec. (e)(2). Pub. L. 109–59 substituted "Sport Fish Restoration and Boating Trust Fund" for "Aquatic Resources Trust Fund of the Highway Trust Fund".

2003—Subsec. (e)(2). Pub. L. 108–7 inserted before period at end ", and to any funds provided to the Coast Guard from the Aquatic Resources Trust Fund of the Highway Trust Fund for boating safety programs".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2005 AMENDMENT

Pub. L. 109–59, title XI, §11115(d), Aug. 10, 2005, 119 Stat. 1950, provided that: "The amendments made by this section [amending this section and sections 9503 and 9504 of Title 26, Internal Revenue Code] shall take effect on October 1, 2005."

§552. Savings provisions

(a) Completed administrative actions

(1) Completed administrative actions of an agency shall not be affected by the enactment of this chapter or the transfer of such agency to the Department, but shall continue in effect according to their terms until amended, modified, superseded, terminated, set aside, or revoked in accordance with law by an officer of the United States or a court of competent jurisdiction, or by operation of law.

(2) For purposes of paragraph (1), the term "completed administrative action" includes orders, determinations, rules, regulations, personnel actions, permits, agreements, grants, contracts, certificates, licenses, registrations, and privileges.

(b) Pending proceedings

Subject to the authority of the Secretary under this chapter—

(1) pending proceedings in an agency, including notices of proposed rulemaking, and applications for licenses, permits, certificates, grants, and financial assistance, shall continue notwithstanding the enactment of this chapter or the transfer of the agency to the Department, unless discontinued or modified under the same terms and conditions and to the same extent that such discontinuance could have occurred if such enactment or transfer had not occurred; and

(2) orders issued in such proceedings, and appeals therefrom, and payments made pursuant to such orders, shall issue in the same manner and on the same terms as if this chapter had not been enacted or the agency had not been transferred, and any such orders shall continue in effect until amended, modified, superseded, terminated, set aside, or revoked by an officer of the United States or a court of competent jurisdiction, or by operation of law.

(c) Pending civil actions

Subject to the authority of the Secretary under this chapter, pending civil actions shall continue notwithstanding the enactment of this chapter or the transfer of an agency to the Department, and in such civil actions, proceedings shall be had, appeals taken, and judgments rendered and enforced in the same manner and with the same effect as if such enactment or transfer had not occurred.

(d) References

References relating to an agency that is transferred to the Department in statutes, Executive orders, rules, regulations, directives, or delegations of authority that precede such transfer or the effective date of this chapter shall be deemed to refer, as appropriate, to the Department, to its officers, employees, or agents, or to its corresponding organizational units or functions. Statutory reporting requirements that applied in relation to such an agency immediately before the effective date of this chapter shall continue to apply following such transfer if they refer to the agency by name.

(e) Employment provisions

(1) Notwithstanding the generality of the foregoing (including subsections (a) and (d)), in and for the Department the Secretary may, in regulations prescribed jointly with the Director of the Office of Personnel Management, adopt the rules, procedures, terms, and conditions, established by statute, rule, or regulation before the effective date of this chapter, relating to employment in any agency transferred to the Department pursuant to this chapter; and

(2) except as otherwise provided in this chapter, or under authority granted by this chapter, the transfer pursuant to this chapter of personnel shall not alter the terms and conditions of employment, including compensation, of any employee so transferred.

(f) Statutory reporting requirements

Any statutory reporting requirement that applied to an agency, transferred to the Department under this chapter, immediately before the effective date of this chapter shall continue to apply following that transfer if the statutory requirement refers to the agency by name.

(Pub. L. 107–296, title XV, §1512, Nov. 25, 2002, 116 Stat. 2310.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The effective date of this chapter, referred to in subsecs. (d), (e)(1), and (f), is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

§552a. Savings provision of certain transfers made under the Homeland Security

Act of 2002

The transfer of functions under subtitle B of title XI of the Homeland Security Act of 2002 (Public Law 107–296) [6 U.S.C. 531 et seq.] shall not affect any pending or completed administrative actions, including orders, determinations, rules, regulations, personnel actions, permits, agreements, grants, contracts, certificates, licenses, or registrations, in effect on the date immediately prior to the date of such transfer, or any proceeding, unless and until amended, modified, superseded, terminated, set aside, or revoked. Pending civil actions shall not be affected by such transfer of functions.

(Pub. L. 108–7, div. L, §106, Feb. 20, 2003, 117 Stat. 531.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Homeland Security Act of 2002, referred to in text, is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, which is classified principally to this chapter. Subtitle B of title XI of the Act is classified principally to part B (§531 et seq.) of subchapter XI of this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

Section was enacted as part of the Homeland Security Act Amendments of 2003 and also as part of the Consolidated Appropriations Resolution, 2003, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§553. Terminations

Except as otherwise provided in this chapter, whenever all the functions vested by law in any agency have been transferred pursuant to this chapter, each position and office the incumbent of which was authorized to receive compensation at the rates prescribed for an office or position at level II, III, IV, or V, of the Executive Schedule, shall terminate.

(Pub. L. 107–296, title XV, §1513, Nov. 25, 2002, 116 Stat. 2311.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

Levels II, III, IV, and V, of the Executive Schedule, referred to in text, are set out in sections 5313, 5314, 5315, and 5316, respectively, of Title 5, Government Organization and Employees.

§554. National identification system not authorized

Nothing in this chapter shall be construed to authorize the development of a national identification system or card.

(Pub. L. 107–296, title XV, §1514, Nov. 25, 2002, 116 Stat. 2311.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title

and Tables.

§555. Continuity of Inspector General oversight

Notwithstanding the transfer of an agency to the Department pursuant to this chapter, the Inspector General that exercised oversight of such agency prior to such transfer shall continue to exercise oversight of such agency during the period of time, if any, between the transfer of such agency to the Department pursuant to this chapter and the appointment of the Inspector General of the Department of Homeland Security in accordance with section 113(b) of this title.

(Pub. L. 107–296, title XV, §1515, Nov. 25, 2002, 116 Stat. 2311.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§556. Incidental transfers

The Director of the Office of Management and Budget, in consultation with the Secretary, is authorized and directed to make such additional incidental dispositions of personnel, assets, and liabilities held, used, arising from, available, or to be made available, in connection with the functions transferred by this chapter, as the Director may determine necessary to accomplish the purposes of this chapter.

(Pub. L. 107–296, title XV, §1516, Nov. 25, 2002, 116 Stat. 2311.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§557. Reference

With respect to any function transferred by or under this chapter (including under a reorganization plan that becomes effective under section 542 of this title) and exercised on or after the effective date of this chapter, reference in any other Federal law to any department, commission, or agency or any officer or office the functions of which are so transferred shall be deemed to refer to the Secretary, other official, or component of the Department to which such function is so transferred.

(Pub. L. 107–296, title XV, §1517, Nov. 25, 2002, 116 Stat. 2311.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title

and Tables.

The effective date of this chapter, referred to in text, is 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of this title.

SUBCHAPTER XII–A—TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

§561. Definitions

In this subchapter:

(1) Administration

The term "Administration" means the Transportation Security Administration.

(2) Administrator

The term "Administrator" means the Administrator of the Transportation Security Administration.

(3) Plan

The term "Plan" means the strategic 5-year technology investment plan developed by the Administrator under section 563 of this title.

(4) Security-related technology

The term "security-related technology" means any technology that assists the Administration in the prevention of, or defense against, threats to United States transportation systems, including threats to people, property, and information.

(Pub. L. 107–296, title XVI, §1601, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2871.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 1601 of Pub. L. 107–296, title XVI, Nov. 25, 2002, 116 Stat. 2312, amended sections 114 and 40119 of Title 49, Transportation, see section 3(c) of Pub. L. 113–245, set out as a note below.

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 113–245, §2, Dec. 18, 2014, 128 Stat. 2871, provided that: "Congress finds the following:

"(1) The Transportation Security Administration has not consistently implemented Department of Homeland Security policies and Government best practices for acquisition and procurement.

"(2) The Transportation Security Administration has only recently developed a multiyear technology investment plan, and has underutilized innovation opportunities within the private sector, including from small businesses.

"(3) The Transportation Security Administration has faced challenges in meeting key performance requirements for several major acquisitions and procurements, resulting in reduced security effectiveness and wasted expenditures."

PRIOR AMENDMENTS NOT AFFECTED

Pub. L. 113–245, §3(c), Dec. 18, 2014, 128 Stat. 2877, provided that: "Nothing in this section [enacting this subchapter] may be construed to affect any amendment made by title XVI of the Homeland Security Act of

2002 [title XVI of Pub. L. 107–296, amending sections 114, 40119, 44935 and 46301 of Title 49, Transportation] as in effect before the date of enactment of this Act [Dec. 18, 2014]."

PART B—TRANSPORTATION SECURITY ADMINISTRATION ACQUISITION IMPROVEMENTS

§563. 5-year technology investment plan

(a) In general

The Administrator shall—

(1) not later than 180 days after December 18, 2014, develop and submit to Congress a strategic 5-year technology investment plan, that may include a classified addendum to report sensitive transportation security risks, technology vulnerabilities, or other sensitive security information; and

(2) to the extent possible, publish the Plan in an unclassified format in the public domain.

(b) Consultation

The Administrator shall develop the Plan in consultation with—

(1) the Under Secretary for Management;

(2) the Under Secretary for Science and Technology;

(3) the Chief Information Officer; and

(4) the aviation industry stakeholder advisory committee established by the Administrator.

(c) Approval

The Administrator may not publish the Plan under subsection (a)(2) until it has been approved by the Secretary.

(d) Contents of Plan

The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by security-related technology, including consideration of the most recent quadrennial homeland security review under section 347 of this title;

(2) a set of security-related technology acquisition needs that—

(A) is prioritized based on risk and associated capability gaps identified under paragraph (1); and

(B) includes planned technology programs and projects with defined objectives, goals, timelines, and measures;

(3) an analysis of current and forecast trends in domestic and international passenger travel;

(4) an identification of currently deployed security-related technologies that are at or near the end of their lifecycles;

(5) an identification of test, evaluation, modeling, and simulation capabilities, including target methodologies, rationales, and timelines necessary to support the acquisition of the security-related technologies expected to meet the needs under paragraph (2);

(6) an identification of opportunities for public-private partnerships, small and disadvantaged company participation, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer;

(7) an identification of the Administration's acquisition workforce needs for the management of planned security-related technology acquisitions, including consideration of leveraging acquisition expertise of other Federal agencies;

(8) an identification of the security resources, including information security resources, that will be required to protect security-related technology from physical or cyber theft, diversion,

sabotage, or attack;

(9) an identification of initiatives to streamline the Administration's acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation;

(10) an assessment of the impact to commercial aviation passengers;

(11) a strategy for consulting airport management, air carrier representatives, and Federal security directors whenever an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with such officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations; and

(12) in consultation with the National Institutes of Standards and Technology, an identification of security-related technology interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems.

(e) Leveraging the private sector

To the extent possible, and in a manner that is consistent with fair and equitable practices, the Plan shall—

(1) leverage emerging technology trends and research and development investment trends within the public and private sectors;

(2) incorporate private sector input, including from the aviation industry stakeholder advisory committee established by the Administrator, through requests for information, industry days, and other innovative means consistent with the Federal Acquisition Regulation; and

(3) in consultation with the Under Secretary for Science and Technology, identify technologies in existence or in development that, with or without adaptation, are expected to be suitable to meeting mission needs.

(f) Disclosure

The Administrator shall include with the Plan a list of nongovernment persons that contributed to the writing of the Plan.

(g) Update and report

The Administrator shall, in collaboration with relevant industry and government stakeholders, annually submit to Congress in an appendix to the budget request and publish in an unclassified format in the public domain—

(1) an update of the Plan;

(2) a report on the extent to which each security-related technology acquired by the Administration since the last issuance or update of the Plan is consistent with the planned technology programs and projects identified under subsection (d)(2) for that security-related technology; and

(3) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted.

(h) Additional update requirements

Updates and reports under subsection (g) shall—

(1) be prepared in consultation with—

(A) the persons described in subsection (b); and

(B) the Surface Transportation Security Advisory Committee established under section 204 of this title; and

(2) include—

(A) information relating to technology investments by the Transportation Security Administration and the private sector that the Department supports with research, development, testing, and evaluation for aviation, including air cargo, and surface transportation security;

(B) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted;

(C) information relating to equipment of the Transportation Security Administration that is in

operation after the end of the life-cycle of the equipment specified by the manufacturer of the equipment; and

(D) to the extent practicable, a classified addendum to report sensitive transportation security risks and associated capability gaps that would be best addressed by security-related technology described in subparagraph (A).

(i) Notice of covered changes to plan

(1) Notice required

The Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives notice of any covered change to the Plan not later than 90 days after the date that the covered change is made.

(2) Definition of covered change

In this subsection, the term "covered change" means—

(A) an increase or decrease in the dollar amount allocated to the procurement of a technology; or

(B) an increase or decrease in the number of a technology.

(Pub. L. 107–296, title XVI, §1611, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2872; amended Pub. L. 115–254, div. K, title I, §1917, Oct. 5, 2018, 132 Stat. 3557.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (g). Pub. L. 115–254, §1917(1)(A), substituted "The Administrator shall, in collaboration with relevant industry and government stakeholders, annually submit to Congress in an appendix to the budget request and publish in an unclassified format in the public domain—" for "Beginning 2 years after the date the Plan is submitted to Congress under subsection (a), and biennially thereafter, the Administrator shall submit to Congress—" in introductory provisions.

Subsec. (g)(3). Pub. L. 115–254, §1917(1)(B)–(D), added par. (3).

Subsecs. (h), (i). Pub. L. 115–254, §1917(2), added subsecs. (h) and (i).

§563a. Acquisition justification and reports

(a) Acquisition justification

Before the Administration implements any security-related technology acquisition, the Administrator, in accordance with the Department's policies and directives, shall determine whether the acquisition is justified by conducting an analysis that includes—

(1) an identification of the scenarios and level of risk to transportation security from those scenarios that would be addressed by the security-related technology acquisition;

(2) an assessment of how the proposed acquisition aligns to the Plan;

(3) a comparison of the total expected lifecycle cost against the total expected quantitative and qualitative benefits to transportation security;

(4) an analysis of alternative security solutions, including policy or procedure solutions, to determine if the proposed security-related technology acquisition is the most effective and cost-efficient solution based on cost-benefit considerations;

(5) an assessment of the potential privacy and civil liberties implications of the proposed acquisition that includes, to the extent practicable, consultation with organizations that advocate for the protection of privacy and civil liberties;

(6) a determination that the proposed acquisition is consistent with fair information practice principles issued by the Privacy Officer of the Department;

(7) confirmation that there are no significant risks to human health or safety posed by the proposed acquisition; and

(8) an estimate of the benefits to commercial aviation passengers.

(b) Reports and certification to Congress

(1) In general

Not later than the end of the 30-day period preceding the award by the Administration of a contract for any security-related technology acquisition exceeding $30,000,000, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives—

(A) the results of the comprehensive acquisition justification under subsection (a); and

(B) a certification by the Administrator that the benefits to transportation security justify the contract cost.

(2) Extension due to imminent terrorist threat

If there is a known or suspected imminent threat to transportation security, the Administrator—

(A) may reduce the 30-day period under paragraph (1) to 5 days to rapidly respond to the threat; and

(B) shall immediately notify the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives of the known or suspected imminent threat.

(Pub. L. 107–296, title XVI, §1612, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2873.)

§563b. Acquisition baseline establishment and reports

(a) Baseline requirements

(1) In general

Before the Administration implements any security-related technology acquisition, the appropriate acquisition official of the Department shall establish and document a set of formal baseline requirements.

(2) Contents

The baseline requirements under paragraph (1) shall—

(A) include the estimated costs (including lifecycle costs), schedule, and performance milestones for the planned duration of the acquisition;

(B) identify the acquisition risks and a plan for mitigating those risks; and

(C) assess the personnel necessary to manage the acquisition process, manage the ongoing program, and support training and other operations as necessary.

(3) Feasibility

In establishing the performance milestones under paragraph (2)(A), the appropriate acquisition official of the Department, to the extent possible and in consultation with the Under Secretary for Science and Technology, shall ensure that achieving those milestones is technologically feasible.

(4) Test and evaluation plan

The Administrator, in consultation with the Under Secretary for Science and Technology, shall develop a test and evaluation plan that describes—

(A) the activities that are expected to be required to assess acquired technologies against the performance milestones established under paragraph (2)(A);

(B) the necessary and cost-effective combination of laboratory testing, field testing, modeling, simulation, and supporting analysis to ensure that such technologies meet the Administration's mission needs;

(C) an efficient planning schedule to ensure that test and evaluation activities are completed without undue delay; and

(D) if commercial aviation passengers are expected to interact with the security-related

technology, methods that could be used to measure passenger acceptance of and familiarization with the security-related technology.

(5) Verification and validation

The appropriate acquisition official of the Department—

(A) subject to subparagraph (B), shall utilize independent reviewers to verify and validate the performance milestones and cost estimates developed under paragraph (2) for a security-related technology that pursuant to section 563(d)(2) of this title has been identified as a high priority need in the most recent Plan; and

(B) shall ensure that the use of independent reviewers does not unduly delay the schedule of any acquisition.

(6) Streamlining access for interested vendors

The Administrator shall establish a streamlined process for an interested vendor of a security-related technology to request and receive appropriate access to the baseline requirements and test and evaluation plans that are necessary for the vendor to participate in the acquisitions process for that technology.

(b) Review of baseline requirements and deviation; report to Congress

(1) Review

(A) In general

The appropriate acquisition official of the Department shall review and assess each implemented acquisition to determine if the acquisition is meeting the baseline requirements established under subsection (a).

(B) Test and evaluation assessment

The review shall include an assessment of whether—

(i) the planned testing and evaluation activities have been completed; and

(ii) the results of that testing and evaluation demonstrate that the performance milestones are technologically feasible.

(2) Report

Not later than 30 days after making a finding described in clause (i), (ii), or (iii) of subparagraph (A), the Administrator shall submit a report to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives that includes—

(A) the results of any assessment that finds that—

(i) the actual or planned costs exceed the baseline costs by more than 10 percent;

(ii) the actual or planned schedule for delivery has been delayed by more than 180 days; or

(iii) there is a failure to meet any performance milestone that directly impacts security effectiveness;

(B) the cause for such excessive costs, delay, or failure; and

(C) a plan for corrective action.

(Pub. L. 107–296, title XVI, §1613, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2874.)

§563c. Inventory utilization

(a) In general

Before the procurement of additional quantities of equipment to fulfill a mission need, the Administrator, to the extent practicable, shall utilize any existing units in the Administration's inventory to meet that need.

(b) Tracking of inventory

(1) In general

The Administrator shall establish a process for tracking—

(A) the location of security-related equipment in the inventory under subsection (a);

(B) the utilization status of security-related technology in the inventory under subsection (a); and

(C) the quantity of security-related equipment in the inventory under subsection (a).

(2) Internal controls

The Administrator shall implement internal controls to ensure up-to-date accurate data on security-related technology owned, deployed, and in use.

(c) Logistics management

(1) In general

The Administrator shall establish logistics principles for managing inventory in an effective and efficient manner.

(2) Limitation on just-in-time logistics

The Administrator may not use just-in-time logistics if doing so—

(A) would inhibit necessary planning for large-scale delivery of equipment to airports or other facilities; or

(B) would unduly diminish surge capacity for response to a terrorist threat.

(Pub. L. 107–296, title XVI, §1614, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2876.)

§563d. Small business contracting goals

Not later than 90 days after December 18, 2014, and annually thereafter, the Administrator shall submit a report to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives that includes—

(1) the Administration's performance record with respect to meeting its published small-business contracting goals during the preceding fiscal year;

(2) if the goals described in paragraph (1) were not met or the Administration's performance was below the published small-business contracting goals of the Department—

(A) a list of challenges, including deviations from the Administration's subcontracting plans, and factors that contributed to the level of performance during the preceding fiscal year;

(B) an action plan, with benchmarks, for addressing each of the challenges identified in subparagraph (A) that—

(i) is prepared after consultation with the Secretary of Defense and the heads of Federal departments and agencies that achieved their published goals for prime contracting with small and minority-owned businesses, including small and disadvantaged businesses, in prior fiscal years; and

(ii) identifies policies and procedures that could be incorporated by the Administration in furtherance of achieving the Administration's published goal for such contracting; and

(3) a status report on the implementation of the action plan that was developed in the preceding fiscal year in accordance with paragraph (2)(B), if such a plan was required.

(Pub. L. 107–296, title XVI, §1615, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2876.)

§563e. Consistency with the Federal Acquisition Regulation and departmental policies and directives

The Administrator shall execute the responsibilities set forth in this part in a manner consistent with, and not duplicative of, the Federal Acquisition Regulation and the Department's policies and

directives.

(Pub. L. 107–296, title XVI, §1616, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2877.)

§563f. Diversified security technology industry marketplace

(a) In general

Not later than 120 days after October 5, 2018, the Administrator shall develop and submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a strategy to promote a diverse security technology industry marketplace upon which the Administrator can rely to acquire advanced transportation security technologies or capabilities, including by increased participation of small business innovators.

(b) Contents

The strategy required under subsection (a) shall include the following:

(1) Information on how existing Administration solicitation, testing, evaluation, piloting, acquisition, and procurement processes impact the Administrator's ability to acquire from the security technology industry marketplace, including small business innovators that have not previously provided technology to the Administration, innovative technologies or capabilities with the potential to enhance transportation security.

(2) Specific actions that the Administrator will take, including modifications to the processes described in paragraph (1), to foster diversification within the security technology industry marketplace.

(3) Projected timelines for implementing the actions described in paragraph (2).

(4) Plans for how the Administrator could, to the extent practicable, assist a small business innovator periodically during such processes, including when such an innovator lacks adequate resources to participate in such processes, to facilitate an advanced transportation security technology or capability being developed and acquired by the Administrator.

(5) An assessment of the feasibility of partnering with an organization described in section 501(c)(3) of title 26 and exempt from tax under section 501(a) of title 26 to provide venture capital to businesses, particularly small business innovators, for commercialization of innovative transportation security technologies that are expected to be ready for commercialization in the near term and within 36 months.

(c) Feasibility assessment

In conducting the feasibility assessment under subsection (b)(5), the Administrator shall consider the following:

(1) Establishing an organization described in section 501(c)(3) of title 26 and exempt from tax under section 501(a) of title 26 as a venture capital partnership between the private sector and the intelligence community to help businesses, particularly small business innovators, commercialize innovative security-related technologies.

(2) Enhanced engagement through the Science and Technology Directorate of the Department of Homeland Security.

(d) Rule of construction

Nothing in this section may be construed as requiring changes to the Transportation Security Administration standards for security technology.

(e) Definitions

In this section:

(1) Intelligence community

The term "intelligence community" has the meaning given the term in section 3003 of title 50.

(2) Small business concern

The term "small business concern" has the meaning described under section 632 of title 15.

(3) Small business innovator

The term "small business innovator" means a small business concern that has an advanced transportation security technology or capability.

(Pub. L. 107–296, title XVI, §1617, as added Pub. L. 115–254, div. K, title I, §1913(a), Oct. 5, 2018, 132 Stat. 3554.)

PART C—MAINTENANCE OF SECURITY-RELATED TECHNOLOGY

§565. Maintenance validation and oversight

(a) In general

Not later than 180 days after October 5, 2018, the Administrator shall develop and implement a preventive maintenance validation process for security-related technology deployed to airports.

(b) Maintenance by Administration personnel at airports

For maintenance to be carried out by Administration personnel at airports, the process referred to in subsection (a) shall include the following:

(1) Guidance to Administration personnel at airports specifying how to conduct and document preventive maintenance actions.

(2) Mechanisms for the Administrator to verify compliance with the guidance issued pursuant to paragraph (1).

(c) Maintenance by contractors at airports

For maintenance to be carried by a contractor at airports, the process referred to in subsection (a) shall require the following:

(1) Provision of monthly preventative maintenance schedules to appropriate Administration personnel at each airport that includes information on each action to be completed by contractor.[1]

(2) Notification to appropriate Administration personnel at each airport when maintenance action is completed by a contractor.

(3) A process for independent validation by a third party of contractor maintenance.

(d) Penalties for noncompliance

The Administrator shall require maintenance for any contracts entered into 60 days after October 5, 2018, or later for security-related technology deployed to airports to include penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.

(Pub. L. 107–296, title XVI, §1621, as added Pub. L. 115–254, div. K, title I, §1918(a), Oct. 5, 2018, 132 Stat. 3558.)

[1] *So in original. Probably should be preceded by "a".*

SUBCHAPTER XIII—EMERGENCY COMMUNICATIONS

EDITORIAL NOTES

CODIFICATION

This subchapter is comprised of title XVIII of Pub. L. 107–296, as added by Pub. L. 109–295, title VI,

§671(b), Oct. 4, 2006, 120 Stat. 1433. Another title XVIII of Pub. L. 107–296 was renumbered title XIX and is classified to subchapter XIV (§591 et seq.) of this chapter.

§571. Emergency Communications Division

(a) In general

There is established in the Department an Emergency Communications Division. The Division shall be located in the Cybersecurity and Infrastructure Security Agency.

(b) Executive Assistant Director

The head of the Division shall be the Executive Assistant Director for Emergency Communications (in this section referred to as the "Executive Assistant Director"). The Executive Assistant Director shall report to the Director of the Cybersecurity and Infrastructure Security Agency. All decisions of the Executive Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director of the Cybersecurity and Infrastructure Security Agency.

(c) Responsibilities

The Executive Assistant Director shall—

(1) assist the Secretary in developing and implementing the program described in section 194(a)(1) of this title, except as provided in section 195 of this title;

(2) administer the Department's responsibilities and authorities relating to the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards;

(3) administer the Department's responsibilities and authorities relating to the Integrated Wireless Network program;

(4) conduct extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(5) conduct extensive, nationwide outreach and foster the development of interoperable emergency communications capabilities by State, regional, local, and tribal governments and public safety agencies, and by regional consortia thereof;

(6) provide technical assistance to State, regional, local, and tribal government officials with respect to use of interoperable emergency communications capabilities;

(7) coordinate with the Regional Administrators regarding the activities of Regional Emergency Communications Coordination Working Groups under section 575 of this title;

(8) promote the development of standard operating procedures and best practices with respect to use of interoperable emergency communications capabilities for incident response, and facilitate the sharing of information on such best practices for achieving, maintaining, and enhancing interoperable emergency communications capabilities for such response;

(9) coordinate, in cooperation with the National Communications System, the establishment of a national response capability with initial and ongoing planning, implementation, and training for the deployment of communications equipment for relevant State, local, and tribal governments and emergency response providers in the event of a catastrophic loss of local and regional emergency communications services;

(10) assist the President, the National Security Council, the Homeland Security Council, and the Director of the Office of Management and Budget in ensuring the continued operation of the telecommunications functions and responsibilities of the Federal Government, excluding spectrum management;

(11) establish, in coordination with the Director of the Office for Interoperability and Compatibility, requirements for interoperable emergency communications capabilities, which shall

be nonproprietary where standards for such capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance administered by the Department, excluding any alert and warning device, technology, or system;

(12) review, in consultation with the Assistant Secretary for Grants and Training, all interoperable emergency communications plans of Federal, State, local, and tribal governments, including Statewide and tactical interoperability plans, developed pursuant to homeland security assistance administered by the Department, but excluding spectrum allocation and management related to such plans;

(13) develop and update periodically, as appropriate, a National Emergency Communications Plan under section 572 of this title;

(14) perform such other duties of the Department necessary to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(15) perform other duties of the Department necessary to achieve the goal of and maintain and enhance interoperable emergency communications capabilities; and

(16) fully participate in the mechanisms required under section 652(c)(7) of this title.

(d) Performance of previously transferred functions

The Secretary shall transfer to, and administer through, the Executive Assistant Director the following programs and responsibilities:

(1) The SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards.

(2) The responsibilities of the Chief Information Officer related to the implementation of the Integrated Wireless Network.

(3) The Interoperable Communications Technical Assistance Program.

(e) Coordination

The Executive Assistant Director shall coordinate—

(1) as appropriate, with the Director of the Office for Interoperability and Compatibility with respect to the responsibilities described in section 195 of this title; and

(2) with the Administrator of the Federal Emergency Management Agency with respect to the responsibilities described in this subchapter.

(f) Sufficiency of resources plan

(1) Report

Not later than 120 days after October 4, 2006, the Secretary shall submit to Congress a report on the resources and staff necessary to carry out fully the responsibilities under this subchapter.

(2) Comptroller General review

The Comptroller General shall review the validity of the report submitted by the Secretary under paragraph (1). Not later than 60 days after the date on which such report is submitted, the Comptroller General shall submit to Congress a report containing the findings of such review.

(g) Reference

Any reference to the Assistant Director for Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Emergency Communications.

(Pub. L. 107–296, title XVIII, §1801, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1433; amended Pub. L. 115–278, §2(g)(6)(A), Nov. 16, 2018, 132 Stat. 4179; Pub. L. 116–283, div. H, title XC, §9001(e)(1), Jan. 1, 2021, 134 Stat. 4767; Pub. L. 117–263, div. G, title LXXI, §7143(c)(3), Dec. 23, 2022, 136 Stat. 3662.)

EDITORIAL NOTES

CODIFICATION

Another section 1801 of Pub. L. 107–296 was renumbered section 1901 and is classified to section 591 of this title.

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–263 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security" in two places.

2021—Subsec. (b). Pub. L. 116–283, §9001(e)(1)(A), in heading, substituted "Executive Assistant Director" for "Assistant Director" and, in text, substituted "Executive Assistant Director for Emergency Communications (in this section referred to as the 'Executive Assistant Director')." for "Assistant Director for Emergency Communications." and "Executive Assistant Director" for "Assistant Director" in two places.

Subsec. (c). Pub. L. 116–283, §9001(e)(1)(B), substituted "Executive Assistant Director" for "Assistant Director for Emergency Communications" in introductory provisions.

Subsec. (d). Pub. L. 116–283, §9001(e)(1)(C), substituted "Executive Assistant Director" for "Assistant Director for Emergency Communications" in introductory provisions.

Subsec. (e). Pub. L. 116–283, §9001(e)(1)(D), substituted "Executive Assistant Director" for "Assistant Director for Emergency Communications" in introductory provisions.

Subsec. (g). Pub. L. 116–283, §9001(e)(1)(E), added subsec. (g).

2018—Pub. L. 115–278, §2(g)(6)(A)(i), substituted "Emergency Communications Division" for "Office of Emergency Communications" in section catchline.

Subsec. (a). Pub. L. 115–278, §2(g)(6)(A)(ii), substituted "Emergency Communications Division" for "Office of Emergency Communications" and inserted at end "The Division shall be located in the Cybersecurity and Infrastructure Security Agency."

Subsec. (b). Pub. L. 115–278, §2(g)(6)(A)(iii), amended subsec. (b) generally. Prior to amendment, text read as follows: "The head of the office shall be the Director for Emergency Communications. The Director shall report to the Assistant Secretary for Cybersecurity and Communications."

Subsec. (c). Pub. L. 115–278, §2(g)(6)(A)(iv)(I), inserted "Assistant" before "Director" in introductory provisions.

Subsec. (c)(16). Pub. L. 115–278, §2(g)(6)(A)(iv)(II)–(IV), added par. (16).

Subsecs. (d), (e). Pub. L. 115–278, §2(g)(6)(A)(v), (vi), inserted "Assistant" before "Director" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Pub. L. 115–278, §2(c), Nov. 16, 2018, 132 Stat. 4175, provided that: "Any reference to—

"(1) the Office of Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Emergency Communications Division; and

"(2) the Director for Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Emergency Communications."

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

SAVINGS CLAUSE

Pub. L. 109–295, title VI, §675, Oct. 4, 2006, 120 Stat. 1444, provided that: "Nothing in this subtitle [subtitle D (§§671–675) of title VI of Pub. L. 109–295, enacting this subchapter and sections 195 and 195a of this title and provisions set out as a note under section 101 of this title] shall be construed to transfer to the Office of Emergency Communications any function, personnel, asset, component, authority, grant program, or liability of the Federal Emergency Management Agency as constituted on June 1, 2006."

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

CONTINUATION IN OFFICE

Pub. L. 116–283, div. H, title XC, §9001(e)(2), Jan. 1, 2021, 134 Stat. 4768, provided that: "The individual serving as the Assistant Director for Emergency Communications of the Department of Homeland Security on the day before the date of enactment of this Act [Jan. 1, 2021] may serve as the Executive Assistant Director for Emergency Communications on and after that date."

DIRECTOR FOR EMERGENCY COMMUNICATIONS AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR OF EMERGENCY COMMUNICATIONS

Pub. L. 115–278, §2(b)(2), Nov. 16, 2018, 132 Stat. 4175, provided that: "The individual serving as the Director for Emergency Communications of the Department of Homeland Security on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Emergency Communications of the Department on and after such date."

§572. National Emergency Communications Plan

(a) In general

The Secretary, acting through the Assistant Director for Emergency Communications, and in cooperation with the Department of National Communications System (as appropriate), shall, in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, develop not later than 180 days after the completion of the baseline assessment under section 573 of this title, and periodically update, a National Emergency Communications Plan to provide recommendations regarding how the United States should—

(1) support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) ensure, accelerate, and attain interoperable emergency communications nationwide.

(b) Coordination

The Emergency Communications Preparedness Center under section 576 of this title shall coordinate the development of the Federal aspects of the National Emergency Communications Plan.

(c) Contents

The National Emergency Communications Plan shall—

(1) include recommendations developed in consultation with the Federal Communications Commission and the National Institute of Standards and Technology for a process for expediting national voluntary consensus standards for emergency communications equipment for the purchase and use by public safety agencies of interoperable emergency communications equipment and technologies;

(2) identify the appropriate capabilities necessary for emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) identify the appropriate interoperable emergency communications capabilities necessary for Federal, State, local, and tribal governments in the event of natural disasters, acts of terrorism, and other man-made disasters;

(4) recommend both short-term and long-term solutions for ensuring that emergency response providers and relevant government officials can continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(5) recommend both short-term and long-term solutions for deploying interoperable emergency communications systems for Federal, State, local, and tribal governments throughout the Nation, including through the provision of existing and emerging technologies;

(6) identify how Federal departments and agencies that respond to natural disasters, acts of terrorism, and other man-made disasters can work effectively with State, local, and tribal governments, in all States, and with other entities;

(7) identify obstacles to deploying interoperable emergency communications capabilities

nationwide and recommend short-term and long-term measures to overcome those obstacles, including recommendations for multijurisdictional coordination among Federal, State, local, and tribal governments;

(8) recommend goals and timeframes for the deployment of emergency, command-level communications systems based on new and existing equipment across the United States and develop a timetable for the deployment of interoperable emergency communications systems nationwide;

(9) recommend appropriate measures that emergency response providers should employ to ensure the continued operation of relevant governmental communications infrastructure in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(10) set a date, including interim benchmarks, as appropriate, by which State, local, and tribal governments, Federal departments and agencies, and emergency response providers expect to achieve a baseline level of national interoperable communications, as that term is defined under section 194(g)(1) of this title.

(Pub. L. 107–296, title XVIII, §1802, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1435; amended Pub. L. 110–53, title III, §301(d), Aug. 3, 2007, 121 Stat. 300; Pub. L. 115–278, §2(g)(6)(B), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

CODIFICATION

Another section 1802 of Pub. L. 107–296 was renumbered section 1902 and is classified to section 592 of this title.

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278 substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications" in introductory provisions.

2007—Subsec. (c)(10). Pub. L. 110–53 added par. (10).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

§573. Assessments and reports

(a) Baseline assessment

Not later than 1 year after October 4, 2006, and not less than every 5 years thereafter, the Secretary, acting through the Assistant Director for Emergency Communications, shall conduct an assessment of Federal, State, local, and tribal governments that—

(1) defines the range of capabilities needed by emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(2) defines the range of interoperable emergency communications capabilities needed for specific events;

(3) assesses the current available capabilities to meet such communications needs;

(4) identifies the gap between such current capabilities and defined requirements; and

(5) includes a national interoperable emergency communications inventory to be completed by the Secretary of Homeland Security, the Secretary of Commerce, and the Chairman of the Federal Communications Commission that—

(A) identifies for each Federal department and agency—

(i) the channels and frequencies used;
(ii) the nomenclature used to refer to each channel or frequency used; and
(iii) the types of communications systems and equipment used; and

(B) identifies the interoperable emergency communications systems in use by public safety agencies in the United States.

(b) Classified annex

The baseline assessment under this section may include a classified annex including information provided under subsection (a)(5)(A).

(c) Savings clause

In conducting the baseline assessment under this section, the Secretary may incorporate findings from assessments conducted before, or ongoing on, October 4, 2006.

(d) Progress reports

Not later than one year after October 4, 2006, and biennially thereafter, the Secretary, acting through the Assistant Director for Emergency Communications, shall submit to Congress a report on the progress of the Department in achieving the goals of, and carrying out its responsibilities under, this subchapter, including—

(1) a description of the findings of the most recent baseline assessment conducted under subsection (a);

(2) a determination of the degree to which interoperable emergency communications capabilities have been attained to date and the gaps that remain for interoperability to be achieved;

(3) an evaluation of the ability to continue to communicate and to provide and maintain interoperable emergency communications by emergency managers, emergency response providers, and relevant government officials in the event of—

(A) natural disasters, acts of terrorism, or other man-made disasters, including Incidents of National Significance declared by the Secretary under the National Response Plan; and

(B) a catastrophic loss of local and regional communications services;

(4) a list of best practices relating to the ability to continue to communicate and to provide and maintain interoperable emergency communications in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(A) [1] an evaluation of the feasibility and desirability of the Department developing, on its own or in conjunction with the Department of Defense, a mobile communications capability, modeled on the Army Signal Corps, that could be deployed to support emergency communications at the site of natural disasters, acts of terrorism, or other man-made disasters.

(Pub. L. 107–296, title XVIII, §1803, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1437; amended Pub. L. 115–278, §2(g)(6)(B), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

CODIFICATION

Another section 1803 of Pub. L. 107–296 was renumbered section 1903 and is classified to section 593 of this title.

AMENDMENTS

2018—Subsecs. (a), (d). Pub. L. 115–278 substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

[1] *So in original. Probably should be "(5)".*

§574. Coordination of Department emergency communications grant programs

(a) Coordination of grants and standards programs

The Secretary, acting through the Assistant Director for Emergency Communications, shall ensure that grant guidelines for the use of homeland security assistance administered by the Department relating to interoperable emergency communications are coordinated and consistent with the goals and recommendations in the National Emergency Communications Plan under section 572 of this title.

(b) Denial of eligibility for grants

(1) In general

The Secretary, acting through the Assistant Secretary for Grants and Planning, and in consultation with the Assistant Director for Emergency Communications, may prohibit any State, local, or tribal government from using homeland security assistance administered by the Department to achieve, maintain, or enhance emergency communications capabilities, if—

(A) such government has not complied with the requirement to submit a Statewide Interoperable Communications Plan as required by section 194(f) of this title;

(B) such government has proposed to upgrade or purchase new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards and has not provided a reasonable explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards; and

(C) as of the date that is 3 years after the date of the completion of the initial National Emergency Communications Plan under section 572 of this title, national voluntary consensus standards for interoperable emergency communications capabilities have not been developed and promulgated.

(2) Standards

The Secretary, in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies with responsibility for standards, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for interoperable emergency communications.

(Pub. L. 107–296, title XVIII, §1804, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1438; amended Pub. L. 115–278, §2(g)(6)(B), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

CODIFICATION

Another section 1804 of Pub. L. 107–296 was renumbered section 1904 and is classified to section 594 of this title.

AMENDMENTS

2018—Subsecs. (a), (b)(1). Pub. L. 115–278 substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

§575. Regional emergency communications coordination

(a) In general

There is established in each Regional Office a Regional Emergency Communications Coordination Working Group (in this section referred to as an "RECC Working Group"). Each RECC Working Group shall report to the relevant Regional Administrator and coordinate its activities with the relevant Regional Advisory Council.

(b) Membership

Each RECC Working Group shall consist of the following:

(1) Non-Federal

Organizations representing the interests of the following:

(A) State officials.
(B) Local government officials, including sheriffs.
(C) State police departments.
(D) Local police departments.
(E) Local fire departments.
(F) Public safety answering points (9–1–1 services).
(G) State emergency managers, homeland security directors, or representatives of State Administrative Agencies.
(H) Local emergency managers or homeland security directors.
(I) Other emergency response providers as appropriate.

(2) Federal

Representatives from the Department, the Federal Communications Commission, and other Federal departments and agencies with responsibility for coordinating interoperable emergency communications with or providing emergency support services to State, local, and tribal governments.

(c) Coordination

Each RECC Working Group shall coordinate its activities with the following:

(1) Communications equipment manufacturers and vendors (including broadband data service providers).
(2) Local exchange carriers.
(3) Local broadcast media.
(4) Wireless carriers.
(5) Satellite communications services.
(6) Cable operators.
(7) Hospitals.
(8) Public utility services.
(9) Emergency evacuation transit services.
(10) Ambulance services.
(11) HAM and amateur radio operators.
(12) Representatives from other private sector entities and nongovernmental organizations as the Regional Administrator determines appropriate.

(d) Duties

The duties of each RECC Working Group shall include—

(1) assessing the survivability, sustainability, and interoperability of local emergency communications systems to meet the goals of the National Emergency Communications Plan;

(2) reporting annually to the relevant Regional Administrator, the Assistant Director for Emergency Communications, the Chairman of the Federal Communications Commission, and the Assistant Secretary for Communications and Information of the Department of Commerce on the status of its region in building robust and sustainable interoperable voice and data emergency communications networks and, not later than 60 days after the completion of the initial National Emergency Communications Plan under section 572 of this title, on the progress of the region in meeting the goals of such plan;

(3) ensuring a process for the coordination of effective multijurisdictional, multi-agency emergency communications networks for use during natural disasters, acts of terrorism, and other man-made disasters through the expanded use of emergency management and public safety communications mutual aid agreements; and

(4) coordinating the establishment of Federal, State, local, and tribal support services and networks designed to address the immediate and critical human needs in responding to natural disasters, acts of terrorism, and other man-made disasters.

(Pub. L. 107–296, title XVIII, §1805, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1439; amended Pub. L. 115–278, §2(g)(6)(B), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

CODIFICATION

Another section 1805 of Pub. L. 107–296 was renumbered section 1905 and was classified to section 595 of this title, prior to repeal by Pub. L. 115–387, §2(a)(4), Dec. 21, 2018, 132 Stat. 5163.

AMENDMENTS

2018—Subsec. (d)(2). Pub. L. 115–278 substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

§576. Emergency Communications Preparedness Center

(a) Establishment

There is established the Emergency Communications Preparedness Center (in this section referred to as the "Center").

(b) Operation

The Secretary, the Chairman of the Federal Communications Commission, the Secretary of Defense, the Secretary of Commerce, the Attorney General of the United States, and the heads of other Federal departments and agencies or their designees shall jointly operate the Center in accordance with the Memorandum of Understanding entitled, "Emergency Communications Preparedness Center (ECPC) Charter".

(c) Functions

The Center shall—

(1) serve as the focal point for interagency efforts and as a clearinghouse with respect to all relevant intergovernmental information to support and promote (including specifically by working to avoid duplication, hindrances, and counteractive efforts among the participating Federal departments and agencies)—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications;

(2) prepare and submit to Congress, on an annual basis, a strategic assessment regarding the coordination efforts of Federal departments and agencies to advance—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications;

(3) consider, in preparing the strategic assessment under paragraph (2), the goals stated in the National Emergency Communications Plan under section 572 of this title; and

(4) perform such other functions as are provided in the Emergency Communications Preparedness Center (ECPC) Charter described in subsection (b)(1).[1]

(Pub. L. 107–296, title XVIII, §1806, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1440.)

EDITORIAL NOTES

CODIFICATION

Another section 1806 of Pub. L. 107–296 was renumbered section 1906 and is classified to section 596 of this title.

[1] *So in original. Subsection (b) of this section does not contain a paragraph (1).*

§577. Urban and other high risk area communications capabilities

(a) In general

The Secretary, in consultation with the Chairman of the Federal Communications Commission and the Secretary of Defense, and with appropriate State, local, and tribal government officials, shall provide technical guidance, training, and other assistance, as appropriate, to support the rapid establishment of consistent, secure, and effective interoperable emergency communications capabilities in the event of an emergency in urban and other areas determined by the Secretary to be at consistently high levels of risk from natural disasters, acts of terrorism, and other man-made disasters.

(b) Minimum capabilities

The interoperable emergency communications capabilities established under subsection (a) shall ensure the ability of all levels of government, emergency response providers, the private sector, and other organizations with emergency response capabilities—

(1) to communicate with each other in the event of an emergency;

(2) to have appropriate and timely access to the Information Sharing Environment described in section 485 of this title; and

(3) to be consistent with any applicable State or Urban Area homeland strategy or plan.

(Pub. L. 107–296, title XVIII, §1807, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1441.)

§578. Definition

In this subchapter, the term "interoperable" has the meaning given the term "interoperable communications" under section 194(g)(1) of this title.

(Pub. L. 107–296, title XVIII, §1808, as added Pub. L. 109–295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1441.)

§579. Interoperable Emergency Communications Grant Program

(a) Establishment

The Secretary shall establish the Interoperable Emergency Communications Grant Program to make grants to States to carry out initiatives to improve local, tribal, statewide, regional, national and, where appropriate, international interoperable emergency communications, including communications in collective response to natural disasters, acts of terrorism, and other man-made disasters.

(b) Policy

The Assistant Director for Emergency Communications shall ensure that a grant awarded to a State under this section is consistent with the policies established pursuant to the responsibilities and authorities of the Emergency Communications Division under this subchapter, including ensuring that activities funded by the grant—

(1) comply with the statewide plan for that State required by section 194(f) of this title; and

(2) comply with the National Emergency Communications Plan under section 572 of this title, when completed.

(c) Administration

(1) In general

The Administrator of the Federal Emergency Management Agency shall administer the Interoperable Emergency Communications Grant Program pursuant to the responsibilities and authorities of the Administrator under subchapter V.

(2) Guidance

In administering the grant program, the Administrator shall ensure that the use of grants is consistent with guidance established by the Assistant Director for Emergency Communications pursuant to section 194(a)(1)(H) of this title.

(d) Use of funds

A State that receives a grant under this section shall use the grant to implement that State's Statewide Interoperability Plan required under section 194(f) of this title and approved under subsection (e), and to assist with activities determined by the Secretary to be integral to interoperable emergency communications.

(e) Approval of plans

(1) Approval as condition of grant

Before a State may receive a grant under this section, the Assistant Director for Emergency Communications shall approve the State's Statewide Interoperable Communications Plan required under section 194(f) of this title.

(2) Plan requirements

In approving a plan under this subsection, the Assistant Director for Emergency Communications shall ensure that the plan—

(A) is designed to improve interoperability at the city, county, regional, State and interstate level;

(B) considers any applicable local or regional plan; and

(C) complies, to the maximum extent practicable, with the National Emergency Communications Plan under section 572 of this title.

(3) Approval of revisions

The Assistant Director for Emergency Communications may approve revisions to a State's plan if the Assistant Director determines that doing so is likely to further interoperability.

(f) Limitations on uses of funds

(1) In general

The recipient of a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any State or local government cost-sharing contribution; or

(C) for recreational or social purposes.

(2) Penalties

In addition to other remedies currently available, the Secretary may take such actions as necessary to ensure that recipients of grant funds are using the funds for the purpose for which they were intended.

(g) Limitations on award of grants

(1) National emergency communications plan required

The Secretary may not award a grant under this section before the date on which the Secretary completes and submits to Congress the National Emergency Communications Plan required under section 572 of this title.

(2) Voluntary consensus standards

The Secretary may not award a grant to a State under this section for the purchase of equipment that does not meet applicable voluntary consensus standards, unless the State demonstrates that there are compelling reasons for such purchase.

(h) Award of grants

In approving applications and awarding grants under this section, the Secretary shall consider—

(1) the risk posed to each State by natural disasters, acts of terrorism, or other manmade disasters, including—

(A) the likely need of a jurisdiction within the State to respond to such risk in nearby jurisdictions;

(B) the degree of threat, vulnerability, and consequences related to critical infrastructure (from all critical infrastructure sectors) or key resources identified by the Administrator or the State homeland security and emergency management plans, including threats to, vulnerabilities of, and consequences from damage to critical infrastructure and key resources in nearby jurisdictions;

(C) the size of the population and density of the population of the State, including appropriate consideration of military, tourist, and commuter populations;

(D) whether the State is on or near an international border;

(E) whether the State encompasses an economically significant border crossing; and

(F) whether the State has a coastline bordering an ocean, a major waterway used for interstate commerce, or international waters; and

(2) the anticipated effectiveness of the State's proposed use of grant funds to improve interoperability.

(i) Opportunity to amend applications

In considering applications for grants under this section, the Administrator shall provide applicants with a reasonable opportunity to correct defects in the application, if any, before making final awards.

(j) Minimum grant amounts

(1) States

In awarding grants under this section, the Secretary shall ensure that for each fiscal year, except as provided in paragraph (2), no State receives a grant in an amount that is less than the following percentage of the total amount appropriated for grants under this section for that fiscal year:

(A) For fiscal year 2008, 0.50 percent.

(B) For fiscal year 2009, 0.50 percent.

(C) For fiscal year 2010, 0.45 percent.

(D) For fiscal year 2011, 0.40 percent.

(E) For fiscal year 2012 and each subsequent fiscal year, 0.35 percent.

(2) Territories and possessions

In awarding grants under this section, the Secretary shall ensure that for each fiscal year, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands each receive grants in amounts that are not less than 0.08 percent of the total amount appropriated for grants under this section for that fiscal year.

(k) Certification

Each State that receives a grant under this section shall certify that the grant is used for the purpose for which the funds were intended and in compliance with the State's approved Statewide Interoperable Communications Plan.

(l) State responsibilities

(1) Availability of funds to local and tribal governments

Not later than 45 days after receiving grant funds, any State that receives a grant under this section shall obligate or otherwise make available to local and tribal governments—

(A) not less than 80 percent of the grant funds;

(B) with the consent of local and tribal governments, eligible expenditures having a value of not less than 80 percent of the amount of the grant; or

(C) grant funds combined with other eligible expenditures having a total value of not less than 80 percent of the amount of the grant.

(2) Allocation of funds

A State that receives a grant under this section shall allocate grant funds to tribal governments in the State to assist tribal communities in improving interoperable communications, in a manner consistent with the Statewide Interoperable Communications Plan. A State may not impose unreasonable or unduly burdensome requirements on a tribal government as a condition of providing grant funds or resources to the tribal government.

(3) Penalties

If a State violates the requirements of this subsection, in addition to other remedies available to the Secretary, the Secretary may terminate or reduce the amount of the grant awarded to that State or transfer grant funds previously awarded to the State directly to the appropriate local or tribal government.

(m) Reports

(1) Annual reports by State grant recipients

A State that receives a grant under this section shall annually submit to the Assistant Director for Emergency Communications a report on the progress of the State in implementing that State's Statewide Interoperable Communications Plans required under section 194(f) of this title and achieving interoperability at the city, county, regional, State, and interstate levels. The Assistant Director shall make the reports publicly available, including by making them available on the Internet website of the Cybersecurity and Infrastructure Security Agency, subject to any redactions that the Assistant Director determines are necessary to protect classified or other sensitive information.

(2) Annual reports to Congress

At least once each year, the Assistant Director for Emergency Communications shall submit to Congress a report on the use of grants awarded under this section and any progress in implementing Statewide Interoperable Communications Plans and improving interoperability at the city, county, regional, State, and interstate level, as a result of the award of such grants.

(n) Rule of construction

Nothing in this section shall be construed or interpreted to preclude a State from using a grant awarded under this section for interim or long-term Internet Protocol-based interoperable solutions.

(o) Authorization of appropriations

There are authorized to be appropriated for grants under this section—

(1) for fiscal year 2008, such sums as may be necessary;

(2) for each of fiscal years 2009 through 2012, $400,000,000; and

(3) for each subsequent fiscal year, such sums as may be necessary.

(Pub. L. 107–296, title XVIII, §1809, as added Pub. L. 110–53, title III, §301(a), Aug. 3, 2007, 121 Stat. 296; amended Pub. L. 115–278, §2(g)(6)(C), Nov. 16, 2018, 132 Stat. 4179.)

EDITORIAL NOTES

AMENDMENTS

2018—Pub. L. 115–278, §2(g)(6)(C)(i), substituted "Assistant Director for Emergency Communications" for "Director of Emergency Communications" wherever appearing.

Subsec. (b). Pub. L. 115–278, §2(g)(6)(C)(ii), substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications" and "Emergency Communications Division" for "Office of Emergency Communications" in introductory provisions.

Subsec. (e)(3). Pub. L. 115–278, §2(g)(6)(C)(iii), substituted "the Assistant Director" for "the Director".

Subsec. (m)(1). Pub. L. 115–278, §2(g)(6)(C)(iv), substituted "The Assistant Director" for "the Director", "Cybersecurity and Infrastructure Security Agency" for "Office of Emergency Communications", and "the Assistant Director determines" for "the Director determines".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

§580. Border interoperability demonstration project

(a) In general

(1) Establishment

The Secretary, acting through the Assistant Director for Emergency Communications (referred to in this section as the "Assistant Director"), and in coordination with the Federal Communications Commission and the Secretary of Commerce, shall establish an International Border Community Interoperable Communications Demonstration Project (referred to in this section as the "demonstration project").

(2) Minimum number of communities

The Assistant Director shall select no fewer than 6 communities to participate in a demonstration project.

(3) Location of communities

No fewer than 3 of the communities selected under paragraph (2) shall be located on the northern border of the United States and no fewer than 3 of the communities selected under

paragraph (2) shall be located on the southern border of the United States.

(b) Conditions

The Assistant Director, in coordination with the Federal Communications Commission and the Secretary of Commerce, shall ensure that the project is carried out as soon as adequate spectrum is available as a result of the 800 megahertz rebanding process in border areas, and shall ensure that the border projects do not impair or impede the rebanding process, but under no circumstances shall funds be distributed under this section unless the Federal Communications Commission and the Secretary of Commerce agree that these conditions have been met.

(c) Program requirements

Consistent with the responsibilities of the Emergency Communications Division under section 571 of this title, the Assistant Director shall foster local, tribal, State, and Federal interoperable emergency communications, as well as interoperable emergency communications with appropriate Canadian and Mexican authorities in the communities selected for the demonstration project. The Assistant Director shall—

(1) identify solutions to facilitate interoperable communications across national borders expeditiously;

(2) help ensure that emergency response providers can communicate with each other in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) provide technical assistance to enable emergency response providers to deal with threats and contingencies in a variety of environments;

(4) identify appropriate joint-use equipment to ensure communications access;

(5) identify solutions to facilitate communications between emergency response providers in communities of differing population densities; and

(6) take other actions or provide equipment as the Assistant Director deems appropriate to foster interoperable emergency communications.

(d) Distribution of funds

(1) In general

The Secretary shall distribute funds under this section to each community participating in the demonstration project through the State, or States, in which each community is located.

(2) Other participants

A State shall make the funds available promptly to the local and tribal governments and emergency response providers selected by the Secretary to participate in the demonstration project.

(3) Report

Not later than 90 days after a State receives funds under this subsection the State shall report to the Assistant Director on the status of the distribution of such funds to local and tribal governments.

(e) Maximum period of grants

The Assistant Director may not fund any participant under the demonstration project for more than 3 years.

(f) Transfer of information and knowledge

The Assistant Director shall establish mechanisms to ensure that the information and knowledge gained by participants in the demonstration project are transferred among the participants and to other interested parties, including other communities that submitted applications to the participant in the project.

(g) Authorization of appropriations

There is authorized to be appropriated for grants under this section such sums as may be necessary.

(Pub. L. 107–296, title XVIII, §1810, as added Pub. L. 110–53, title III, §302(a), Aug. 3, 2007, 121 Stat. 300; amended Pub. L. 115–278, §2(g)(6)(D), Nov. 16, 2018, 132 Stat. 4180.)

EDITORIAL NOTES

AMENDMENTS

2018—Pub. L. 115–278, §2(g)(6)(D)(iii), substituted "Assistant Director" for "Director" wherever appearing.

Subsec. (a)(1). Pub. L. 115–278, §2(g)(6)(D)(i), substituted "Assistant Director for Emergency Communications (referred to in this section as the 'Assistant Director')" for "Director of the Office of Emergency Communications (referred to in this section as the 'Director')".

Subsec. (c). Pub. L. 115–278, §2(g)(6)(D)(ii), substituted "Emergency Communications Division" for "Office of Emergency Communications" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

SUBCHAPTER XIV—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

EDITORIAL NOTES

CODIFICATION

Pub. L. 115–387, §2(a)(1), Dec. 21, 2018, 132 Stat. 5162, substituted "COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE" for "DOMESTIC NUCLEAR DETECTION OFFICE" in subchapter heading.

This subchapter is comprised of title XIX, formerly title XVIII, of Pub. L. 107–296, as added by Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1932, and renumbered title XIX by Pub. L. 110–53, title I, §104(a)(1), Aug. 3, 2007, 121 Stat. 294.

§590. Definitions

In this subchapter:

(1) Assistant Secretary

The term "Assistant Secretary" means the Assistant Secretary for the Countering Weapons of Mass Destruction Office.

(2) Intelligence community

The term "intelligence community" has the meaning given such term in section 3003(4) of title 50.

(3) Office

The term "Office" means the Countering Weapons of Mass Destruction Office established under section 591(a) of this title.

(4) Weapon of mass destruction

The term "weapon of mass destruction" has the meaning given the term in section 1801 of title 50.

(Pub. L. 107–296, title XIX, §1900, as added Pub. L. 115–387, §2(a)(2), Dec. 21, 2018, 132 Stat. 5162.)

PART A—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

§591. Countering Weapons of Mass Destruction Office

(a) Establishment

There is established in the Department a Countering Weapons of Mass Destruction Office.

(b) Assistant Secretary

The Office shall be headed by an Assistant Secretary for the Countering Weapons of Mass Destruction Office, who shall be appointed by the President.

(c) Responsibilities

The Assistant Secretary shall serve as the Secretary's principal advisor on—

(1) weapons of mass destruction matters and strategies; and

(2) coordinating the efforts of the Department to counter weapons of mass destruction.

(d) Details

The Secretary may request that the Secretary of Defense, the Secretary of Energy, the Secretary of State, the Attorney General, the Nuclear Regulatory Commission, and the heads of other Federal agencies, including elements of the intelligence community, provide for the reimbursable detail of personnel with relevant expertise to the Office.

(e) Termination

The Office shall terminate on the date that is 5 years after December 21, 2018.

(Pub. L. 107–296, title XIX, §1901, as added Pub. L. 115–387, §2(a)(2), Dec. 21, 2018, 132 Stat. 5162.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 591, Pub. L. 107–296, title XIX, §1901, formerly title XVIII, §1801, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1932; renumbered title XIX, §1901, Pub. L. 110–53, title I, §104(a)(1), (2), Aug. 3, 2007, 121 Stat. 294, related to establishment of a Domestic Nuclear Detection Office, prior to repeal by Pub. L. 115–387, §2(a)(2), Dec. 21, 2018, 132 Stat. 5162.

STATUTORY NOTES AND RELATED SUBSIDIARIES

REFERENCES AND CONSTRUCTION

Pub. L. 115–387, §2(b), Dec. 21, 2018, 132 Stat. 5166, provided that:

"(1) IN GENERAL.—Any reference in any law, regulation, document, paper, or other record of the United States to—

"(A) the Domestic Nuclear Detection Office shall be deemed to be a reference to the Countering Weapons of Mass Destruction Office; and

"(B) the Director for Domestic Nuclear Detection shall be deemed to be a reference to the Assistant Secretary for the Countering Weapons of Mass Destruction Office.

"(2) CONSTRUCTION.—Sections 1923 through 1927 of the Homeland Security Act of 2002 [6 U.S.C. 592, 593, 594, 596, 596a], as redesignated by subsection (a), shall be construed to cover the chemical and biological responsibilities of the Assistant Secretary for the Countering Weapons of Mass Destruction Office.

"(3) AUTHORITY.—The authority of the Director of the Domestic Nuclear Detection Office to make grants or enter into cooperative agreements is transferred to the Assistant Secretary for the Countering

Weapons of Mass Destruction Office, and such authority shall be construed to include grants for all purposes of title XIX of the Homeland Security Act of 2002 [6 U.S.C. 590 et seq.], as amended by this Act."

DOMESTIC NUCLEAR DETECTION OFFICE AND OFFICE OF HEALTH AFFAIRS: ABOLISHMENT AND TRANSFER TO COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

Pub. L. 115–387, §2(e), Dec. 21, 2018, 132 Stat. 5167, provided that:

"(1) TRANSFERS.—The Secretary of Homeland Security shall transfer to—

"(A) the Countering Weapons of Mass Destruction Office all functions, personnel, budget authority, and assets of—

"(i) the Domestic Nuclear Detection Office, as in existence on the day before the date of the enactment of this Act [Dec. 21, 2018]; and

"(ii) the Office of Health Affairs, as in existence on the day before the date of the enactment of this Act, except for the functions, personnel, budget authority, and assets of such office necessary to perform the functions specified in section 710 of the Homeland Security Act of 2002 [6 U.S.C. 350] (relating to workforce health and medical support), as added by this Act; and

"(B) the Management Directorate of the Department of Homeland Security all functions, personnel, budget authority, and assets of the Office of Health Affairs, as in existence on the day before the date of the enactment of this Act, that are necessary to perform the functions of such section 710.

"(2) ABOLISHMENT.—Upon completion of all transfers pursuant to paragraph (1)—

"(A) the Domestic Nuclear Detection Office of the Department of Homeland Security and the Office of Health Affairs of the Department of Homeland Security are abolished; and

"(B) the positions of Assistant Secretary for Health Affairs and Director for Domestic Nuclear Detection are abolished."

DEPARTMENT OF HOMELAND SECURITY CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR ACTIVITIES

Pub. L. 115–387, §2(g), Dec. 21, 2018, 132 Stat. 5169, provided that: "Not later than one year after the date of the enactment of this Act [Dec. 21, 2018], and annually thereafter, the Secretary of Homeland Security shall provide a briefing and report to the appropriate congressional committees (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) on—

"(1) the organization and management of the chemical, biological, radiological, and nuclear activities of the Department of Homeland Security, including research and development activities, and the location of each activity under the organizational structure of the Countering Weapons of Mass Destruction Office;

"(2) a comprehensive inventory of chemical, biological, radiological, and nuclear activities, including research and development activities, of the Department of Homeland Security, highlighting areas of collaboration between components, coordination with other agencies, and the effectiveness and accomplishments of consolidated chemical, biological, radiological, and nuclear activities of the Department of Homeland Security, including research and development activities;

"(3) information relating to how the organizational structure of the Countering Weapons of Mass Destruction Office will enhance the development of chemical, biological, radiological, and nuclear priorities and capabilities across the Department of Homeland Security;

"(4) a discussion of any resulting cost savings and efficiencies gained through activities described in paragraphs (1) and (2);

"(5) information on how the Assistant Secretary for the Countering Weapons of Mass Destruction Office is coordinating with the Under Secretary of Science and Technology of the Department of Homeland Security on research and development activities; and

"(6) recommendations for any necessary statutory changes, or, if no statutory changes are necessary, an explanation of why no statutory or organizational changes are necessary."

PART B—MISSION OF THE OFFICE

§591g. Mission of the Office

The Office shall be responsible for coordinating with other Federal efforts and developing a

strategy and policy for the Department to plan for, detect, and protect against the importation, possession, storage, transportation, development, or use of unauthorized chemical, biological, radiological, or nuclear materials, devices, or agents in the United States and to protect against an attack using such materials, devices, or agents against the people, territory, or interests of the United States.

(Pub. L. 107–296, title XIX, §1921, as added Pub. L. 115–387, §2(a)(3), Dec. 21, 2018, 132 Stat. 5163.)

§591h. Relationship to other Department components and Federal agencies

(a) In general

The authority of the Assistant Secretary under this subchapter shall not affect or diminish the authority or the responsibility of any officer of the Department or any officer of any other Federal agency with respect to the command, control, or direction of the functions, personnel, funds, assets, or liabilities of any component of the Department or any other Federal agency.

(b) Office for Strategy, Policy, and Plans

Not later than one year after December 21, 2018, the Assistant Secretary shall, in coordination with the Under Secretary for Strategy, Policy, and Plans, submit to the appropriate congressional committees a strategy and implementation plan to direct programs within the Office and to integrate those programs with other programs and activities of the Department.

(c) Federal Emergency Management Agency

Nothing in this subchapter or any other provision of law may be construed to affect or reduce the responsibilities of the Federal Emergency Management Agency or the Administrator of the Agency, including the diversion of any asset, function, or mission of the Agency or the Administrator of the Agency.

(Pub. L. 107–296, title XIX, §1922, as added Pub. L. 115–387, §2(a)(3), Dec. 21, 2018, 132 Stat. 5163.)

§592. Responsibilities

(a) Mission

The Office shall be responsible for coordinating Federal efforts to detect and protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using such devices or materials against the people, territory, or interests of the United States and, to this end, shall—

(1) serve as the primary entity of the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States, and improve that system over time;

(2) enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(3) establish, with the approval of the Secretary and in coordination with the Attorney General, the Secretary of Defense, and the Secretary of Energy, additional protocols and procedures for use within the United States to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Secretary, the Secretary of Defense, the Secretary of Energy, and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities;

(4) develop, with the approval of the Secretary and in coordination with the Attorney General,

the Secretary of State, the Secretary of Defense, and the Secretary of Energy, an enhanced global nuclear detection architecture with implementation under which—

(A) the Office will be responsible for the implementation of the domestic portion of the global architecture;

(B) the Secretary of Defense will retain responsibility for implementation of Department of Defense requirements within and outside the United States; and

(C) the Secretary of State, the Secretary of Defense, and the Secretary of Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with applicable law and relevant international arrangements;

(5) ensure that the expertise necessary to accurately interpret detection data is made available in a timely manner for all technology deployed by the Office to implement the global nuclear detection architecture;

(6) conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development to generate and improve technologies to detect and prevent the illicit entry, transport, assembly, or potential use within the United States of a nuclear explosive device or fissile or radiological material, and coordinate with the Under Secretary for Science and Technology on basic and advanced or transformational research and development efforts relevant to the mission of both organizations;

(7) carry out a program to test and evaluate technology for detecting a nuclear explosive device and fissile or radiological material, in coordination with the Secretary of Defense and the Secretary of Energy, as appropriate, and establish performance metrics for evaluating the effectiveness of individual detectors and detection systems in detecting such devices or material—

(A) under realistic operational and environmental conditions; and

(B) against realistic adversary tactics and countermeasures;

(8) support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to such entities;

(9) further enhance and maintain continuous awareness by analyzing information from all Office mission-related detection systems;

(10) lead the development and implementation of the national strategic five-year plan for improving the nuclear forensic and attribution capabilities of the United States required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010;

(11) establish, within the Office, the National Technical Nuclear Forensics Center to provide centralized stewardship, planning, assessment, gap analysis, exercises, improvement, and integration for all Federal nuclear forensics and attribution activities—

(A) to ensure an enduring national technical nuclear forensics capability to strengthen the collective response of the United States to nuclear terrorism or other nuclear attacks; and

(B) to coordinate and implement the national strategic five-year plan referred to in paragraph (10);

(12) establish a National Nuclear Forensics Expertise Development Program, which—

(A) is devoted to developing and maintaining a vibrant and enduring academic pathway from undergraduate to post-doctorate study in nuclear and geochemical science specialties directly relevant to technical nuclear forensics, including radiochemistry, geochemistry, nuclear physics, nuclear engineering, materials science, and analytical chemistry;

(B) shall—

(i) make available for undergraduate study student scholarships, with a duration of up to 4 years per student, which shall include, if possible, at least 1 summer internship at a national laboratory or appropriate Federal agency in the field of technical nuclear forensics during the

course of the student's undergraduate career;

(ii) make available for doctoral study student fellowships, with a duration of up to 5 years per student, which shall—

(I) include, if possible, at least 2 summer internships at a national laboratory or appropriate Federal agency in the field of technical nuclear forensics during the course of the student's graduate career; and

(II) require each recipient to commit to serve for 2 years in a post-doctoral position in a technical nuclear forensics-related specialty at a national laboratory or appropriate Federal agency after graduation;

(iii) make available to faculty awards, with a duration of 3 to 5 years each, to ensure faculty and their graduate students have a sustained funding stream; and

(iv) place a particular emphasis on reinvigorating technical nuclear forensics programs while encouraging the participation of undergraduate students, graduate students, and university faculty from historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, Asian American and Native American Pacific Islander-serving institutions, Alaska Native-serving institutions, and Hawaiian Native-serving institutions; and

(C) shall—

(i) provide for the selection of individuals to receive scholarships or fellowships under this section through a competitive process primarily on the basis of academic merit and the nuclear forensics and attribution needs of the United States Government;

(ii) provide for the setting aside of up to 10 percent of the scholarships or fellowships awarded under this section for individuals who are Federal employees to enhance the education of such employees in areas of critical nuclear forensics and attribution needs of the United States Government, for doctoral education under the scholarship on a full-time or part-time basis;

(iii) provide that the Secretary may enter into a contractual agreement with an institution of higher education under which the amounts provided for a scholarship under this section for tuition, fees, and other authorized expenses are paid directly to the institution with respect to which such scholarship is awarded;

(iv) require scholarship recipients to maintain satisfactory academic progress; and

(v) require that—

(I) a scholarship recipient who fails to maintain a high level of academic standing, as defined by the Secretary, who is dismissed for disciplinary reasons from the educational institution such recipient is attending, or who voluntarily terminates academic training before graduation from the educational program for which the scholarship was awarded shall be liable to the United States for repayment within 1 year after the date of such default of all scholarship funds paid to such recipient and to the institution of higher education on the behalf of such recipient, provided that the repayment period may be extended by the Secretary if the Secretary determines it necessary, as established by regulation; and

(II) a scholarship recipient who, for any reason except death or disability, fails to begin or complete the post-doctoral service requirements in a technical nuclear forensics-related specialty at a national laboratory or appropriate Federal agency after completion of academic training shall be liable to the United States for an amount equal to—

(aa) the total amount of the scholarship received by such recipient under this section; and

(bb) the interest on such amounts which would be payable if at the time the scholarship was received such scholarship was a loan bearing interest at the maximum legally prevailing rate;

(13) provide an annual report to Congress on the activities carried out under paragraphs (10), (11), and (12); and

(14) perform other duties as assigned by the Secretary.

(b) Definitions

In this section:

(1) Alaska Native-serving institution

The term "Alaska Native-serving institution" has the meaning given the term in section 1059d of title 20.

(2) Asian American and Native American Pacific Islander-serving institution

The term "Asian American and Native American Pacific Islander-serving institution" has the meaning given the term in section 1059g of title 20.

(3) Hawaiian native-serving institution

The term "Hawaiian native-serving institution" [1] has the meaning given the term in section 1059d of title 20.

(4) Hispanic-serving institution

The term "Hispanic-serving institution" has the meaning given that term in section 1101a of title 20.

(5) Historically Black college or university

The term "historically Black college or university" has the meaning given the term "part B institution" in section 1061(2) of title 20.

(6) Tribal College or University

The term "Tribal College or University" has the meaning given that term in section 1059c(b) of title 20.

(Pub. L. 107–296, title XIX, §1923, formerly title XVIII, §1802, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1932; renumbered title XIX, §1902, Pub. L. 110–53, title I, §104(a)(1), (2), Aug. 3, 2007, 121 Stat. 294; amended Pub. L. 111–140, §4(a), Feb. 16, 2010, 124 Stat. 32; renumbered §1923 and amended Pub. L. 115–387, §2(a)(5), (6), Dec. 21, 2018, 132 Stat. 5163, 5164.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1036 of the National Defense Authorization Act for Fiscal Year 2010, referred to in subsec. (a)(10), is section 1036 of Pub. L. 111–84, Oct. 28, 2009, 123 Stat. 2190, which is not classified to the Code. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2018—Pub. L. 115–387, §2(a)(6)(A), substituted "Responsibilities" for "Mission of Office" in section catchline.

Subsec. (a)(11). Pub. L. 115–387, §2(a)(6)(B), substituted "Office" for "Domestic Nuclear Detection Office" in introductory provisions.

2010—Subsec. (a)(10) to (14). Pub. L. 111–140, §4(a)(1), added pars. (10) to (13) and redesignated former par. (10) as (14).

Subsec. (b). Pub. L. 111–140, §4(a)(2), added subsec. (b).

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 111–140, §2, Feb. 16, 2010, 124 Stat. 31, provided that: "Congress finds the following:

"(1) The threat of a nuclear terrorist attack on American interests, both domestic and abroad, is one of

the most serious threats to the national security of the United States. In the wake of an attack, attribution of responsibility would be of utmost importance. Because of the destructive power of a nuclear weapon, there could be little forensic evidence except the radioactive material in the weapon itself.

"(2) Through advanced nuclear forensics, using both existing techniques and those under development, it may be possible to identify the source and pathway of a weapon or material after it is interdicted or detonated. Though identifying intercepted smuggled material is now possible in some cases, pre-detonation forensics is a relatively undeveloped field. The post-detonation nuclear forensics field is also immature, and the challenges are compounded by the pressures and time constraints of performing forensics after a nuclear or radiological attack.

"(3) A robust and well-known capability to identify the source of nuclear or radiological material intended for or used in an act of terror could also deter prospective proliferators. Furthermore, the threat of effective attribution could compel improved security at material storage facilities, preventing the unwitting transfer of nuclear or radiological materials.

"(4)(A) In order to identify special nuclear material and other radioactive materials confidently, it is necessary to have a robust capability to acquire samples in a timely manner, analyze and characterize samples, and compare samples against known signatures of nuclear and radiological material.

"(B) Many of the radioisotopes produced in the detonation of a nuclear device have short half-lives, so the timely acquisition of samples is of the utmost importance. Over the past several decades, the ability of the United States to gather atmospheric samples—often the preferred method of sample acquisition—has diminished. This ability must be restored and modern techniques that could complement or replace existing techniques should be pursued.

"(C) The discipline of pre-detonation forensics is a relatively undeveloped field. The radiation associated with a nuclear or radiological device may affect traditional forensics techniques in unknown ways. In a post-detonation scenario, radiochemistry may provide the most useful tools for analysis and characterization of samples. The number of radiochemistry programs and radiochemists in United States National Laboratories and universities has dramatically declined over the past several decades. The narrowing pipeline of qualified people into this critical field is a serious impediment to maintaining a robust and credible nuclear forensics program.

"(5) Once samples have been acquired and characterized, it is necessary to compare the results against samples of known material from reactors, weapons, and enrichment facilities, and from medical, academic, commercial, and other facilities containing such materials, throughout the world. Some of these samples are available to the International Atomic Energy Agency through safeguards agreements, and some countries maintain internal sample databases. Access to samples in many countries is limited by national security concerns.

"(6) In order to create a sufficient deterrent, it is necessary to have the capability to positively identify the source of nuclear or radiological material, and potential traffickers in nuclear or radiological material must be aware of that capability. International cooperation may be essential to catalogue all existing sources of nuclear or radiological material."

[1] So in original. Section 1059d of title 20 defines "Native Hawaiian-serving institution".

§592a. Technology research and development investment strategy for nuclear and radiological detection

(a) In general

Not later than 1 year after October 13, 2006, the Secretary, the Secretary of Energy, the Secretary of Defense, and the Director of National Intelligence shall submit to Congress a research and development investment strategy for nuclear and radiological detection.

(b) Contents

The strategy under subsection (a) shall include—

(1) a long term technology roadmap for nuclear and radiological detection applicable to the mission needs of the Department, the Department of Energy, the Department of Defense, and the Office of the Director of National Intelligence;

(2) budget requirements necessary to meet the roadmap; and

(3) documentation of how the Department, the Department of Energy, the Department of Defense, and the Office of the Director of National Intelligence will execute this strategy.

(c) Initial report

Not later than 1 year after October 13, 2006, the Secretary shall submit a report to the appropriate congressional committees on—

(1) the impact of this title,[1] and the amendments made by this title, on the responsibilities under section 182 of this title; and

(2) the efforts of the Department to coordinate, integrate, and establish priorities for conducting all basic and applied research, development, testing, and evaluation of technology and systems to detect, prevent, protect, and respond to chemical, biological, radiological, and nuclear terrorist attacks.

(d) Annual report

The Director for Domestic Nuclear Detection [2] and the Under Secretary for Science and Technology shall jointly and annually notify Congress that the strategy and technology road map for nuclear and radiological detection developed under subsections (a) and (b) is consistent with the national policy and strategic plan for identifying priorities, goals, objectives, and policies for coordinating the Federal Government's civilian efforts to identify and develop countermeasures to terrorist threats from weapons of mass destruction that are required under section 182(2) of this title.

(Pub. L. 109–347, title V, §502, Oct. 13, 2006, 120 Stat. 1935.)

EDITORIAL NOTES

REFERENCES IN TEXT

This title, referred to in subsec. (c)(1), is title V of Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1932, which enacted this subchapter and this section and amended sections 113 and 182 of this title. For complete classification of title V to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director for Domestic Nuclear Detection deemed to be a reference to the Assistant Secretary for the Countering Weapons of Mass Destruction Office, see section 2(b)(1)(B) of Pub. L. 115–387, set out as a note under section 591 of this title.

DEFINITIONS

For definitions of terms used in this section, see section 901 of this title.

[1] *See References in Text note below.*

[2] *See Change of Name note below.*

§593. Hiring authority

In hiring personnel for the Office, the Secretary shall have the hiring and management authorities provided in section 1101 [1] of the Strom Thurmond National Defense Authorization Act for Fiscal

Year 1999 (5 U.S.C. 3104 note). The term of appointments for employees under subsection (c)(1) of such section may not exceed 5 years before granting any extension under subsection (c)(2) of such section.

(Pub. L. 107–296, title XIX, §1924, formerly title XVIII, §1803, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1934; renumbered title XIX, §1903, Pub. L. 110–53, title I, §104(a)(1), (2), Aug. 3, 2007, 121 Stat. 294; renumbered §1924, Pub. L. 115–387, §2(a)(5), Dec. 21, 2018, 132 Stat. 5163.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, referred to in text, is section 1101 of Pub. L. 105–261, which was formerly set out as a note under section 3104 of Title 5, Government Organization and Employees, prior to repeal by Pub. L. 114–328, div. A, title XI, §1121(b), Dec. 23, 2016, 130 Stat. 2452. See section 4092 of Title 10, Armed Forces.

[1] *See References in Text note below.*

§594. Testing authority

(a) In general

The Director shall coordinate with the responsible Federal agency or other entity to facilitate the use by the Office, by its contractors, or by other persons or entities, of existing Government laboratories, centers, ranges, or other testing facilities for the testing of materials, equipment, models, computer software, and other items as may be related to the missions identified in section 592 of this title. Any such use of Government facilities shall be carried out in accordance with all applicable laws, regulations, and contractual provisions, including those governing security, safety, and environmental protection, including, when applicable, the provisions of section 189 of this title. The Office may direct that private sector entities utilizing Government facilities in accordance with this section pay an appropriate fee to the agency that owns or operates those facilities to defray additional costs to the Government resulting from such use.

(b) Confidentiality of test results

The results of tests performed with services made available shall be confidential and shall not be disclosed outside the Federal Government without the consent of the persons for whom the tests are performed.

(c) Fees

Fees for services made available under this section shall not exceed the amount necessary to recoup the direct and indirect costs involved, such as direct costs of utilities, contractor support, and salaries of personnel that are incurred by the United States to provide for the testing.

(d) Use of fees

Fees received for services made available under this section may be credited to the appropriation from which funds were expended to provide such services.

(Pub. L. 107–296, title XIX, §1925, formerly title XVIII, §1804, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1934; renumbered title XIX, §1904, and amended Pub. L. 110–53, title I, §104(a)(1)–(3), Aug. 3, 2007, 121 Stat. 294; renumbered §1925 and amended Pub. L. 115–387, §2(a)(5), (7), Dec. 21, 2018, 132 Stat. 5163, 5164.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–387, §2(a)(7), made technical amendment to reference in original act which appears in text as reference to section 592 of this title.

2007—Subsec. (a). Pub. L. 110–53, §104(a)(3), made technical amendment to reference in original act which appears in text as reference to section 592 of this title.

§595. Repealed. Pub. L. 115–387, §2(a)(4), Dec. 21, 2018, 132 Stat. 5163

Section, Pub. L. 107–296, title XIX, §1905, formerly title XVIII, §1805, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1934; renumbered title XIX, §1905, Pub. L. 110–53, title I, §104(a)(1), (2), Aug. 3, 2007, 121 Stat. 294, related to relationship of Director's authority under this subchapter to other Department entities and Federal agencies.

§596. Contracting and grant making authorities

The Secretary, acting through the Assistant Secretary, in carrying out the responsibilities under section 592 of this title, shall—

(1) operate extramural and intramural programs and distribute funds through grants, cooperative agreements, and other transactions and contracts;

(2) ensure that activities under section 592 of this title include investigations of radiation detection equipment in configurations suitable for deployment at seaports, which may include underwater or water surface detection equipment and detection equipment that can be mounted on cranes and straddle cars used to move shipping containers; and

(3) have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues and carry out other responsibilities under this subchapter.

(Pub. L. 107–296, title XIX, §1926, formerly title XVIII, §1806, as added Pub. L. 109–347, title V, §501(a), Oct. 13, 2006, 120 Stat. 1935; renumbered title XIX, §1906, and amended Pub. L. 110–53, title I, §104(a)(1), (2), (4), Aug. 3, 2007, 121 Stat. 294; renumbered §1926 and amended Pub. L. 115–387, §2(a)(5), (8), Dec. 21, 2018, 132 Stat. 5163, 5164.)

EDITORIAL NOTES

AMENDMENTS

2018—Pub. L. 115–387, §2(a)(8)(A), in introductory provisions, substituted "Assistant Secretary" for "Director for Domestic Nuclear Detection" and "section 592" for "paragraphs (6) and (7) of section 592(a)".

Par. (2). Pub. L. 115–387, §2(a)(8)(B), substituted "section 592" for "paragraphs (6) and (7) of section 592(a)".

2007—Pub. L. 110–53, §104(a)(4), made technical amendment to reference in original act which appears in two places in text as reference to section 592(a) of this title.

§596a. Joint annual interagency review of global nuclear detection architecture

(a) Annual review

(1) In general

The Secretary, the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence shall jointly ensure interagency coordination on the development and implementation of the global nuclear detection architecture by ensuring that, not less frequently than once each year—

(A) each relevant agency, office, or entity—

(i) assesses its involvement, support, and participation in the development, revision, and implementation of the global nuclear detection architecture; and

(ii) examines and evaluates components of the global nuclear detection architecture (including associated strategies and acquisition plans) relating to the operations of that agency, office, or entity, to determine whether such components incorporate and address current threat assessments, scenarios, or intelligence analyses developed by the Director of National Intelligence or other agencies regarding threats relating to nuclear or radiological weapons of mass destruction;

(B) each agency, office, or entity deploying or operating any nuclear or radiological detection technology under the global nuclear detection architecture—

(i) evaluates the deployment and operation of nuclear or radiological detection technologies under the global nuclear detection architecture by that agency, office, or entity;

(ii) identifies performance deficiencies and operational or technical deficiencies in nuclear or radiological detection technologies deployed under the global nuclear detection architecture; and

(iii) assesses the capacity of that agency, office, or entity to implement the responsibilities of that agency, office, or entity under the global nuclear detection architecture; and

(C) the Assistant Secretary and each of the relevant departments that are partners in the National Technical Forensics Center—

(i) include, as part of the assessments, evaluations, and reviews required under this paragraph, each office's or department's activities and investments in support of nuclear forensics and attribution activities and specific goals and objectives accomplished during the previous year pursuant to the national strategic five-year plan for improving the nuclear forensic and attribution capabilities of the United States required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010;

(ii) attaches, as an appendix to the Joint Interagency Annual Review, the most current version of such strategy and plan; and

(iii) includes a description of new or amended bilateral and multilateral agreements and efforts in support of nuclear forensics and attribution activities accomplished during the previous year.

(2) Technology

Not less frequently than once each year, the Secretary shall examine and evaluate the development, assessment, and acquisition of radiation detection technologies deployed or implemented in support of the domestic portion of the global nuclear detection architecture.

(b) Annual report on joint interagency review

(1) In general

Not later than March 31 of each year, the Secretary, the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall jointly submit a report regarding the implementation of this section and the results of the reviews required under subsection (a) to—

(A) the President;

(B) the Committee on Appropriations, the Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Appropriations, the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Science and Technology of the House of Representatives.

(2) Form

The annual report submitted under paragraph (1) shall be submitted in unclassified form to the maximum extent practicable, but may include a classified annex.

(c) Definition

In this section, the term "global nuclear detection architecture" means the global nuclear detection architecture developed under section 592 of this title.

(Pub. L. 107–296, title XIX, §1927, formerly §1907, as added Pub. L. 110–53, title XI, §1103(a), Aug. 3, 2007, 121 Stat. 379; amended Pub. L. 111–140, §4(b), Feb. 16, 2010, 124 Stat. 35; renumbered §1927 and amended Pub. L. 115–387, §2(a)(5), (9), Dec. 21, 2018, 132 Stat. 5163, 5164.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1036 of the National Defense Authorization Act for Fiscal Year 2010, referred to in subsec. (a)(1)(C)(i), is section 1036 of Pub. L. 111–84, Oct. 28, 2009, 123 Stat. 2190, which is not classified to the Code. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2018—Subsec. (a)(1)(C). Pub. L. 115–387, §2(a)(9)(A), substituted "Assistant Secretary" for "Director of the Domestic Nuclear Detection Office" in introductory provisions.

Subsec. (c). Pub. L. 115–387, §2(a)(9)(B), made technical amendment to reference in original act which appears in text as reference to section 592 of this title.

2010—Subsec. (a)(1)(C). Pub. L. 111–140 added subpar. (C).

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Science and Technology of House of Representatives changed to Committee on Science, Space, and Technology of House of Representatives by House Resolution No. 5, One Hundred Twelfth Congress, Jan. 5, 2011.

§596b. Securing the Cities program

(a) Establishment

The Secretary, through the Assistant Secretary, shall establish a program, to be known as the "Securing the Cities" or "STC" program, to enhance the ability of the United States to detect and prevent terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials that pose a high risk to homeland security in high-risk urban areas.

(b) Elements

Through the STC program the Secretary shall—

(1) assist State, local, Tribal, and territorial governments in designing and implementing, or enhancing existing, architectures for coordinated and integrated detection and interdiction of nuclear or other radiological materials that are out of regulatory control;

(2) support the development of an operating capability to detect and report on nuclear and other radiological materials out of regulatory control;

(3) provide resources to enhance detection, analysis, communication, and coordination to better integrate State, local, Tribal, and territorial assets into Federal operations;

(4) facilitate alarm adjudication and provide subject matter expertise and technical assistance on concepts of operations, training, exercises, and alarm response protocols;

(5) communicate with, and promote sharing of information about the presence or detection of nuclear or other radiological materials among appropriate Federal, State, local, Tribal, and territorial government agencies, in a manner that ensures transparency with the jurisdictions designated under subsection (c);

(6) provide augmenting resources, as appropriate, to enable State, local, Tribal, and territorial governments to sustain and refresh their capabilities developed under the STC program;

(7) monitor expenditures under the STC program and track performance in meeting the goals of the STC program; and

(8) provide any other assistance the Secretary determines appropriate.

(c) Designation of jurisdictions

(1) In general

In carrying out the STC program under subsection (a), the Secretary shall designate jurisdictions from among high-risk urban areas under section 604 of this title.

(2) Congressional notification

The Secretary shall notify the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate not later than 3 days before the designation of a new jurisdiction under paragraph (1) or any change to a jurisdiction previously designated under that paragraph.

(d) Accountability

(1) Implementation plan

(A) In general

The Secretary shall develop, in consultation with relevant stakeholders, an implementation plan for carrying out the STC program that includes—

(i) a discussion of the goals of the STC program and a strategy to achieve those goals;

(ii) performance metrics and milestones for the STC program;

(iii) measures for achieving and sustaining capabilities under the STC program; and

(iv) costs associated with achieving the goals of the STC program.

(B) Submission to Congress

Not later than one year after December 21, 2018, the Secretary shall submit to the appropriate congressional committees and the Comptroller General of the United States the implementation plan required by subparagraph (A).

(2) Report required

Not later than one year after the submission of the implementation plan under paragraph (1)(B), the Secretary shall submit to the appropriate congressional committees and the Comptroller General a report that includes—

(A) an assessment of the effectiveness of the STC program, based on the performance metrics and milestones required by paragraph (1)(A)(ii); and

(B) proposals for any changes to the STC program, including an explanation of how those changes align with the strategy and goals of the STC program and, as appropriate, address any challenges faced by the STC program.

(3) Comptroller general review

Not later than 18 months after the submission of the report required by paragraph (2), the Comptroller General of the United States shall submit to the appropriate congressional committees a report evaluating the implementation plan required by paragraph (1) and the report required by paragraph (2), including an assessment of progress made with respect to the performance metrics and milestones required by paragraph (1)(A)(ii) and the sustainment of the capabilities of the STC program.

(4) Briefing and submission requirements

Before making any changes to the structure or requirements of the STC program, the Assistant Secretary shall—

(A) consult with the appropriate congressional committees; and

(B) provide to those committees—

(i) a briefing on the proposed changes, including a justification for the changes;

(ii) documentation relating to the changes, including plans, strategies, and resources to implement the changes; and

(iii) an assessment of the effect of the changes on the capabilities of the STC program, taking into consideration previous resource allocations and stakeholder input.

(Pub. L. 107–296, title XIX, §1928, as added Pub. L. 115–387, §2(a)(10), Dec. 21, 2018, 132 Stat. 5164.)

PART C—CHIEF MEDICAL OFFICER

§597. Chief Medical Officer

(a) In general

There is in the Office a Chief Medical Officer, who shall be appointed by the President. The Chief Medical Officer shall report to the Assistant Secretary.

(b) Qualifications

The individual appointed as Chief Medical Officer shall be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health.

(c) Responsibilities

The Chief Medical Officer shall have the responsibility within the Department for medical issues related to natural disasters, acts of terrorism, and other man-made disasters, including—

(1) serving as the principal advisor on medical and public health issues to the Secretary, the Administrator of the Federal Emergency Management Agency, the Assistant Secretary, and other Department officials;

(2) providing operational medical support to all components of the Department;

(3) as appropriate, providing medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on operational medical issues;

(4) coordinating with Federal, State, local, and Tribal governments, the medical community, and others within and outside the Department, including the Centers for Disease Control and Prevention and the Office of the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, with respect to medical and public health matters; and

(5) performing such other duties relating to such responsibilities as the Secretary may require.

(Pub. L. 107–296, title XIX, §1931, as added Pub. L. 115–387, §2(c)(2), Dec. 21, 2018, 132 Stat. 5166.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

SIMILAR PROVISIONS

Provisions similar to those in this section were contained in section 321e of this title prior to repeal by Pub. L. 115–387, §2(c)(1).

§597a. Medical countermeasures

(a) In general

Subject to the availability of appropriations, the Secretary shall, as appropriate, establish a medical countermeasures program within the components of the Department to—

(1) facilitate personnel readiness and protection for the employees and working animals of the Department in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic; and

(2) support the mission continuity of the Department.

(b) Oversight

The Secretary, acting through the Chief Medical Officer of the Department, shall—

(1) provide programmatic oversight of the medical countermeasures program established under subsection (a); and

(2) develop standards for—

(A) medical countermeasure storage, security, dispensing, and documentation;

(B) maintaining a stockpile of medical countermeasures, including antibiotics, antivirals, antidotes, therapeutics, and radiological countermeasures, as appropriate;

(C) ensuring adequate partnerships with manufacturers and executive agencies that enable advance prepositioning by vendors of inventories of appropriate medical countermeasures in strategic locations nationwide, based on risk and employee density, in accordance with applicable Federal statutes and regulations;

(D) providing oversight and guidance regarding the dispensing of stockpiled medical countermeasures;

(E) ensuring rapid deployment and dispensing of medical countermeasures in a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic;

(F) providing training to employees of the Department on medical countermeasures; and

(G) supporting dispensing exercises.

(c) Medical countermeasures working group

The Secretary, acting through the Chief Medical Officer of the Department, shall establish a medical countermeasures working group comprised of representatives from appropriate components and offices of the Department to ensure that medical countermeasures standards are maintained and guidance is consistent.

(d) Medical countermeasures management

Not later than 120 days after the date on which appropriations are made available to carry out subsection (a), the Chief Medical Officer shall develop and submit to the Secretary an integrated logistics support plan for medical countermeasures, including—

(1) a methodology for determining the ideal types and quantities of medical countermeasures to stockpile and how frequently such methodology shall be reevaluated;

(2) a replenishment plan; and

(3) inventory tracking, reporting, and reconciliation procedures for existing stockpiles and new medical countermeasure purchases.

(e) Transfer

Not later than 120 days after December 27, 2021, the Secretary shall transfer all medical countermeasures-related programmatic and personnel resources from the Under Secretary for Management to the Chief Medical Officer.

(f) Stockpile elements

In determining the types and quantities of medical countermeasures to stockpile under subsection (d), the Secretary, acting through the Chief Medical Officer of the Department—

(1) shall use a risk-based methodology for evaluating types and quantities of medical countermeasures required; and

(2) may use, if available—

(A) chemical, biological, radiological, and nuclear risk assessments of the Department; and

(B) guidance on medical countermeasures of the Office of the Assistant Secretary for Preparedness and Response and the Centers for Disease Control and Prevention.

(g) Briefing

Not later than 180 days after December 27, 2021, the Secretary shall provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on

Homeland Security of the House of Representatives regarding—

(1) the plan developed under subsection (d); and

(2) implementation of the requirements of this section.

(h) Definition

In this section, the term "medical countermeasures" means antibiotics, antivirals, antidotes, therapeutics, radiological countermeasures, and other countermeasures that may be deployed to protect the employees and working animals of the Department in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic.

(Pub. L. 107–296, title XIX, §1932, as added Pub. L. 117–81, div. F, title LXIV, §6408(a), Dec. 27, 2021, 135 Stat. 2404.)

SUBCHAPTER XV—HOMELAND SECURITY GRANTS

§601. Definitions

In this subchapter, the following definitions shall apply:

(1) Administrator

The term "Administrator" means the Administrator of the Federal Emergency Management Agency.

(2) Appropriate committees of Congress

The term "appropriate committees of Congress" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) those committees of the House of Representatives that the Speaker of the House of Representatives determines appropriate.

(3) Critical infrastructure sectors

The term "critical infrastructure sectors" means the following sectors, in both urban and rural areas:

(A) Agriculture and food.

(B) Banking and finance.

(C) Chemical industries.

(D) Commercial facilities.

(E) Commercial nuclear reactors, materials, and waste.

(F) Dams.

(G) The defense industrial base.

(H) Emergency services.

(I) Energy.

(J) Government facilities.

(K) Information technology.

(L) National monuments and icons.

(M) Postal and shipping.

(N) Public health and health care.

(O) Telecommunications.

(P) Transportation systems.

(Q) Water.

(4) Directly eligible tribe

The term "directly eligible tribe" means—

(A) any Indian tribe—

(i) that is located in the continental United States;

(ii) that operates a law enforcement or emergency response agency with the capacity to respond to calls for law enforcement or emergency services;

(iii)(I) that is located on or near an international border or a coastline bordering an ocean (including the Gulf of Mexico) or international waters;

(II) that is located within 10 miles of a system or asset included on the prioritized critical infrastructure list established under section 664(a)(2) of this title or has such a system or asset within its territory;

(III) that is located within or contiguous to 1 of the 50 most populous metropolitan statistical areas in the United States; or

(IV) the jurisdiction of which includes not less than 1,000 square miles of Indian country, as that term is defined in section 1151 of title 18; and

(iv) that certifies to the Secretary that a State has not provided funds under section 604 or 605 of this title to the Indian tribe or consortium of Indian tribes for the purpose for which direct funding is sought; and

(B) a consortium of Indian tribes, if each tribe satisfies the requirements of subparagraph (A).

(5) Eligible metropolitan area

The term "eligible metropolitan area" means any of the 100 most populous metropolitan statistical areas in the United States.

(6) High-risk urban area

The term "high-risk urban area" means a high-risk urban area designated under section 604(b)(3)(A) of this title.

(7) Indian tribe

The term "Indian tribe" has the meaning given that term in section 5304(e) of title 25.

(8) Metropolitan statistical area

The term "metropolitan statistical area" means a metropolitan statistical area, as defined by the Office of Management and Budget.

(9) National Special Security Event

The term "National Special Security Event" means a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.

(10) Population

The term "population" means population according to the most recent United States census population estimates available at the start of the relevant fiscal year.

(11) Population density

The term "population density" means population divided by land area in square miles.

(12) Qualified intelligence analyst

The term "qualified intelligence analyst" means an intelligence analyst (as that term is defined in section 124h(j) of this title), including law enforcement personnel—

(A) who has successfully completed training to ensure baseline proficiency in intelligence analysis and production, as determined by the Secretary, which may include training using a curriculum developed under section 124f of this title; or

(B) whose experience ensures baseline proficiency in intelligence analysis and production equivalent to the training required under subparagraph (A), as determined by the Secretary.

(13) Target capabilities

The term "target capabilities" means the target capabilities for Federal, State, local, and tribal government preparedness for which guidelines are required to be established under section 746(a)

of this title.

(14) Tribal government

The term "tribal government" means the government of an Indian tribe.

(Pub. L. 107–296, title XX, §2001, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 271; amended Pub. L. 115–278, §2(g)(7)(A), Nov. 16, 2018, 132 Stat. 4180.)

EDITORIAL NOTES

AMENDMENTS

2018—Par. (4)(A)(iii)(II). Pub. L. 115–278 substituted "section 664(a)(2) of this title" for "section 124l(a)(2) of this title".

PART A—GRANTS TO STATES AND HIGH-RISK URBAN AREAS

§603. Homeland security grant programs

(a) Grants authorized

The Secretary, through the Administrator, may award grants under sections 604, 605, and 609a of this title to State, local, and tribal governments.

(b) Programs not affected

This part shall not be construed to affect any of the following Federal programs:

(1) Firefighter and other assistance programs authorized under the Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2201 et seq.).

(2) Grants authorized under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(3) Emergency Management Performance Grants under the amendments made by title II of the Implementing Recommendations of the 9/11 Commission Act of 2007.

(4) Grants to protect critical infrastructure, including port security grants authorized under section 70107 of title 46 and the grants authorized under title [1] XIV and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 [6 U.S.C. 1131 et seq., 1151 et seq.] and the amendments made by such titles.

(5) The Metropolitan Medical Response System authorized under section 723 of this title.

(6) The Interoperable Emergency Communications Grant Program authorized under subchapter XIII.

(7) Grant programs other than those administered by the Department.

(c) Relationship to other laws

(1) In general

The grant programs authorized under sections 604 and 605 of this title shall supercede all grant programs authorized under section 1014 of the USA PATRIOT Act (42 U.S.C. 3714).[2]

(2) Allocation

The allocation of grants authorized under section 604 or 605 of this title shall be governed by the terms of this part and not by any other provision of law.

(Pub. L. 107–296, title XX, §2002, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 273; amended Pub. L. 116–108, §2(b), Jan. 24, 2020, 133 Stat. 3295.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Federal Fire Prevention and Control Act of 1974, referred to in subsec. (b)(1), is Pub. L. 93–498, Oct. 29, 1974, 88 Stat. 1535, which is classified principally to chapter 49 (§2201 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 2201 of Title 15 and Tables.

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (b)(2), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

The Implementing Recommendations of the 9/11 Commission Act of 2007, referred to in subsec. (b)(3), (4), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266. Title II of the Act amended section 762 of this title and section 5196c of Title 42, The Public Health and Welfare. Title XIV of the Act is classified generally to subchapter III (§1131 et seq.) of chapter 4 of this title. Title XV of the Act is classified principally to subchapter IV (§1151 et seq.) of chapter 4 of this title. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

Section 1014 of the USA PATRIOT Act, referred to in subsec. (c)(1), is section 1014 of Pub. L. 107–56, which is set out as a note under this section.

AMENDMENTS

2020—Subsec. (a). Pub. L. 116–108 substituted "sections 604, 605, and 609a" for "sections 604 and 605".

STATUTORY NOTES AND RELATED SUBSIDIARIES

GRANT PROGRAM FOR STATE AND LOCAL DOMESTIC PREPAREDNESS SUPPORT

Pub. L. 107–56, title X, §1014, Oct. 26, 2001, 115 Stat. 399, as amended by Pub. L. 107–273, div. C, title I, §11003, Nov. 2, 2002, 116 Stat. 1816, provided that:

"(a) IN GENERAL.—The Office for Domestic Preparedness of the Office of Justice Programs shall make a grant to each State, which shall be used by the State, in conjunction with units of local government, to enhance the capability of State and local jurisdictions to prepare for and respond to terrorist acts including events of terrorism involving weapons of mass destruction and biological, nuclear, radiological, incendiary, chemical, and explosive devices.

"(b) USE OF GRANT AMOUNTS.—Grants under this section may be used to purchase needed equipment and to provide training and technical assistance to State and local first responders. In addition, grants under this section may be used to construct, develop, expand, modify, operate, or improve facilities to provide training or assistance to State and local first responders.

"(c) AUTHORIZATION OF APPROPRIATIONS.—

"(1) IN GENERAL.—There is authorized to be appropriated to carry out this section such sums as necessary for each of fiscal years 2002 through 2007.

"(2) LIMITATIONS.—Of the amount made available to carry out this section in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

"(3) MINIMUM AMOUNT.—Each State shall be allocated in each fiscal year under this section not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this section, except that the United States Virgin Islands, America Samoa, Guam, and the Northern Mariana Islands each shall be allocated not less than 0.25 percent."

[For transfer of functions, personnel, assets, and liabilities of the Office for Domestic Preparedness of the Office of Justice Programs, including the functions of the Attorney General relating thereto, to the Secretary of Homeland Security, and for treatment of related references, see sections 203(5), 551(d), 552(d), and 557 of this title and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of this title.]

[1] So in original. Probably should be "titles".

[2] See References in Text note below.

§604. Urban Area Security Initiative

(a) Establishment

There is established an Urban Area Security Initiative to provide grants to assist high-risk urban areas in preventing, preparing for, protecting against, and responding to acts of terrorism.

(b) Assessment and designation of high-risk urban areas

(1) In general

The Administrator shall designate high-risk urban areas to receive grants under this section based on procedures under this subsection.

(2) Initial assessment

(A) In general

For each fiscal year, the Administrator shall conduct an initial assessment of the relative threat, vulnerability, and consequences from acts of terrorism faced by each eligible metropolitan area, including consideration of—

(i) the factors set forth in subparagraphs (A) through (H) and (K) of section 608(a)(1) of this title; and

(ii) information and materials submitted under subparagraph (B).

(B) Submission of information by eligible metropolitan areas

Prior to conducting each initial assessment under subparagraph (A), the Administrator shall provide each eligible metropolitan area with, and shall notify each eligible metropolitan area of, the opportunity to—

(i) submit information that the eligible metropolitan area believes to be relevant to the determination of the threat, vulnerability, and consequences it faces from acts of terrorism; and

(ii) review the risk assessment conducted by the Department of that eligible metropolitan area, including the bases for the assessment by the Department of the threat, vulnerability, and consequences from acts of terrorism faced by that eligible metropolitan area, and remedy erroneous or incomplete information.

(3) Designation of high-risk urban areas

(A) Designation

(i) In general

For each fiscal year, after conducting the initial assessment under paragraph (2), and based on that assessment, the Administrator shall designate high-risk urban areas that may submit applications for grants under this section.

(ii) Additional areas

Notwithstanding paragraph (2), the Administrator may—

(I) in any case where an eligible metropolitan area consists of more than 1 metropolitan division (as that term is defined by the Office of Management and Budget) designate more than 1 high-risk urban area within a single eligible metropolitan area; and

(II) designate an area that is not an eligible metropolitan area as a high-risk urban area based on the assessment by the Administrator of the relative threat, vulnerability, and consequences from acts of terrorism faced by the area.

(iii) Rule of construction

Nothing in this subsection may be construed to require the Administrator to—

(I) designate all eligible metropolitan areas that submit information to the Administrator under paragraph (2)(B)(i) as high-risk urban areas; or

(II) designate all areas within an eligible metropolitan area as part of the high-risk urban area.

(B) Jurisdictions included in high-risk urban areas

(i) In general

In designating high-risk urban areas under subparagraph (A), the Administrator shall determine which jurisdictions, at a minimum, shall be included in each high-risk urban area.

(ii) Additional jurisdictions

A high-risk urban area designated by the Administrator may, in consultation with the State or States in which such high-risk urban area is located, add additional jurisdictions to the high-risk urban area.

(c) Application

(1) In general

An area designated as a high-risk urban area under subsection (b) may apply for a grant under this section.

(2) Minimum contents of application

In an application for a grant under this section, a high-risk urban area shall submit—

(A) a plan describing the proposed division of responsibilities and distribution of funding among the local and tribal governments in the high-risk urban area;

(B) the name of an individual to serve as a high-risk urban area liaison with the Department and among the various jurisdictions in the high-risk urban area; and

(C) such information in support of the application as the Administrator may reasonably require.

(3) Annual applications

Applicants for grants under this section shall apply or reapply on an annual basis.

(4) State review and transmission

(A) In general

To ensure consistency with State homeland security plans, a high-risk urban area applying for a grant under this section shall submit its application to each State within which any part of that high-risk urban area is located for review before submission of such application to the Department.

(B) Deadline

Not later than 30 days after receiving an application from a high-risk urban area under subparagraph (A), a State shall transmit the application to the Department.

(C) Opportunity for State comment

If the Governor of a State determines that an application of a high-risk urban area is inconsistent with the State homeland security plan of that State, or otherwise does not support the application, the Governor shall—

(i) notify the Administrator, in writing, of that fact; and

(ii) provide an explanation of the reason for not supporting the application at the time of transmission of the application.

(5) Opportunity to amend

In considering applications for grants under this section, the Administrator shall provide applicants with a reasonable opportunity to correct defects in the application, if any, before making final awards.

(d) Distribution of awards

(1) In general

If the Administrator approves the application of a high-risk urban area for a grant under this section, the Administrator shall distribute the grant funds to the State or States in which that high-risk urban area is located.

(2) State distribution of funds

(A) In general

Not later than 45 days after the date that a State receives grant funds under paragraph (1), that State shall provide the high-risk urban area awarded that grant not less than 80 percent of the grant funds. Any funds retained by a State shall be expended on items, services, or activities that benefit the high-risk urban area.

(B) Funds retained

A State shall provide each relevant high-risk urban area with an accounting of the items, services, or activities on which any funds retained by the State under subparagraph (A) were expended.

(3) Interstate urban areas

If parts of a high-risk urban area awarded a grant under this section are located in 2 or more States, the Administrator shall distribute to each such State—

(A) a portion of the grant funds in accordance with the proposed distribution set forth in the application; or

(B) if no agreement on distribution has been reached, a portion of the grant funds determined by the Administrator to be appropriate.

(4) Certifications regarding distribution of grant funds to high-risk urban areas

A State that receives grant funds under paragraph (1) shall certify to the Administrator that the State has made available to the applicable high-risk urban area the required funds under paragraph (2).

(e) Authorization of appropriations

There are authorized to be appropriated for grants under this section—

(1) $850,000,000 for fiscal year 2008;
(2) $950,000,000 for fiscal year 2009;
(3) $1,050,000,000 for fiscal year 2010;
(4) $1,150,000,000 for fiscal year 2011;
(5) $1,300,000,000 for fiscal year 2012; and
(6) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.

(Pub. L. 107–296, title XX, §2003, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 274.)

§605. State Homeland Security Grant Program

(a) Establishment

There is established a State Homeland Security Grant Program to assist State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism.

(b) Application

(1) In general

Each State may apply for a grant under this section, and shall submit such information in support of the application as the Administrator may reasonably require.

(2) Minimum contents of application

The Administrator shall require that each State include in its application, at a minimum—

(A) the purpose for which the State seeks grant funds and the reasons why the State needs the grant to meet the target capabilities of that State;

(B) a description of how the State plans to allocate the grant funds to local governments and Indian tribes; and

(C) a budget showing how the State intends to expend the grant funds.

(3) Annual applications

Applicants for grants under this section shall apply or reapply on an annual basis.

(c) Distribution to local and tribal governments

(1) In general

Not later than 45 days after receiving grant funds, any State receiving a grant under this section shall make available to local and tribal governments, consistent with the applicable State homeland security plan—

(A) not less than 80 percent of the grant funds;

(B) with the consent of local and tribal governments, items, services, or activities having a value of not less than 80 percent of the amount of the grant; or

(C) with the consent of local and tribal governments, grant funds combined with other items, services, or activities having a total value of not less than 80 percent of the amount of the grant.

(2) Certifications regarding distribution of grant funds to local governments

A State shall certify to the Administrator that the State has made the distribution to local and tribal governments required under paragraph (1).

(3) Extension of period

The Governor of a State may request in writing that the Administrator extend the period under paragraph (1) for an additional period of time. The Administrator may approve such a request if the Administrator determines that the resulting delay in providing grant funding to the local and tribal governments is necessary to promote effective investments to prevent, prepare for, protect against, or respond to acts of terrorism.

(4) Exception

Paragraph (1) shall not apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, or the Virgin Islands.

(5) Direct funding

If a State fails to make the distribution to local or tribal governments required under paragraph (1) in a timely fashion, a local or tribal government entitled to receive such distribution may petition the Administrator to request that grant funds be provided directly to the local or tribal government.

(d) Multistate applications

(1) In general

Instead of, or in addition to, any application for a grant under subsection (b), 2 or more States may submit an application for a grant under this section in support of multistate efforts to prevent, prepare for, protect against, and respond to acts of terrorism.

(2) Administration of grant

If a group of States applies for a grant under this section, such States shall submit to the Administrator at the time of application a plan describing—

(A) the division of responsibilities for administering the grant; and

(B) the distribution of funding among the States that are parties to the application.

(e) Minimum allocation

(1) In general

In allocating funds under this section, the Administrator shall ensure that—

(A) except as provided in subparagraph (B), each State receives, from the funds appropriated for the State Homeland Security Grant Program established under this section, not less than an amount equal to—

(i) 0.375 percent of the total funds appropriated for grants under this section and section 604 of this title in fiscal year 2008;

(ii) 0.365 percent of the total funds appropriated for grants under this section and section 604 of this title in fiscal year 2009;

(iii) 0.36 percent of the total funds appropriated for grants under this section and section 604 of this title in fiscal year 2010;

(iv) 0.355 percent of the total funds appropriated for grants under this section and section 604 of this title in fiscal year 2011; and

(v) 0.35 percent of the total funds appropriated for grants under this section and section 604 of this title in fiscal year 2012 and in each fiscal year thereafter; and

(B) for each fiscal year, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands each receive, from the funds appropriated for the State Homeland Security Grant Program established under this section, not less than an amount equal to 0.08 percent of the total funds appropriated for grants under this section and section 604 of this title.

(2) Effect of multistate award on State minimum

Any portion of a multistate award provided to a State under subsection (d) shall be considered in calculating the minimum State allocation under this subsection.

(f) Authorization of appropriations

There are authorized to be appropriated for grants under this section—

(1) $950,000,000 for each of fiscal years 2008 through 2012; and

(2) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.

(Pub. L. 107–296, title XX, §2004, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 277.)

§606. Grants to directly eligible tribes

(a) In general

Notwithstanding section 605(b) of this title, the Administrator may award grants to directly eligible tribes under section 605 of this title.

(b) Tribal applications

A directly eligible tribe may apply for a grant under section 605 of this title by submitting an application to the Administrator that includes, as appropriate, the information required for an application by a State under section 605(b) of this title.

(c) Consistency with State plans

(1) In general

To ensure consistency with any applicable State homeland security plan, a directly eligible tribe applying for a grant under section 605 of this title shall provide a copy of its application to each State within which any part of the tribe is located for review before the tribe submits such application to the Department.

(2) Opportunity for comment

If the Governor of a State determines that the application of a directly eligible tribe is inconsistent with the State homeland security plan of that State, or otherwise does not support the application, not later than 30 days after the date of receipt of that application the Governor shall—

(A) notify the Administrator, in writing, of that fact; and

(B) provide an explanation of the reason for not supporting the application.

(d) Final authority

The Administrator shall have final authority to approve any application of a directly eligible tribe. The Administrator shall notify each State within the boundaries of which any part of a directly eligible tribe is located of the approval of an application by the tribe.

(e) Prioritization

The Administrator shall allocate funds to directly eligible tribes in accordance with the factors applicable to allocating funds among States under section 608 of this title.

(f) Distribution of awards to directly eligible tribes

If the Administrator awards funds to a directly eligible tribe under this section, the Administrator shall distribute the grant funds directly to the tribe and not through any State.

(g) Minimum allocation

(1) In general

In allocating funds under this section, the Administrator shall ensure that, for each fiscal year, directly eligible tribes collectively receive, from the funds appropriated for the State Homeland Security Grant Program established under section 605 of this title, not less than an amount equal to 0.1 percent of the total funds appropriated for grants under sections 604 and 605 of this title.

(2) Exception

This subsection shall not apply in any fiscal year in which the Administrator—

(A) receives fewer than 5 applications under this section; or

(B) does not approve at least 2 applications under this section.

(h) Tribal liaison

A directly eligible tribe applying for a grant under section 605 of this title shall designate an individual to serve as a tribal liaison with the Department and other Federal, State, local, and regional government officials concerning preventing, preparing for, protecting against, and responding to acts of terrorism.

(i) Eligibility for other funds

A directly eligible tribe that receives a grant under section 605 of this title may receive funds for other purposes under a grant from the State or States within the boundaries of which any part of such tribe is located and from any high-risk urban area of which it is a part, consistent with the homeland security plan of the State or high-risk urban area.

(j) State obligations

(1) In general

States shall be responsible for allocating grant funds received under section 605 of this title to tribal governments in order to help those tribal communities achieve target capabilities not achieved through grants to directly eligible tribes.

(2) Distribution of grant funds

With respect to a grant to a State under section 605 of this title, an Indian tribe shall be eligible for funding directly from that State, and shall not be required to seek funding from any local government.

(3) Imposition of requirements

A State may not impose unreasonable or unduly burdensome requirements on an Indian tribe as a condition of providing the Indian tribe with grant funds or resources under section 605 of this title.

(k) Rule of construction

Nothing in this section shall be construed to affect the authority of an Indian tribe that receives funds under this part.

(Pub. L. 107–296, title XX, §2005, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat.

279.)

§607. Terrorism prevention

(a) Law enforcement terrorism prevention program

(1) In general

The Administrator shall ensure that not less than 25 percent of the total combined funds appropriated for grants under sections 604 and 605 of this title is used for law enforcement terrorism prevention activities.

(2) Law enforcement terrorism prevention activities

Law enforcement terrorism prevention activities include—

(A) information sharing and analysis;

(B) target hardening;

(C) threat recognition;

(D) terrorist interdiction;

(E) training exercises to enhance preparedness for and response to mass casualty and active shooter incidents and security events at public locations, including airports and mass transit systems;

(F) overtime expenses consistent with a State homeland security plan, including for the provision of enhanced law enforcement operations in support of Federal agencies, including for increased border security and border crossing enforcement;

(G) establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under section 124h(i) of this title;

(H) paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts;

(I) any other activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the Law Enforcement Terrorism Prevention Program; and

(J) any other terrorism prevention activity authorized by the Administrator.

(3) Participation of underrepresented communities in fusion centers

The Administrator shall ensure that grant funds described in paragraph (1) are used to support the participation, as appropriate, of law enforcement and other emergency response providers from rural and other underrepresented communities at risk from acts of terrorism in fusion centers.

(b) Office for State and Local Law Enforcement

(1) Establishment

There is established in the Policy Directorate of the Department an Office for State and Local Law Enforcement, which shall be headed by an Assistant Secretary for State and Local Law Enforcement.

(2) Qualifications

The Assistant Secretary for State and Local Law Enforcement shall have an appropriate background with experience in law enforcement, intelligence, and other counterterrorism functions.

(3) Assignment of personnel

The Secretary shall assign to the Office for State and Local Law Enforcement permanent staff and, as appropriate and consistent with sections 316(c)(2), 381, and 468(d) of this title, other appropriate personnel detailed from other components of the Department to carry out the responsibilities under this subsection.

(4) Responsibilities

The Assistant Secretary for State and Local Law Enforcement shall—

(A) lead the coordination of Department-wide policies relating to the role of State and local law enforcement in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

(B) serve as a liaison between State, local, and tribal law enforcement agencies and the Department;

(C) coordinate with the Office of Intelligence and Analysis to ensure the intelligence and information sharing requirements of State, local, and tribal law enforcement agencies are being addressed;

(D) work with the Administrator to ensure that law enforcement and terrorism-focused grants to State, local, and tribal government agencies, including grants under sections 604 and 605 of this title, the Commercial Equipment Direct Assistance Program, and other grants administered by the Department to support fusion centers and law enforcement-oriented programs, are appropriately focused on terrorism prevention activities;

(E) coordinate with the Science and Technology Directorate, the Federal Emergency Management Agency, the Department of Justice, the National Institute of Justice, law enforcement organizations, and other appropriate entities to support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for training and personal protective equipment to be used in a tactical environment by law enforcement officers; and

(F) conduct, jointly with the Administrator, a study to determine the efficacy and feasibility of establishing specialized law enforcement deployment teams to assist State, local, and tribal governments in responding to natural disasters, acts of terrorism, or other man-made disasters and report on the results of that study to the appropriate committees of Congress.

(5) Rule of construction

Nothing in this subsection shall be construed to diminish, supercede, or replace the responsibilities, authorities, or role of the Administrator.

(Pub. L. 107–296, title XX, §2006, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 280; amended Pub. L. 114–190, title III, §3602, July 15, 2016, 130 Stat. 665.)

EDITORIAL NOTES

AMENDMENTS

2016—Subsec. (a)(2)(E) to (J). Pub. L. 114–190 added subpar. (E) and redesignated former subpars. (E) to (I) as (F) to (J), respectively.

§608. Prioritization

(a) In general

In allocating funds among States and high-risk urban areas applying for grants under section 604 or 605 of this title, the Administrator shall consider, for each State or high-risk urban area—

(1) its relative threat, vulnerability, and consequences from acts of terrorism, including consideration of—

(A) its population, including appropriate consideration of military, tourist, and commuter populations;

(B) its population density;

(C) its history of threats, including whether it has been the target of a prior act of terrorism;

(D) its degree of threat, vulnerability, and consequences related to critical infrastructure (for all critical infrastructure sectors) or key resources identified by the Administrator or the State homeland security plan, including threats, vulnerabilities, and consequences related to critical infrastructure or key resources in nearby jurisdictions;

(E) the most current threat assessments available to the Department;

(F) whether the State has, or the high-risk urban area is located at or near, an international border;

(G) whether it has a coastline bordering an ocean (including the Gulf of Mexico) or international waters;

(H) its likely need to respond to acts of terrorism occurring in nearby jurisdictions;

(I) the extent to which it has unmet target capabilities;

(J) in the case of a high-risk urban area, the extent to which that high-risk urban area includes—

(i) those incorporated municipalities, counties, parishes, and Indian tribes within the relevant eligible metropolitan area, the inclusion of which will enhance regional efforts to prevent, prepare for, protect against, and respond to acts of terrorism; and

(ii) other local and tribal governments in the surrounding area that are likely to be called upon to respond to acts of terrorism within the high-risk urban area; and

(K) such other factors as are specified in writing by the Administrator; and

(2) the anticipated effectiveness of the proposed use of the grant by the State or high-risk urban area in increasing the ability of that State or high-risk urban area to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

(b) Types of threat

In assessing threat under this section, the Administrator shall consider the following types of threat to critical infrastructure sectors and to populations in all areas of the United States, urban and rural:

(1) Biological.

(2) Chemical.

(3) Cyber.

(4) Explosives.

(5) Incendiary.

(6) Nuclear.

(7) Radiological.

(8) Suicide bombers.

(9) Such other types of threat determined relevant by the Administrator.

(Pub. L. 107–296, title XX, §2007, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 282.)

§609. Use of funds

(a) Permitted uses

The Administrator shall permit the recipient of a grant under section 604 or 605 of this title to use grant funds to achieve target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism, consistent with a State homeland security plan and relevant local, tribal, and regional homeland security plans, including by working in conjunction with a National Laboratory (as defined in section 15801(3) of title 42), through—

(1) developing and enhancing homeland security, emergency management, or other relevant plans, assessments, or mutual aid agreements;

(2) designing, conducting, and evaluating training and exercises, including training and exercises conducted under section 321a of this title and section 748 of this title;

(3) protecting a system or asset included on the prioritized critical infrastructure list established under section 664(a)(2) of this title;

(4) purchasing, upgrading, storing, or maintaining equipment, including computer hardware and

software;

(5) ensuring operability and achieving interoperability of emergency communications;

(6) responding to an increase in the threat level under the Homeland Security Advisory System, or to the needs resulting from a National Special Security Event;

(7) establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under section 124h(i) of this title;

(8) enhancing school preparedness;

(9) enhancing the security and preparedness of secure and nonsecure areas of eligible airports and surface transportation systems;

(10) supporting public safety answering points;

(11) paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts, regardless of whether such analysts are current or new full-time employees or contract employees;

(12) paying expenses directly related to administration of the grant, except that such expenses may not exceed 3 percent of the amount of the grant;

(13) any activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the State Homeland Security Grant Program, the Urban Area Security Initiative (including activities permitted under the full-time counterterrorism staffing pilot), or the Law Enforcement Terrorism Prevention Program;

(14) migrating any online service (as defined in section 3 of the DOTGOV Online Trust in Government Act of 2020) [1] to the .gov internet domain; and

(15) any other appropriate activity, as determined by the Administrator.

(b) Limitations on use of funds

(1) In general

Funds provided under section 604 or 605 of this title may not be used—

(A) to supplant State or local funds, except that nothing in this paragraph shall prohibit the use of grant funds provided to a State or high-risk urban area for otherwise permissible uses under subsection (a) on the basis that a State or high-risk urban area has previously used State or local funds to support the same or similar uses; or

(B) for any State or local government cost-sharing contribution.

(2) Personnel

(A) In general

Not more than 50 percent of the amount awarded to a grant recipient under section 604 or 605 of this title in any fiscal year may be used to pay for personnel, including overtime and backfill costs, in support of the permitted uses under subsection (a).

(B) Waiver

At the request of the recipient of a grant under section 604 or 605 of this title, the Administrator may grant a waiver of the limitation under subparagraph (A).

(3) Limitations on discretion

(A) In general

With respect to the use of amounts awarded to a grant recipient under section 604 or 605 of this title for personnel costs in accordance with paragraph (2) of this subsection, the Administrator may not—

(i) impose a limit on the amount of the award that may be used to pay for personnel, or personnel-related, costs that is higher or lower than the percent limit imposed in paragraph (2)(A); or

(ii) impose any additional limitation on the portion of the funds of a recipient that may be used for a specific type, purpose, or category of personnel, or personnel-related, costs.

(B) Analysts

If amounts awarded to a grant recipient under section 604 or 605 of this title are used for paying salary or benefits of a qualified intelligence analyst under subsection (a)(10),[1] the Administrator shall make such amounts available without time limitations placed on the period of time that the analyst can serve under the grant.

(4) Construction

(A) In general

A grant awarded under section 604 or 605 of this title may not be used to acquire land or to construct buildings or other physical facilities.

(B) Exceptions

(i) In general

Notwithstanding subparagraph (A), nothing in this paragraph shall prohibit the use of a grant awarded under section 604 or 605 of this title to achieve target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, including through the alteration or remodeling of existing buildings for the purpose of making such buildings secure against acts of terrorism.

(ii) Requirements for exception

No grant awarded under section 604 or 605 of this title may be used for a purpose described in clause (i) unless—

(I) specifically approved by the Administrator;

(II) any construction work occurs under terms and conditions consistent with the requirements under section 5196(j)(9) of title 42; and

(III) the amount allocated for purposes under clause (i) does not exceed the greater of $1,000,000 or 15 percent of the grant award.

(5) Recreation

Grants awarded under this part may not be used for recreational or social purposes.

(c) Multiple-purpose funds

Nothing in this part shall be construed to prohibit State, local, or tribal governments from using grant funds under sections 604, 605, and 609a of this title in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such governments in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

(d) Reimbursement of costs

(1) Paid-on-call or volunteer reimbursement

In addition to the activities described in subsection (a), a grant under section 604 or 605 of this title may be used to provide a reasonable stipend to paid-on-call or volunteer emergency response providers who are not otherwise compensated for travel to or participation in training or exercises related to the purposes of this part. Any such reimbursement shall not be considered compensation for purposes of rendering an emergency response provider an employee under the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.).

(2) Performance of Federal duty

An applicant for a grant under section 604 or 605 of this title may petition the Administrator to use the funds from its grants under those sections for the reimbursement of the cost of any activity relating to preventing, preparing for, protecting against, or responding to acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government under agreement with a Federal agency.

(e) Flexibility in unspent homeland security grant funds

Upon request by the recipient of a grant under section 604, 605, or 609a of this title, the

Administrator may authorize the grant recipient to transfer all or part of the grant funds from uses specified in the grant agreement to other uses authorized under this section, if the Administrator determines that such transfer is in the interests of homeland security.

(f) Equipment standards

(1) Application requirement

If an applicant for a grant under section 604 or 605 of this title proposes to upgrade or purchase, with assistance provided under that grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 747 of this title, the applicant shall include in its application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

(2) Review process

The Administrator shall implement a uniform process for reviewing applications that, in accordance with paragraph (1), contain explanations to use grants provided under section 604 or 605 of this title to purchase equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 747 of this title.

(3) Factors

In carrying out the review process under paragraph (2), the Administrator shall consider the following:

(A) Current or past use of proposed equipment or systems by Federal agencies or the Armed Forces.

(B) The absence of a national voluntary consensus standard for such equipment or systems.

(C) The existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard.

(D) The nature of the capability gap identified by the applicant and how such equipment or systems will address such gap.

(E) The degree to which such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed existing consensus standards.

(F) Any other factor determined appropriate by the Administrator.

(g) Review process

The Administrator shall implement a uniform process for reviewing applications to use grants provided under section 604 or 605 of this title to purchase equipment or systems not included on the Authorized Equipment List maintained by the Administrator.

(Pub. L. 107–296, title XX, §2008, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 283; amended Pub. L. 110–412, §2, Oct. 14, 2008, 122 Stat. 4336; Pub. L. 114–113, div. M, title VII, §711, Dec. 18, 2015, 129 Stat. 2934; Pub. L. 114–190, title III, §3603, July 15, 2016, 130 Stat. 665; Pub. L. 115–278, §2(g)(7)(B), Nov. 16, 2018, 132 Stat. 4180; Pub. L. 116–260, div. U, title IX, §904(c), Dec. 27, 2020, 134 Stat. 2302; Pub. L. 117–263, div. G, title LXXI, §7101(c), Dec. 23, 2022, 136 Stat. 3619; Pub. L. 118–165, §2(a), Dec. 23, 2024, 138 Stat. 2581.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 3 of the DOTGOV Online Trust in Government Act of 2020, referred to in subsec. (a)(14), probably means section 903 of title IX of div. U of Pub. L. 116–260, which defines "online service" and is set out as a note under section 665 of this title.

Subsection (a)(10), referred to in subsec. (b)(3)(B), was redesignated subsec. (a)(11) by Pub. L. 114–190, title III, §3603(1), July 15, 2016, 130 Stat. 665.

The Fair Labor Standards Act of 1938, referred to in subsec. (d)(1), is act June 25, 1938, ch. 676, 52 Stat. 1060, which is classified generally to chapter 8 (§201 et seq.) of Title 29, Labor. For complete classification of this Act to the Code, see section 201 of Title 29 and Tables.

AMENDMENTS

2024—Subsec. (f). Pub. L. 118–165, §2(a)(1), designated existing provisions as par. (1), inserted heading, and added pars. (2) and (3).

Subsec. (g). Pub. L. 118–165, §2(a)(2), added subsec. (g).

2022—Subsec. (c). Pub. L. 117–263, §7101(c)(1), substituted "sections 604, 605, and 609a of this title" for "sections 604 and 605 of this title".

Subsec. (e). Pub. L. 117–263, §7101(c)(2), substituted "section 604, 605, or 609a of this title" for "section 604 or 605 of this title".

2020—Subsec. (a)(14), (15). Pub. L. 116–260 added par. (14) and redesignated former par. (14) as (15).

2018—Subsec. (a)(3). Pub. L. 115–278 substituted "section 664(a)(2) of this title" for "section 124l(a)(2) of this title".

2016—Subsec. (a)(9) to (14). Pub. L. 114–190 added par. (9) and redesignated former pars. (9) to (13) as (10) to (14), respectively.

2015—Subsec. (a). Pub. L. 114–113 inserted "including by working in conjunction with a National Laboratory (as defined in section 15801(3) of title 42)," after "plans," in introductory provisions.

2008—Subsec. (a). Pub. L. 110–412, §2(1)(A), substituted "The Administrator shall permit the recipient of a grant under section 604 or 605 of this title to use grant funds" for "Grants awarded under section 604 or 605 of this title may be used" in introductory provisions.

Subsec. (a)(10). Pub. L. 110–412, §2(1)(B), inserted ", regardless of whether such analysts are current or new full-time employees or contract employees" after "analysts".

Subsec. (b)(3) to (5). Pub. L. 110–412, §2(2), added par. (3) and redesignated former pars. (3) and (4) as (4) and (5), respectively.

[1] *See References in Text note below.*

§609a. Nonprofit Security Grant Program

(a) Establishment

There is established in the Department a program to be known as the "Nonprofit Security Grant Program" (in this section referred to as the "Program"). Under the Program, the Secretary, acting through the Administrator, shall make grants to eligible nonprofit organizations described in subsection (b), through the State in which such organizations are located, for target hardening and other security enhancements to protect against terrorist attacks or other threats.

(b) Eligible recipients

Eligible nonprofit organizations described in this subsection are organizations that are—

(1) described in section 501(c)(3) of title 26 and exempt from tax under section 501(a) of such title; and

(2) determined by the Secretary to be at risk of terrorist attacks or other threats.

(c) Permitted uses

(1) In general

The recipient of a grant under this section may use such grant for any of the following uses:

(A) Target hardening activities, including physical security enhancement equipment, inspection and screening systems, and alteration or remodeling of existing buildings or physical facilities.

(B) Fees for security training relating to physical security and cybersecurity, target hardening, terrorism awareness, and employee awareness.

(C) Facility security personnel costs.

(D) Expenses directly related to the administration of the grant, except that those expenses may not exceed 5 percent of the amount of the grant.

(E) Any other appropriate activity, including cybersecurity resilience activities, as determined by the Administrator.

(2) Retention

Each State through which a recipient receives a grant under this section may retain not more than 5 percent of each grant for expenses directly related to the administration of the grant.

(3) Outreach and technical assistance

(A) In general

If the Administrator establishes target allocations in determining award amounts under the Program, a State may request a project to use a portion of the target allocation for outreach and technical assistance if the State does not receive enough eligible applications from nonprofit organizations located outside high-risk urban areas.

(B) Priority

Any outreach or technical assistance described in subparagraph (A) should prioritize underserved communities and nonprofit organizations that are traditionally underrepresented in the Program.

(C) Parameters

In determining grant guidelines under subsection (g), the Administrator may determine the parameters for outreach and technical assistance.

(d) Period of performance

The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

(e) Report

The Administrator shall annually for each of fiscal years 2022 through 2028 submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing information on the following:

(1) The expenditure by each grant recipient of grant funds made under this section.

(2) The number of applications submitted by eligible nonprofit organizations to each State.

(3) The number of applications submitted by each State to the Administrator.

(4) The operations of the program office of the Program, including staffing resources and efforts with respect to subparagraphs (A) through (D) of subsection (c)(1).

(f) Administration

Not later than 120 days after December 23, 2022, the Administrator shall ensure that within the Federal Emergency Management Agency a program office for the Program (in this subsection referred to as the "program office") shall—

(1) be headed by a senior official of the Agency; and

(2) administer the Program (including, where appropriate, in coordination with States), including relating to—

(A) outreach, engagement, education, and technical assistance and support to eligible nonprofit organizations described in subsection (b), with particular attention to those organizations in underserved communities, before, during, and after the awarding of grants, including web-based training videos for eligible nonprofit organizations that provide guidance on preparing an application and the environmental planning and historic preservation process;

(B) the establishment of mechanisms to ensure program office processes are conducted in accordance with constitutional, statutory, and regulatory requirements that protect civil rights and civil liberties and advance equal access for members of underserved communities;

(C) the establishment of mechanisms for the Administrator to provide feedback to eligible nonprofit organizations that do not receive grants;

(D) the establishment of mechanisms to identify and collect data to measure the effectiveness of grants under the Program;

(E) the establishment and enforcement of standardized baseline operational requirements for States, including requirements for States to eliminate or prevent any administrative or

operational obstacles that may impact eligible nonprofit organizations described in subsection (b) from receiving grants under the Program;

(F) carrying out efforts to prevent waste, fraud, and abuse, including through audits of grantees; and

(G) promoting diversity in the types and locations of eligible nonprofit organizations that are applying for grants under the Program.

(g) Grant guidelines

For each fiscal year, before awarding grants under this section, the Administrator—

(1) shall publish guidelines, including a notice of funding opportunity or similar announcement, as the Administrator determines appropriate; and

(2) may prohibit States from closing application processes before the publication of those guidelines.

(h) Paperwork Reduction Act

Chapter 35 of title 44 (commonly known as the "Paperwork Reduction Act") shall not apply to any changes to the application materials, Program forms, or other core Program documentation intended to enhance participation by eligible nonprofit organizations in the Program.

(i) Authorization of appropriations

(1) In general

There is authorized to be appropriated $360,000,000 for each of fiscal years 2023 through 2028 for grants under this section, of which—

(A) $180,000,000 each such fiscal year shall be for recipients in high-risk urban areas that receive funding under section 2003; and

(B) $180,000,000 each such fiscal year shall be for recipients in jurisdictions that do not so receive such funding.

(2) Operations and support

There is authorized to be appropriated $18,000,000 for each of fiscal years 2023 through 2028 for Operations and Support at the Federal Emergency Management Agency for costs incurred for the management and administration (including evaluation) of this section.

(Pub. L. 107–296, title XX, §2009, as added Pub. L. 116–108, §2(a), Jan. 24, 2020, 133 Stat. 3294; amended Pub. L. 117–263, div. G, title LXXI, §7101(a), Dec. 23, 2022, 136 Stat. 3616.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7101(a)(1), inserted "or other threats" before period at end.

Subsec. (b). Pub. L. 117–263, §7101(a)(2)(A), struck out "(a)" after "this subsection" in introductory provisions.

Subsec. (b)(2). Pub. L. 117–263, §7101(a)(2)(B), amended par. (2) generally. Prior to amendment, par. (2) read as follows: "determined to be at risk of a terrorist attack by the Administrator."

Subsec. (c). Pub. L. 117–263, §7101(a)(3)(A), (B), (D), (E), designated existing provisions as par. (1) and inserted heading, redesignated former pars. (1) to (3) as subpars. (A), (B), and (E), respectively, of par. (1) and realigned margins, added subpars. (C) and (D) of par. (1), and added pars. (2) and (3).

Subsec. (c)(1)(A). Pub. L. 117–263, §7101(a)(3)(C), substituted "equipment, inspection and screening systems, and alteration or remodeling of existing buildings or physical facilities" for "equipment and inspection and screening systems".

Subsec. (e). Pub. L. 117–263, §7101(a)(4)(B), (C), substituted "on the following:" and "(1) The expenditure" for "on the expenditure" and added pars. (2) to (4).

Pub. L. 117–263, §7101(a)(4)(A), substituted "2022 through 2028" for "2020 through 2024".

Subsecs. (f) to (i). Pub. L. 117–263, §7101(a)(5), added subsecs. (f) to (i) and struck out former subsec. (f) which related to authorization of appropriations for fiscal years 2020 through 2024.

PART B—GRANTS ADMINISTRATION

§611. Administration and coordination

(a) Regional coordination

The Administrator shall ensure that—

(1) all recipients of grants administered by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters (excluding assistance provided under section 203, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 5191 et seq.)) coordinate, as appropriate, their prevention, preparedness, and protection efforts with neighboring State, local, and tribal governments; and

(2) all high-risk urban areas and other recipients of grants administered by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters (excluding assistance provided under section 203, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 5191 et seq.)) that include or substantially affect parts or all of more than 1 State coordinate, as appropriate, across State boundaries, including, where appropriate, through the use of regional working groups and requirements for regional plans.

(b) Planning committees

(1) In general

Any State or high-risk urban area receiving a grant under section 604 or 605 of this title shall establish a State planning committee or urban area working group to assist in preparation and revision of the State, regional, or local homeland security plan or the threat and hazard identification and risk assessment, as the case may be, and to assist in determining effective funding priorities for grants under such sections.

(2) Composition

(A) In general

The State planning committees and urban area working groups referred to in paragraph (1) shall include at least one representative from each of the following significant stakeholders:

(i) Local or tribal government officials.

(ii) Emergency response providers, which shall include representatives of the fire service, law enforcement, emergency medical services, and emergency managers.

(iii) Public health officials and other appropriate medical practitioners.

(iv) Individuals representing educational institutions, including elementary schools, community colleges, and other institutions of higher education.

(v) State and regional interoperable communications coordinators, as appropriate.

(vi) State and major urban area fusion centers, as appropriate.

(B) Geographic representation

The members of the State planning committee or urban area working group, as the case may be, shall be a representative group of individuals from the counties, cities, towns, and Indian tribes within the State or high-risk urban area, including, as appropriate, representatives of rural, high-population, and high-threat jurisdictions.

(3) Existing planning committees

Nothing in this subsection may be construed to require that any State or high-risk urban area create a State planning committee or urban area working group, as the case may be, if that State or high-risk urban area has established and uses a multijurisdictional planning committee or commission that meets the requirements of this subsection.

(c) Sense of Congress

It is the sense of Congress that, in order to ensure that the Nation is most effectively able to prevent, prepare for, protect against, and respond to all hazards, including natural disasters, acts of terrorism, and other man-made disasters—

(1) the Department should administer a coherent and coordinated system of both terrorism-focused and all-hazards grants;

(2) there should be a continuing and appropriate balance between funding for terrorism-focused and all-hazards preparedness, as reflected in the authorizations of appropriations for grants under the amendments made by titles I and II, as applicable, of the Implementing Recommendations of the 9/11 Commission Act of 2007; and

(3) with respect to terrorism-focused grants, it is necessary to ensure both that the target capabilities of the highest risk areas are achieved quickly and that basic levels of preparedness, as measured by the attainment of target capabilities, are achieved nationwide.

(Pub. L. 107–296, title XX, §2021, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 285; amended Pub. L. 114–328, div. A, title XIX, §1911, Dec. 23, 2016, 130 Stat. 2682; Pub. L. 115–278, §2(g)(7)(C), Nov. 16, 2018, 132 Stat. 4180.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143. Section 203 of the Act is classified to section 5133 of Title 42, The Public Health and Welfare. Titles IV and V of the Act are classified generally to subchapters IV (§5170 et seq.) and IV–A (§5191 et seq.), respectively, of chapter 68 of Title 42. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

The Implementing Recommendations of the 9/11 Commission Act of 2007, referred to in subsec. (c)(2), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266. Title I of the Act enacted this subchapter and amended sections 318, 321a, 594, 596, and 752 of this title. Title II of the Act amended section 762 of this title and section 5196c of Title 42, The Public Health and Welfare. For complete classification of titles I and II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c), (d). Pub. L. 115–278 redesignated subsec. (d) as (c) and struck out former subsec. (c). Prior to amendment, subsec. (c) related to interagency coordination.

2016—Subsec. (b). Pub. L. 114–328 amended subsec. (b) generally. Prior to amendment, subsec. (b) related to planning committees to assist in preparation and revision of State, regional, or local homeland security plans, and to assist in determining effective funding priorities for grants under sections 604 and 605 of this title.

§612. Accountability

(a) Audits of grant programs

(1) Compliance requirements

(A) Audit requirement

Each recipient of a grant administered by the Department that expends not less than $500,000 in Federal funds during its fiscal year shall submit to the Administrator a copy of the organization-wide financial and compliance audit report required under chapter 75 of title 31.

(B) Access to information

The Department and each recipient of a grant administered by the Department shall provide the Comptroller General and any officer or employee of the Government Accountability Office with full access to information regarding the activities carried out related to any grant administered by the Department.

(C) Improper payments

Consistent with subchapter IV of chapter 33 of title 31, for each of the grant programs under sections 604 and 605 of this title and section 762 of this title, the Administrator shall specify policies and procedures for—

(i) identifying activities funded under any such grant program that are susceptible to significant improper payments; and

(ii) reporting any improper payments to the Department.

(2) Agency program review

(A) In general

Not less than once every 2 years, the Administrator shall conduct, for each State and high-risk urban area receiving a grant administered by the Department, a programmatic and financial review of all grants awarded by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters, excluding assistance provided under section 203, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 5191 et seq.).

(B) Contents

Each review under subparagraph (A) shall, at a minimum, examine—

(i) whether the funds awarded were used in accordance with the law, program guidance, and State homeland security plans or other applicable plans; and

(ii) the extent to which funds awarded enhanced the ability of a grantee to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other man-made disasters.

(C) Authorization of appropriations

In addition to any other amounts authorized to be appropriated to the Administrator, there are authorized to be appropriated to the Administrator for reviews under this paragraph—

(i) $8,000,000 for each of fiscal years 2008, 2009, and 2010; and

(ii) such sums as are necessary for fiscal year 2011, and each fiscal year thereafter.

(3) Performance assessment

In order to ensure that States and high-risk urban areas are using grants administered by the Department appropriately to meet target capabilities and preparedness priorities, the Administrator shall—

(A) ensure that any such State or high-risk urban area conducts or participates in exercises under section 748(b) of this title;

(B) use performance metrics in accordance with the comprehensive assessment system under section 749 of this title and ensure that any such State or high-risk urban area regularly tests its progress against such metrics through the exercises required under subparagraph (A);

(C) use the remedial action management program under section 750 of this title; and

(D) ensure that each State receiving a grant administered by the Department submits a report to the Administrator on its level of preparedness, as required by section 752(c) of this title.

(4) Consideration of assessments

In conducting program reviews and performance audits under paragraph (2), the Administrator and the Inspector General of the Department shall take into account the performance assessment elements required under paragraph (3).

(5) Recovery audits

The Administrator shall conduct a recovery audit under section 3352(i) of title 31 for any grant administered by the Department with a total value of not less than $1,000,000, if the Administrator finds that—

(A) a financial audit has identified improper payments that can be recouped; and

(B) it is cost effective to conduct a recovery audit to recapture the targeted funds.

(6) Remedies for noncompliance

(A) In general

If, as a result of a review or audit under this subsection or otherwise, the Administrator finds that a recipient of a grant under this subchapter has failed to substantially comply with any provision of law or with any regulations or guidelines of the Department regarding eligible expenditures, the Administrator shall—

(i) reduce the amount of payment of grant funds to the recipient by an amount equal to the amount of grants funds that were not properly expended by the recipient;

(ii) limit the use of grant funds to programs, projects, or activities not affected by the failure to comply;

(iii) refer the matter to the Inspector General of the Department for further investigation;

(iv) terminate any payment of grant funds to be made to the recipient; or

(v) take such other action as the Administrator determines appropriate.

(B) Duration of penalty

The Administrator shall apply an appropriate penalty under subparagraph (A) until such time as the Administrator determines that the grant recipient is in full compliance with the law and with applicable guidelines or regulations of the Department.

(b) Reports by grant recipients

(1) Quarterly reports on homeland security spending

(A) In general

As a condition of receiving a grant under section 604 or 605 of this title, a State, high-risk urban area, or directly eligible tribe shall, not later than 30 days after the end of each Federal fiscal quarter, submit to the Administrator a report on activities performed using grant funds during that fiscal quarter.

(B) Contents

Each report submitted under subparagraph (A) shall at a minimum include, for the applicable State, high-risk urban area, or directly eligible tribe, and each subgrantee thereof—

(i) the amount obligated to that recipient under section 604 or 605 of this title in that quarter;

(ii) the amount of funds received and expended under section 604 or 605 of this title by that recipient in that quarter; and

(iii) a summary description of expenditures made by that recipient using such funds, and the purposes for which such expenditures were made.

(C) End-of-year report

The report submitted under subparagraph (A) by a State, high-risk urban area, or directly eligible tribe relating to the last quarter of any fiscal year shall include—

(i) the amount and date of receipt of all funds received under the grant during that fiscal year;

(ii) the identity of, and amount provided to, any subgrantee for that grant during that fiscal year;

(iii) the amount and the dates of disbursements of all such funds expended in compliance with section 611(a)(1) of this title or under mutual aid agreements or other sharing arrangements that apply within the State, high-risk urban area, or directly eligible tribe, as applicable, during that fiscal year; and

(iv) how the funds were used by each recipient or subgrantee during that fiscal year.

(2) Annual report

Any State applying for a grant under section 605 of this title shall submit to the Administrator annually a State preparedness report, as required by section 752(c) of this title.

(c) Reports by the Administrator

(1) Federal Preparedness Report

The Administrator shall submit to the appropriate committees of Congress annually the Federal Preparedness Report required under section 752(a) of this title.

(2) Risk assessment

(A) In general

For each fiscal year, the Administrator shall provide to the appropriate committees of Congress a detailed and comprehensive explanation of the methodologies used to calculate risk and compute the allocation of funds for grants administered by the Department, including—

(i) all variables included in the risk assessment and the weights assigned to each such variable;

(ii) an explanation of how each such variable, as weighted, correlates to risk, and the basis for concluding there is such a correlation; and

(iii) any change in the methodologies from the previous fiscal year, including changes in variables considered, weighting of those variables, and computational methods.

(B) Classified annex

The information required under subparagraph (A) shall be provided in unclassified form to the greatest extent possible, and may include a classified annex if necessary.

(C) Deadline

For each fiscal year, the information required under subparagraph (A) shall be provided on the earlier of—

(i) October 31; or

(ii) 30 days before the issuance of any program guidance for grants administered by the Department.

(3) Tribal funding report

At the end of each fiscal year, the Administrator shall submit to the appropriate committees of Congress a report setting forth the amount of funding provided during that fiscal year to Indian tribes under any grant program administered by the Department, whether provided directly or through a subgrant from a State or high-risk urban area.

(Pub. L. 107–296, title XX, §2022, as added Pub. L. 110–53, title I, §101, Aug. 3, 2007, 121 Stat. 287; amended Pub. L. 111–204, §2(h)(6)(B)(iii), July 22, 2010, 124 Stat. 2231; Pub. L. 113–284, §2(c)(1), (2), Dec. 18, 2014, 128 Stat. 3089; Pub. L. 116–117, §3(b)(2), Mar. 2, 2020, 134 Stat. 133.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a)(2)(A), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143. Section 203 of the Act is classified to section 5133 of Title 42, The Public Health and Welfare. Titles IV and V of the Act are classified generally to subchapters IV (§5170 et seq.) and IV–A (§5191 et seq.), respectively, of chapter 68 of Title 42. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

AMENDMENTS

2020—Subsec. (a)(1)(C). Pub. L. 116–117, §3(b)(2)(A), substituted "Consistent with subchapter IV of chapter 33 of title 31" for "Consistent with the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note)" in introductory provisions.

Subsec. (a)(5). Pub. L. 116–117, §3(b)(2)(B), substituted "section 3352(i) of title 31" for "section 2(h) of the Improper Payments Elimination and Recovery Act of 2010 (31 U.S.C. 3321 note)" in introductory provisions.

2014—Subsec. (a)(3) to (7). Pub. L. 113–284 redesignated pars. (4) to (7) as (3) to (6), respectively, substituted, in par. (4), "paragraph (2)" for "paragraphs (2) and (3)" and "paragraph (3)" for "paragraph (4)",

and struck out former par. (3) which related to Office of Inspector General performance audits.

2010—Subsec. (a)(6). Pub. L. 111–204 substituted "under section 2(h) of the Improper Payments Elimination and Recovery Act of 2010 (31 U.S.C. 3321 note)" for "(as that term is defined by the Director of the Office of Management and Budget under section 3561 of title 31)".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2014 AMENDMENT

Pub. L. 113–284, §2(c)(3), Dec. 18, 2014, 128 Stat. 3090, provided that: "The amendments made by this subsection [amending this section] shall take effect on January 1, 2015."

§613. Identification of reporting redundancies and development of performance metrics

(a) Definition

In this section, the term "covered grants" means grants awarded under section 604 of this title, grants awarded under section 605 of this title, and any other grants specified by the Administrator.

(b) Initial report

Not later than 90 days after October 12, 2010, the Administrator shall submit to the appropriate committees of Congress a report that includes—

(1) an assessment of redundant reporting requirements imposed by the Administrator on State, local, and tribal governments in connection with the awarding of grants, including—

(A) a list of each discrete item of data requested by the Administrator from grant recipients as part of the process of administering covered grants;

(B) identification of the items of data from the list described in subparagraph (A) that are required to be submitted by grant recipients on multiple occasions or to multiple systems; and

(C) identification of the items of data from the list described in subparagraph (A) that are not necessary to be collected in order for the Administrator to effectively and efficiently administer the programs under which covered grants are awarded;

(2) a plan, including a specific timetable, for eliminating any redundant and unnecessary reporting requirements identified under paragraph (1); and

(3) a plan, including a specific timetable, for promptly developing a set of quantifiable performance measures and metrics to assess the effectiveness of the programs under which covered grants are awarded.

(c) Biennial reports

Not later than 1 year after the date on which the initial report is required to be submitted under subsection (b), and once every 2 years thereafter, the Administrator shall submit to the appropriate committees of Congress a grants management report that includes—

(1) the status of efforts to eliminate redundant and unnecessary reporting requirements imposed on grant recipients, including—

(A) progress made in implementing the plan required under subsection (b)(2);

(B) a reassessment of the reporting requirements to identify and eliminate redundant and unnecessary requirements;

(2) the status of efforts to develop quantifiable performance measures and metrics to assess the effectiveness of the programs under which the covered grants are awarded, including—

(A) progress made in implementing the plan required under subsection (b)(3);

(B) progress made in developing and implementing additional performance metrics and measures for grants, including as part of the comprehensive assessment system required under section 749 of this title; and

(3) a performance assessment of each program under which the covered grants are awarded, including—

(A) a description of the objectives and goals of the program;

(B) an assessment of the extent to which the objectives and goals described in subparagraph (A) have been met, based on the quantifiable performance measures and metrics required under this section, section 612(a)(4) [1] of this title, and section 749 of this title;

(C) recommendations for any program modifications to improve the effectiveness of the program, to address changed or emerging conditions; and

(D) an assessment of the experience of recipients of covered grants, including the availability of clear and accurate information, the timeliness of reviews and awards, and the provision of technical assistance, and recommendations for improving that experience.

(d) Grants program measurement study

(1) In general

Not later than 30 days after October 12, 2010, the Administrator shall enter into a contract with the National Academy of Public Administration under which the National Academy of Public Administration shall assist the Administrator in studying, developing, and implementing—

(A) quantifiable performance measures and metrics to assess the effectiveness of grants administered by the Department, as required under this section and section 749 of this title; and

(B) the plan required under subsection (b)(3).

(2) Report

Not later than 1 year after the date on which the contract described in paragraph (1) is awarded, the Administrator shall submit to the appropriate committees of Congress a report that describes the findings and recommendations of the study conducted under paragraph (1).

(3) Authorization of appropriations

There are authorized to be appropriated to the Administrator such sums as may be necessary to carry out this subsection.

(Pub. L. 107–296, title XX, §2023, as added Pub. L. 111–271, §2(a), Oct. 12, 2010, 124 Stat. 2852.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 612(a)(4) of this title, referred to in subsec. (c)(3)(B), was redesignated section 612(a)(3) of this title by Pub. L. 113–284, §2(c)(2)(A), Dec. 18, 2014, 128 Stat. 3089.

[1] *See References in Text note below.*

SUBCHAPTER XVI—CHEMICAL FACILITY ANTI-TERRORISM STANDARDS

§§621 to 629. Omitted

EDITORIAL NOTES

CODIFICATION

The authority provided under sections 621 to 629, comprising subchapter XVI of this chapter, terminated on July 27, 2023, pursuant to section 5 of Pub. L. 113–254, set out as a note below.

Section 621, Pub. L. 107–296, title XXI, §2101, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2898, provided definitions for this subchapter.

Section 622, Pub. L. 107–296, title XXI, §2102, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2900; amended Pub. L. 115–278, §2(g)(8)(A), Nov. 16, 2018, 132 Stat. 4180, established a Chemical Facility Anti-Terrorism Standards Program within the Cybersecurity and Infrastructure Security Agency.

Section 623, Pub. L. 107–296, title XXI, §2103, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2911, related to protection and sharing of information.

Section 624, Pub. L. 107–296, title XXI, §2104, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2912; amended Pub. L. 115–278, §2(g)(8)(B), Nov. 16, 2018, 132 Stat. 4180; Pub. L. 117–263, div. G, title LXXI, §7143(c)(4), Dec. 23, 2022, 136 Stat. 3663, related to civil enforcement.

Section 625, Pub. L. 107–296, title XXI, §2105, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2914, related to whistleblower protections.

Section 626, Pub. L. 107–296, title XXI, §2106, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2915, related to relationship of provisions of this subchapter to other laws.

Section 627, Pub. L. 107–296, title XXI, §2107, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2916, related to CFATS regulations.

Section 628, Pub. L. 107–296, title XXI, §2108, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2916, related to small covered chemical facilities.

Section 629, Pub. L. 107–296, title XXI, §2109, as added Pub. L. 113–254, §2(a), Dec. 18, 2014, 128 Stat. 2916, related to outreach to chemical facilities of interest.

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE AND TERMINATION DATES

Pub. L. 113–254, §4(a), Dec. 18, 2014, 128 Stat. 2918, provided that: "This Act [see Short Title of 2014 Amendment note set out under section 101 of this title], and the amendments made by this Act, shall take effect on the date that is 30 days after the date of enactment of this Act [Dec. 18, 2014]."

Pub. L. 113–254, §5, Dec. 18, 2014, 128 Stat. 2919, as amended by Pub. L. 116–2, §2, Jan. 18, 2019, 133 Stat. 5; Pub. L. 116–136, div. B, title VI, §16007, Mar. 27, 2020, 134 Stat. 546; Pub. L. 116–150, §1(a), July 22, 2020, 134 Stat. 679, provided that: "The authority provided under title XXI of the Homeland Security Act of 2002 [6 U.S.C. 621 et seq.], as added by section 2(a), shall terminate on July 27, 2023."

[Pub. L. 116–150, §1(b), July 22, 2020, 134 Stat. 679, provided that: "The amendment made by subsection (a) [amending section 5 of Pub. L. 113–254, set out above] shall take effect on the date that is 1 day after the date of enactment of this Act [July 22, 2020]."]

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13650. IMPROVING CHEMICAL FACILITY SAFETY AND SECURITY

Ex. Ord. No. 13650, Aug. 1, 2013, 78 F.R. 48029, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Purpose*. Chemicals, and the facilities where they are manufactured, stored, distributed, and used, are essential to today's economy. Past and recent tragedies have reminded us, however, that the handling and storage of chemicals are not without risk. The Federal Government has developed and implemented numerous programs aimed at reducing the safety risks and security risks associated with hazardous chemicals. However, additional measures can be taken by executive departments and agencies (agencies) with regulatory authority to further improve chemical facility safety and security in coordination with owners and operators.

SEC. 2. *Establishment of the Chemical Facility Safety and Security Working Group*. (a) There is established a Chemical Facility Safety and Security Working Group (Working Group) co-chaired by the Secretary of Homeland Security, the Administrator of the Environmental Protection Agency (EPA), and the Secretary of Labor or their designated representatives at the Assistant Secretary level or higher. In addition, the Working Group shall consist of the head of each of the following agencies or their designated representatives at the Assistant Secretary level or higher:

(i) the Department of Justice;

(ii) the Department of Agriculture; and

(iii) the Department of Transportation.

(b) In carrying out its responsibilities under this order, the Working Group shall consult with representatives

from:

(i) the Council on Environmental Quality;

(ii) the National Security Staff;

(iii) the Domestic Policy Council;

(iv) the Office of Science and Technology Policy;

(v) the Office of Management and Budget (OMB);

(vi) the White House Office of Cabinet Affairs; and

(vii) such other agencies and offices as the President may designate.

(c) The Working Group shall meet no less than quarterly to discuss the status of efforts to implement this order. The Working Group is encouraged to invite other affected agencies, such as the Nuclear Regulatory Commission, to attend these meetings as appropriate. Additionally, the Working Group shall provide, within 270 days of the date of this order, a status report to the President through the Chair of the Council on Environmental Quality and the Assistant to the President for Homeland Security and Counterterrorism.

SEC. 3. *Improving Operational Coordination with State, Local, and Tribal Partners*. (a) Within 135 days of the date of this order, the Working Group shall develop a plan to support and further enable efforts by State regulators, State, local, and tribal emergency responders, chemical facility owners and operators, and local and tribal communities to work together to improve chemical facility safety and security. In developing this plan, the Working Group shall:

(i) identify ways to improve coordination among the Federal Government, first responders, and State, local, and tribal entities;

(ii) take into account the capabilities, limitations, and needs of the first responder community;

(iii) identify ways to ensure that State homeland security advisors, State Emergency Response Commissions (SERCs), Tribal Emergency Response Commissions (TERCs), Local Emergency Planning Committees (LEPCs), Tribal Emergency Planning Committees (TEPCs), State regulators, and first responders have ready access to key information in a useable format, including by thoroughly reviewing categories of chemicals for which information is provided to first responders and the manner in which it is made available, so as to prevent, prepare for, and respond to chemical incidents;

(iv) identify areas, in collaboration with State, local, and tribal governments and private sector partners, where joint collaborative programs can be developed or enhanced, including by better integrating existing authorities, jurisdictional responsibilities, and regulatory programs in order to achieve a more comprehensive engagement on chemical risk management;

(v) identify opportunities and mechanisms to improve response procedures and to enhance information sharing and collaborative planning between chemical facility owners and operators, TEPCs, LEPCs, and first responders;

(vi) working with the National Response Team (NRT) and Regional Response Teams (RRTs), identify means for Federal technical assistance to support developing, implementing, exercising, and revising State, local, and tribal emergency contingency plans, including improved training; and

(vii) examine opportunities to improve public access to information about chemical facility risks consistent with national security needs and appropriate protection of confidential business information.

(b) Within 90 days of the date of this order, the Attorney General, through the head of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), shall assess the feasibility of sharing data related to the storage of explosive materials with SERCs, TEPCs, and LEPCs.

(c) Within 90 days of the date of this order, the Secretary of Homeland Security shall assess the feasibility of sharing Chemical Facility Anti-Terrorism Standards (CFATS) data with SERCs, TEPCs, and LEPCs on a categorical basis.

SEC. 4. *Enhanced Federal Coordination*. In order to enhance Federal coordination regarding chemical facility safety and security:

(a) Within 45 days of the date of this order, the Working Group shall deploy a pilot program, involving the EPA, Department of Labor, Department of Homeland Security, and any other appropriate agency, to validate best practices and to test innovative methods for Federal interagency collaboration regarding chemical facility safety and security. The pilot program shall operate in at least one region and shall integrate regional Federal, State, local, and tribal assets, where appropriate. The pilot program shall include innovative and effective methods of collecting, storing, and using facility information, stakeholder outreach, inspection planning, and, as appropriate, joint inspection efforts. The Working Group shall take into account the results of the pilot program in developing integrated standard operating procedures pursuant to subsection (b) of this section.

(b) Within 270 days of the date of this order, the Working Group shall create comprehensive and integrated standard operating procedures for a unified Federal approach for identifying and responding to risks in chemical facilities (including during pre-inspection, inspection execution, post-inspection, and post-accident

investigation activities), incident reporting and response procedures, enforcement, and collection, storage, and use of facility information. This effort shall reflect best practices and shall include agency-to-agency referrals and joint inspection procedures where possible and appropriate, as well as consultation with the Federal Emergency Management Agency on post-accident response activities.

(c) Within 90 days of the date of this order, the Working Group shall consult with the Chemical Safety Board (CSB) and determine what, if any, changes are required to existing memorandums of understanding (MOUs) and processes between EPA and CSB, ATF and CSB, and the Occupational Safety and Health Administration and CSB for timely and full disclosure of information. To the extent appropriate, the Working Group may develop a single model MOU with CSB in lieu of existing agreements.

SEC. 5. *Enhanced Information Collection and Sharing*. In order to enhance information collection by and sharing across agencies to support more informed decisionmaking, streamline reporting requirements, and reduce duplicative efforts:

(a) Within 90 days of the date of this order, the Working Group shall develop an analysis, including recommendations, on the potential to improve information collection by and sharing between agencies to help identify chemical facilities which may not have provided all required information or may be non-compliant with Federal requirements to ensure chemical facility safety. This analysis should consider ongoing data-sharing efforts, other federally collected information, and chemical facility reporting among agencies (including information shared with State, local, and tribal governments).

(b) Within 180 days of the date of this order, the Working Group shall produce a proposal for a coordinated, flexible data-sharing process which can be utilized to track data submitted to agencies for federally regulated chemical facilities, including locations, chemicals, regulated entities, previous infractions, and other relevant information. The proposal shall allow for the sharing of information with and by State, local, and tribal entities where possible, consistent with section 3 of this order, and shall address computer-based and non-computer-based means for improving the process in the short-term, if they exist.

(c) Within 180 days of the date of this order, the Working Group shall identify and recommend possible changes to streamline and otherwise improve data collection to meet the needs of the public and Federal, State, local, and tribal agencies (including those charged with protecting workers and the public), consistent with the Paperwork Reduction Act and other relevant authorities, including opportunities to lessen the reporting burden on regulated industries. To the extent feasible, efforts shall minimize the duplicative collection of information while ensuring that pertinent information is shared with all key entities.

SEC. 6. *Policy, Regulation, and Standards Modernization*. (a) In order to enhance safety and security in chemical facilities by modernizing key policies, regulations, and standards, the Working Group shall:

(i) within 90 days of the date of this order, develop options for improved chemical facility safety and security that identifies improvements to existing risk management practices through agency programs, private sector initiatives, Government guidance, outreach, standards, and regulations;

(ii) within 90 days of developing the options described in subsection (a)(i) of this section, engage key stakeholders to discuss the options and other means to improve chemical risk management that may be available; and

(iii) within 90 days of completing the outreach and consultation effort described in subsection (a)(ii) of this section, develop a plan for implementing practical and effective improvements to chemical risk management identified pursuant to subsections (a)(i) and (ii) of this section.

(b) Within 90 days of the date of this order, the Secretary of Homeland Security, the Secretary of Labor, and the Secretary of Agriculture shall develop a list of potential regulatory and legislative proposals to improve the safe and secure storage, handling, and sale of ammonium nitrate and identify ways in which ammonium nitrate safety and security can be enhanced under existing authorities.

(c) Within 90 days of the date of this order, the Administrator of EPA and the Secretary of Labor shall review the chemical hazards covered by the Risk Management Program (RMP) and the Process Safety Management Standard (PSM) and determine if the RMP or PSM can and should be expanded to address additional regulated substances and types of hazards. In addition, the EPA and the Department of Labor shall develop a plan, including a timeline and resource requirements, to expand, implement, and enforce the RMP and PSM in a manner that addresses the additional regulated substances and types of hazards.

(d) Within 90 days of the date of this order, the Secretary of Homeland Security shall identify a list of chemicals, including poisons and reactive substances, that should be considered for addition to the CFATS Chemicals of Interest list.

(e) Within 90 days of the date of this order, the Secretary of Labor shall:

(i) identify any changes that need to be made in the retail and commercial grade exemptions in the PSM Standard; and

(ii) issue a Request for Information designed to identify issues related to modernization of the PSM

Standard and related standards necessary to meet the goal of preventing major chemical accidents.

SEC. 7. *Identification of Best Practices*. The Working Group shall convene stakeholders, including chemical producers, chemical storage companies, agricultural supply companies, State and local regulators, chemical critical infrastructure owners and operators, first responders, labor organizations representing affected workers, environmental and community groups, and consensus standards organizations, in order to identify and share successes to date and best practices to reduce safety risks and security risks in the production and storage of potentially harmful chemicals, including through the use of safer alternatives, adoption of best practices, and potential public-private partnerships.

SEC. 8. *General Provisions*. (a) This order shall be implemented consistent with applicable law, including international trade obligations, and subject to the availability of appropriations.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to a department, agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to the National Security Staff deemed to be a reference to the National Security Council Staff, see Ex. Ord. No. 13657, set out as a note under section 3021 of Title 50, War and National Defense.]

SUBCHAPTER XVII—ANTI-TRAFFICKING TRAINING FOR DEPARTMENT OF HOMELAND SECURITY PERSONNEL

§641. Definitions

In this subchapter:

(1) Department

The term "Department" means the Department of Homeland Security.

(2) Human trafficking

The term "human trafficking" means an act or practice described in paragraph (9) or (10) [1] of section 7102 of title 22.

(3) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(Pub. L. 114–22, title IX, §901, May 29, 2015, 129 Stat. 264.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title IX of Pub. L. 114–22, which is classified principally to this subchapter. For complete classification of title IX to the Code, see Tables.

Paragraphs (9) and (10) of section 7102 of title 22, referred to in par. (2), were redesignated pars. (11) and (12), respectively, of section 7102 of title 22 by Pub. L. 115–427, §2(1), Jan. 9, 2019, 132 Stat. 5503.

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *See References in Text note below.*

§642. Training for Department personnel to identify human trafficking

(a) In general

Not later than 180 days after May 29, 2015, the Secretary shall implement a program to—

(1) train and periodically retrain relevant Transportation Security Administration, U.S. Customs and Border Protection, and other Department personnel that the Secretary considers appropriate, with respect to how to effectively deter, detect, and disrupt human trafficking, and, where appropriate, interdict a suspected perpetrator of human trafficking, during the course of their primary roles and responsibilities; and

(2) ensure that the personnel referred to in paragraph (1) regularly receive current information on matters related to the detection of human trafficking, including information that becomes available outside of the Department's initial or periodic retraining schedule, to the extent relevant to their official duties and consistent with applicable information and privacy laws.

(b) Training described

The training referred to in subsection (a) may be conducted through in-class or virtual learning capabilities, and shall include—

(1) methods for identifying suspected victims of human trafficking and, where appropriate, perpetrators of human trafficking;

(2) for appropriate personnel, methods to approach a suspected victim of human trafficking, where appropriate, in a manner that is sensitive to the suspected victim and is not likely to alert a suspected perpetrator of human trafficking;

(3) training that is most appropriate for a particular location or environment in which the personnel receiving such training perform their official duties;

(4) other topics determined by the Secretary to be appropriate; and

(5) a post-training evaluation for personnel receiving the training.

(c) Training curriculum review

The Secretary shall annually reassess the training program established under subsection (a) to ensure it is consistent with current techniques, patterns, and trends associated with human trafficking.

(Pub. L. 114–22, title IX, §902, May 29, 2015, 129 Stat. 265.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§643. Certification and report to Congress

(a) Certification

Not later than 1 year after May 29, 2015, the Secretary shall certify to Congress that all personnel referred to in section 402(a) [1] have successfully completed the training required under that section.

(b) Report to Congress

Not later than 1 year after May 29, 2015, and annually thereafter, the Secretary shall report to Congress with respect to the overall effectiveness of the program required by this subchapter, the number of cases reported by Department personnel in which human trafficking was suspected, and, of those cases, the number of cases that were confirmed cases of human trafficking.

(Pub. L. 114–22, title IX, §903, May 29, 2015, 129 Stat. 265.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 402(a), referred to in subsec. (a), probably should be a reference to section 902(a), meaning section 902(a) of Pub. L. 114–22, which is classified to section 642(a) of this title. Section 402 of Pub. L. 114–22, which is classified to section 21301 of Title 34, Crime Control and Law Enforcement, does not contain a subsec. (a) and does not relate to the training of personnel.

This subchapter, referred to in subsec. (b), was in the original "this title", meaning title IX of Pub. L. 114–22, which is classified principally to this subchapter. For complete classification of title IX to the Code, see Tables.

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] *See References in Text note below.*

§644. Assistance to non-Federal entities

The Secretary may provide training curricula to any State, local, or tribal government or private organization to assist the government or organization in establishing a program of training to identify human trafficking, upon request from the government or organization.

(Pub. L. 114–22, title IX, §904, May 29, 2015, 129 Stat. 266.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§645. Victim protection training for the Department of Homeland Security

(a) Directive to DHS law enforcement officials and task forces

(1) In general

Not later than 180 days after December 21, 2018, the Secretary shall issue a directive to—

(A) all Federal law enforcement officers and relevant personnel employed by the Department who may be involved in the investigation of human trafficking offenses; and

(B) members of all task forces led by the Department that participate in the investigation of human trafficking offenses.

(2) Required instructions

The directive required to be issued under paragraph (1) shall include instructions on—

(A) the investigation of individuals who patronize or solicit human trafficking victims as being engaged in severe trafficking in persons and how such individuals should be investigated for their roles in severe trafficking in persons; and

(B) how victims of sex or labor trafficking often engage in criminal acts as a direct result of severe trafficking in persons and such individuals are victims of a crime and affirmative measures should be taken to avoid arresting, charging, or prosecuting such individuals for any offense that is the direct result of their victimization.

(b) Victim screening protocol

(1) In general

Not later than 180 days after December 21, 2018, the Secretary shall issue a screening protocol for use during all anti-trafficking law enforcement operations in which the Department is involved.

(2) Requirements

The protocol required to be issued under paragraph (1) shall—

(A) require the individual screening of all adults and children who are suspected of engaging in commercial sex acts, child labor that is a violation of law, or work in violation of labor standards to determine whether each individual screened is a victim of human trafficking;

(B) require affirmative measures to avoid arresting, charging, or prosecuting human trafficking victims for any offense that is the direct result of their victimization;

(C) be developed in consultation with relevant interagency partners and nongovernmental organizations that specialize in the prevention of human trafficking or in the identification and support of victims of human trafficking and survivors of human trafficking; and

(D) include—

(i) procedures and practices to ensure that the screening process minimizes trauma or revictimization of the person being screened; and

(ii) guidelines on assisting victims of human trafficking in identifying and receiving restorative services.

(c) Mandatory training

The training described in sections 642 and 644 of this title shall include training necessary to implement—

(1) the directive required under subsection (a); and

(2) the protocol required under subsection (b).

(Pub. L. 114–22, title IX, §906, as added Pub. L. 115–392, §5(a), Dec. 21, 2018, 132 Stat. 5252.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§645a. Human trafficking assessment

Not later than 1 year after December 21, 2018, and annually thereafter, the Executive Associate Director of Homeland Security Investigations shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives a report on human trafficking investigations undertaken by Homeland Security Investigations that includes—

(1) the number of confirmed human trafficking investigations by category, including labor trafficking, sex trafficking, and transnational and domestic human trafficking;

(2) the number of victims by category, including—

(A) whether the victim is a victim of sex trafficking or a victim of labor trafficking; and

(B) whether the victim is a minor or an adult; and

(3) an analysis of the data described in paragraphs (1) and (2) and other data available to Homeland Security Investigations that indicates any general human trafficking or investigatory trends.

(Pub. L. 115–393, title IV, §403, Dec. 21, 2018, 132 Stat. 5275.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Trafficking Victims Protection Act of 2017, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

§650. Definitions

Except as otherwise specifically provided, in this subchapter:

(1) Agency

The term "Agency" means the Cybersecurity and Infrastructure Security Agency.

(2) Appropriate congressional committees

The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(3) Cloud service provider

The term "cloud service provider" means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

(4) Critical infrastructure information

The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(5) Cyber threat indicator

The term "cyber threat indicator" means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the

information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(6) Cybersecurity purpose

The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(7) Cybersecurity risk

The term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(8) Cybersecurity threat

(A) In general

Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) Exclusion

The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(9) Defensive measure

(A) In general

Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) Exclusion

The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity, as defined in section 1501 of this title, operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(10) Director

The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(11) Homeland Security Enterprise

The term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

(12) Incident

The term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

(13) Information Sharing and Analysis Organization

The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, a compromise, or an incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(14) Information system

The term "information system"—

(A) has the meaning given the term in section 3502 of title 44; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(15) Intelligence community

The term "intelligence community" has the meaning given the term in section 3003(4) of title 50.

(16) Malicious cyber command and control

The term "malicious cyber command and control" means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(17) Malicious reconnaissance

The term "malicious reconnaissance" [1] a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(18) Managed service provider

The term "managed service provider" means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

(19) Monitor

The term "monitor" means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(20) National cybersecurity asset response activities

The term "national cybersecurity asset response activities" means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading

effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(21) National security system

The term "national security system" has the meaning given the term in section 11103 of title 40.

(22) Ransomware attack

The term "ransomware attack"—

(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(B) does not include any such event in which the demand for payment is—

(i) not genuine; or

(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

(23) Sector Risk Management Agency

The term "Sector Risk Management Agency" means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

(24) Security control

The term "security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(25) Security vulnerability

The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(26) Sharing

The term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

(27) SLTT entity

The term "SLTT entity" means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.

(28) Supply chain compromise

The term "supply chain compromise" means an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

(Pub. L. 107–296, title XXII, §2200, as added Pub. L. 117–263, div. G, title LXXI, §7143(b)(1), Dec. 23, 2022, 136 Stat. 3654.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 117–263, div. G, title LXXI, §7143(f), Dec. 23, 2022, 136 Stat. 3664, provided that:

"(1) INTERPRETATION OF TECHNICAL CORRECTIONS.—Nothing in the amendments made by subsections (a) through (d) [enacting this section and amending sections 195f, 321l, 464, 571, 624, 651 to 652a, 655, 656, 659 to 663, 665, 665b, 665d, 665g, 665i, 671, 681, 1501, 1521, and 1524 of this title, sections 278g–3a and 648 of Title 15, Commerce and Trade, section 824s–1 of Title 16, Conservation, sections 300hh–10 and 18723 of Title 42, The Public Health and Welfare, section 70101 of Title 46, Shipping, and sections 3049a and 3371a of Title 50, War and National Defense] shall be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in section 3502 of title 44, United States Code) or officer or employee of the United States on or before the date of enactment of this Act [Dec. 23, 2022].

"(2) INTERPRETATION OF REFERENCES TO DEFINITIONS.—Any reference to a term defined in the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) on the day before the date of enactment of this Act that is defined in section 2200 of that Act [6 U.S.C. 650] pursuant to the amendments made under this Act [Pub. L. 117–263, see Tables for classification] shall be deemed to be a reference to that term as defined in section 2200 of the Homeland Security Act of 2002, as added by this Act."

[1] *So in original. Probably should be followed by "means".*

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

§651. Definition

In this part, the term "Cybersecurity Advisory Committee" means the advisory committee established under section 665e(a) of this title.

(Pub. L. 107–296, title XXII, §2201, as added Pub. L. 115–278, §2(a), Nov. 16, 2018, 132 Stat. 4168; amended Pub. L. 116–283, div. H, title XC, §9002(c)(2)(C), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–150, §2(1), June 21, 2022, 136 Stat. 1295; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(B), Dec. 23, 2022, 136 Stat. 3659.)

EDITORIAL NOTES

AMENDMENTS

2022—Pub. L. 117–263 amended section generally. Prior to amendment, section defined critical infrastructure information, cybersecurity risk, cybersecurity threat, national cybersecurity asset response activities, Sector Risk Management Agency, sharing, and SLTT entity.

Par. (7). Pub. L. 117–150 added par. (7).

2021—Par. (5). Pub. L. 116–283 substituted "Sector Risk Management Agency" for "Sector-Specific Agency" in heading and "Sector Risk Management Agency" for "Sector-Specific Agency" in text.

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, and references to terms defined in the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) on the day before Dec. 23, 2022, that are defined in section 650 of this title are deemed to be references to those terms as defined in such section 650, see section 7143(f) of Pub. L. 117–263, set out as a note under section 650 of this title.

CONSTRUCTION OF PUB. L. 115–278

Pub. L. 115–278, §5, Nov. 16, 2018, 132 Stat. 4186, provided that: "Nothing in this Act [see section 1 of Pub. L. 115–278, set out as a Short Title of 2018 Amendment note under section 101 of this title] or an amendment made by this Act may be construed as—

"(1) conferring new authorities to the Secretary of Homeland Security, including programmatic,

regulatory, or enforcement authorities, outside of the authorities in existence on the day before the date of enactment of this Act [Nov. 16, 2018];

"(2) reducing or limiting the programmatic, regulatory, or enforcement authority vested in any other Federal agency by statute; or

"(3) affecting in any manner the authority, existing on the day before the date of enactment of this Act, of any other Federal agency or component of the Department of Homeland Security."

NATIONAL CYBER EXERCISES

Pub. L. 116–283, div. A, title XVII, §1744, Jan. 1, 2021, 134 Stat. 4135, provided that:

"(a) REQUIREMENT.—Not later than December 31, 2023, the Secretary of Homeland Security, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall conduct an exercise, which may be a tabletop exercise, to test the resilience, response, and recovery of the United States to a significant cyber incident impacting critical infrastructure. The Secretary shall convene similar exercises not fewer than three times, in consultation with such officials, until 2033.

"(b) PLANNING AND PREPARATION.—The exercises required under subsection (a) shall be prepared by—

"(1) appropriate personnel from—

"(A) the Department of Homeland Security;

"(B) the Department of Defense; and

"(C) the Department of Justice; and

"(2) appropriate elements of the intelligence community, identified by the Director of National Intelligence.

"(c) SUBMISSION TO CONGRESS.—For each fiscal year in which an exercise is planned, the Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall submit to the appropriate congressional committees a plan for the exercise not later than 180 days prior to the exercise. Each such plan shall include information regarding the goals of the exercise at issue, how the exercise is to be carried out, where and when the exercise will take place, how many individuals are expected to participate from each Federal agency specified in subsection (b), and the costs or other resources associated with the exercise.

"(d) PARTICIPANTS.—

"(1) FEDERAL GOVERNMENT PARTICIPANTS.—Appropriate personnel from the following Federal agencies shall participate in each exercise required under subsection (a):

"(A) The Department of Homeland Security.

"(B) The Department of Defense, as identified by the Secretary of Defense.

"(C) Elements of the intelligence community, as identified by the Director of National Intelligence.

"(D) The Department of Justice, as identified by the Attorney General.

"(E) Sector-specific agencies, as determined by the Secretary of Homeland Security.

"(2) STATE AND LOCAL GOVERNMENTS.—The Secretary shall invite representatives from State, local, and Tribal governments to participate in each exercise required under subsection (a) if the Secretary determines such is appropriate.

"(3) PRIVATE ENTITIES.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary, in consultation with the senior representative of the sector-specific agencies participating in such exercise in accordance with paragraph (1)(E), shall invite the following individuals to participate:

"(A) Representatives from appropriate private entities.

"(B) Other individuals whom the Secretary determines will best assist the United States in preparing for, and defending against, a significant cyber incident impacting critical infrastructure.

"(4) INTERNATIONAL PARTNERS.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary may, in coordination with the Secretary of State, invite allies and partners of the United States to participate in such exercise.

"(e) OBSERVERS.—The Secretary may invite representatives from the executive and legislative branches of the Federal Government to observe an exercise required under subsection (a).

"(f) ELEMENTS.—Each exercise required under subsection (a) shall include the following elements:

"(1) Exercising the orchestration of cybersecurity response and the provision of cyber support to Federal, State, local, and Tribal governments and private entities, including the exercise of the command, control, and deconfliction of—

"(A) operational responses through interagency coordination processes and response groups; and

"(B) each Federal agency participating in such exercise in accordance with subsection (d)(1).

"(2) Testing of the information sharing needs and capabilities of exercise participants.

"(3) Testing of the relevant policy, guidance, and doctrine, including the National Cyber Incident Response Plan of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

"(4) Testing of the integration and interoperability between the entities participating in the exercise in accordance with subsection (d).

"(5) Exercising the integration and interoperability of the cybersecurity operation centers of the Federal Government, as appropriate, in coordination with appropriate cabinet level officials.

"(g) BRIEFING.—

"(1) IN GENERAL.—Not later than 180 days after the date on which each exercise required under subsection (a) is conducted, the Secretary shall provide to the appropriate congressional committees a briefing on the exercise.

"(2) CONTENTS.—Each briefing required under paragraph (1) shall include—

"(A) an assessment of the decision and response gaps observed in the exercise at issue;

"(B) proposed recommendations to improve the resilience, response, and recovery of the United States to a significant cyber attack against critical infrastructure; and

"(C) appropriate plans to address the recommendations proposed under subparagraph (B).

"(h) REPEAL.—[Repealed section 1648(b) of Pub. L. 114–92, 129 Stat. 1119.]

"(i) DEFINITIONS.—In this section:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the Committee on Armed Services of the Senate;

"(B) the Committee on Armed Services of the House of Representatives;

"(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(D) the Committee on Homeland Security of the House of Representatives;

"(E) the Select Committee on Intelligence of the Senate;

"(F) the Permanent Select Committee on Intelligence of the House of Representatives;

"(G) the Committee on the Judiciary of the Senate;

"(H) the Committee on the Judiciary of the House of Representatives;

"(I) the Committee on Commerce, Science, and Transportation of the Senate;

"(J) the Committee on Science, Space, and Technology of the House of Representatives;

"(K) the Committee on Foreign Relations of the Senate; and

"(L) the Committee on Foreign Affairs of the House of Representatives.

"(2) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term 'element of the intelligence community' means an element specified or designated under section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(3) PRIVATE ENTITY.—The term 'private entity' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

"(4) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(5) SECTOR-SPECIFIC AGENCY.—The term 'sector-specific agency' has the meaning given the term 'Sector-Specific Agency' in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651) [see 6 U.S.C. 650].

"(6) STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States."

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13905. STRENGTHENING NATIONAL RESILIENCE THROUGH RESPONSIBLE USE OF POSITIONING, NAVIGATION, AND TIMING SERVICES

Ex. Ord. No. 13905, Feb. 12, 2020, 85 F.R. 9359, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Purpose*. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure. Since the United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid,

communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response. Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

SEC. 2. *Definitions*. As used in this order:

(a) "PNT services" means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(b) "Responsible use of PNT services" means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(c) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters.

(d) "PNT profile" means a description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.

(e) "Sector-Specific Agency" (SSA) is the executive department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

SEC. 3. *Policy*. It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.

To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

SEC. 4. *Implementation*. (a) Within 1 year of the date of this order [Feb. 12, 2020], the Secretary of Commerce, in coordination with the heads of SSAs and in consultation, as appropriate, with the private sector, shall develop and make available, to at least the appropriate agencies and private sector users, PNT profiles. The PNT profiles will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Once made available, the PNT profiles shall be reviewed every 2 years and, as necessary, updated.

(b) The Secretary of Defense, Secretary of Transportation, and Secretary of Homeland Security shall refer to the PNT profiles created pursuant to subsection (a) of this section in updates to the Federal Radionavigation Plan.

(c) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services. The results of the tests carried out under that plan shall be used to inform updates to the PNT profiles identified in subsection (a) of this section.

(d) Within 90 days of the PNT profiles being made available, the heads of SSAs and the heads of other executive departments and agencies (agencies), as appropriate, through the Secretary of Homeland Security, shall develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services. The heads of SSAs and the heads of other agencies, as appropriate, shall update the requirements as necessary.

(e) Within 180 days of the completion of any of the duties described in subsection (d) of this section, and consistent with applicable law and to the maximum extent practicable, the Federal Acquisition Regulatory Council, in consultation with the heads of SSAs and the heads of other agencies, as appropriate, shall incorporate the requirements developed under subsection (d) of this section into Federal contracts for products, systems, and services that integrate or use PNT services.

(f) Within 1 year of the PNT profiles being made available, and biennially thereafter, the heads of SSAs and

the heads of other agencies, as appropriate, through the Secretary of Homeland Security, shall submit a report to the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy (OSTP) on the extent to which the PNT profiles have been adopted in their respective agencies' acquisitions and, to the extent possible, the extent to which PNT profiles have been adopted by owners and operators of critical infrastructure.

(g) Within 180 days of the date of this order, the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services. Each pilot program shall be completed within 1 year of developing the plan, and the results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities.

(h) Within 1 year of the date of this order, the Director of OSTP shall coordinate the development of a national plan, which shall be informed by existing initiatives, for the R&D and pilot testing of additional, robust, and secure PNT services that are not dependent on global navigation satellite systems (GNSS). The plan shall also include approaches to integrate and use multiple PNT services to enhance the resilience of critical infrastructure.

Once the plan is published, the Director of OSTP shall coordinate updates to the plan every 4 years, or as appropriate.

(i) Within 180 days of the date of this order, the Secretary of Commerce shall make available a GNSS-independent source of Coordinated Universal Time, to support the needs of critical infrastructure owners and operators, for the public and private sectors to access.

SEC. 5. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

§652. Cybersecurity and Infrastructure Security Agency

(a) Redesignation

(1) In general

The National Protection and Programs Directorate of the Department shall, on and after November 16, 2018, be known as the "Cybersecurity and Infrastructure Security Agency".

(2) References

Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) Director

(1) In general

The Agency shall be headed by the Director, who shall report to the Secretary.

(2) Qualifications

(A) In general

The Director shall be appointed from among individuals who have—

(i) extensive knowledge in at least two of the areas specified in subparagraph (B); and

(ii) not fewer than five years of demonstrated experience in efforts to foster coordination and collaboration between the Federal Government, the private sector, and other entities on issues related to cybersecurity, infrastructure security, or security risk management.

(B) Specified areas

The areas specified in this subparagraph are the following:

(i) Cybersecurity.

(ii) Infrastructure security.

(iii) Security risk management.

(3) Reference

Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 113(a)(1)(H) of this title as in effect on the day before November 16, 2018, in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of the Cybersecurity and Infrastructure Security Agency.

(c) Responsibilities

The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44 and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113)), including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(6) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this chapter;

(8) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

(9) carry out emergency communications responsibilities, in accordance with subchapter XIII;

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate;

(11) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security;

(12) appoint a Cybersecurity State Coordinator in each State, as described in section 665c of

this title;

(13) carry out the duties and authorities relating to the .gov internet domain, as described in section 665 of this title; and

(14) carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) Deputy Director

There shall be in the Agency a Deputy Director of the Cybersecurity and Infrastructure Security Agency who shall—

(1) assist the Director in the management of the Agency; and

(2) report to the Director.

(e) Cybersecurity and infrastructure security authorities of the Secretary

(1) In general

The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 122 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this subchapter, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within the Department to other Federal Government agencies with responsibilities relating to homeland security and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this chapter is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 121(g) of this title.

(P) To carry out the functions of the national cybersecurity and communications integration center under section 659 of this title.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under subchapter XVI and the secure handling of ammonium nitrate program established under part J of subchapter VIII, or any successor programs.

(R) To encourage and build cybersecurity awareness and competency across the United States and to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department, including by—

(i) overseeing elementary and secondary cybersecurity education and awareness related programs at the Agency;

(ii) leading efforts to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department;

(iii) encouraging and building cybersecurity awareness and competency across the United States; and

(iv) carrying out cybersecurity related workforce development activities, including through—

(I) increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and

(II) building awareness of and competency in cybersecurity across the civilian Federal Government workforce.

(2) Reallocation

The Secretary may reallocate within the Agency the functions specified in sections 653(b) and

654(b) of this title, consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) Staff

(A) In general

The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

(B) Private sector analysts

Analysts under this subsection may include analysts from the private sector.

(C) Security clearances

Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) Detail of personnel

(A) In general

In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) Agencies

The Federal agencies described in this subparagraph are—

(i) the Department of State;
(ii) the Central Intelligence Agency;
(iii) the Federal Bureau of Investigation;
(iv) the National Security Agency;
(v) the National Geospatial-Intelligence Agency;
(vi) the Defense Intelligence Agency;
(vii) Sector-Specific Agencies; and
(viii) any other agency of the Federal Government that the President considers appropriate.

(C) Interagency agreements

The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) Basis

The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) Composition

The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Executive Assistant Director.
(2) The Infrastructure Security Division, headed by an Executive Assistant Director.
(3) The Emergency Communications Division under subchapter XIII, headed by an Executive Assistant Director.

(g) Co-location

(1) In general

To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) Coordination

When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) Privacy

(1) In general

There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) Responsibilities

The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5 (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) Savings

Nothing in this subchapter may be construed as affecting in any manner the authority, existing on the day before November 16, 2018, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114–94).

(Pub. L. 107–296, title XXII, §2202, as added Pub. L. 115–278, §2(a), Nov. 16, 2018, 132 Stat. 4169; amended Pub. L. 116–260, div. U, title IX, §904(b)(1)(A), Dec. 27, 2020, 134 Stat. 2298; Pub. L. 116–283, div. A, title XVII, §§1717(a)(1)(A), 1719(a), (b), div. H, title XC, §§9001(a), 9002(c)(2)(D), Jan. 1, 2021, 134 Stat. 4099, 4105, 4766, 4773; Pub. L. 117–81, div. A, title XV, §§1547(b)(1)(A)(i), (B), 1549(a), Dec. 27, 2021, 135 Stat. 2060, 2061, 2063; Pub. L. 117–263, div. G, title LXXI, §7143(a)(1), (b)(2)(C), (c)(5), Dec. 23, 2022, 136 Stat. 3654, 3659, 3663.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Cybersecurity Act of 2015, referred to in subsec. (c)(3), is div. N of Pub. L. 114–113, Dec. 18, 2015, 129 Stat. 2935. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

This chapter, referred to in subsecs. (c)(7) and (e)(1)(J), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2022—Pub. L. 117–263, §7143(a)(1), made amendment identical to that made by Pub. L. 117–81, §1547(b)(1)(B). See 2021 Amendment note below.

Subsec. (a)(1). Pub. L. 117–263, §7143(b)(2)(C)(i), which directed striking out "(in this part referred to as the Agency)", was executed by striking out "(in this part referred to as the 'Agency')" before period at end, to reflect the probable intent of Congress.

Subsec. (b)(1). Pub. L. 117–263, §7143(b)(2)(C)(ii), substituted "the Director" for "a Director of Cybersecurity and Infrastructure Security (in this part referred to as the 'Director')".

Subsec. (b)(3). Pub. L. 117–263, §7143(c)(5)(A), substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security of the Department".

Subsec. (d). Pub. L. 117–263, §7143(c)(5)(B), substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security" in introductory provisions.

Subsec. (f). Pub. L. 117–263, §7143(b)(2)(C)(iii), inserted "Executive" before "Assistant Director" in pars. (1) to (3).

2021—Pub. L. 117–81, §1547(b)(1)(B), made technical amendment to directory language of Pub. L. 116–260, §904(b)(1). See 2020 Amendment notes below.

Subsec. (b)(2), (3). Pub. L. 116–283, §9001(a), added par. (2) and redesignated former par. (2) as (3).

Subsec. (c)(3). Pub. L. 117–81, §1549(a), substituted ", including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;" for semicolon at end.

Subsec. (c)(10). Pub. L. 116–283, §§1717(a)(1)(A)(i), 1719(b)(1), which directed identical amendments of par. (10) by striking out "and" at end, could not be executed because the word "and" did not appear at end after amendment by Pub. L. 116–260, §904(b)(1)(A)(i). See 2020 Amendment note below.

Subsec. (c)(11). Pub. L. 117–81, §1547(b)(1)(A)(i)(I), struck out "and" after the semicolon.

Pub. L. 116–283, §1719(b)(3), added par. (11) relating to providing education, training, and capacity development to Federal and non-Federal entities. Former par. (11), relating to appointment of a Cybersecurity State Coordinator, redesignated (12).

Pub. L. 116–283, §1717(a)(1)(A)(iii), added par. (11) relating to appointment of a Cybersecurity State Coordinator. Former par. (11), relating to the .gov internet domain, redesignated (12).

Subsec. (c)(12). Pub. L. 117–81, §1547(b)(1)(A)(i)(II), struck out "and" at end and made technical amendment to reference in original Act which appears in text as reference to section 665c of this title.

Pub. L. 116–283, §1719(b)(2), redesignated par. (11) relating to appointment of a Cybersecurity State Coordinator as (12).

Pub. L. 116–283, §1717(a)(1)(A)(ii), redesignated par. (11) relating to the .gov internet domain as (12).

Subsec. (c)(13). Pub. L. 117–81, §1547(b)(1)(A)(i)(III), redesignated par. (12) relating to the .gov internet domain as (13).

Subsec. (c)(14). Pub. L. 117–81, §1547(b)(1)(A)(i)(IV), redesignated par. (12) relating to carrying out such other duties and powers as (14).

Subsec. (e)(1)(R). Pub. L. 116–283, §1719(a), added subpar. (R).

Subsec. (i). Pub. L. 116–283, §9002(c)(2)(D), substituted "Sector Risk Management Agency" for "Sector-Specific Agency".

2020—Subsec. (c)(10). Pub. L. 116–260, §904(b)(1)(A)(i), as amended by Pub. L. 117–81, §1547(b)(1)(B), struck out "and" at end.

Subsec. (c)(11), (12). Pub. L. 116–260, §904(b)(1)(A)(ii), (iii), as amended by Pub. L. 117–81, §1547(b)(1)(B), added par. (11) relating to the .gov internet domain and redesignated former par. (11) relating to carrying out such other duties and powers as (12).

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2022 AMENDMENT

Pub. L. 117–263, div. G, title LXXI, §7143(a)(2), Dec. 23, 2022, 136 Stat. 3654, provided that: "The amendment made by paragraph (1) [amending this section and section 665 of this title] shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260)."

CONSTRUCTION OF 2022 AMENDMENT

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

CONSTRUCTION OF 2021 AMENDMENT

Amendment by section 1717(a)(1)(A) of Pub. L. 116–283 not to be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents, see section 1717(a)(4) of Pub. L. 116–283, set out as a note under section 665c of this title.

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM

Pub. L. 117–122, May 12, 2022, 136 Stat. 1193, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'National Cybersecurity Preparedness Consortium Act of 2021'.

"SEC. 2. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

"(a) IN GENERAL.—The Secretary may work with one or more consortia to support efforts to address cybersecurity risks and incidents.

"(b) ASSISTANCE TO DHS.—The Secretary may work with one or more consortia to carry out the Secretary's responsibility pursuant to section 2202(e)(1)(P) of the Homeland Security Act of 2002 (6 U.S.C. 652(e)(1)(P)) to—

"(1) provide training and education to State, Tribal, and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, in accordance with applicable law;

"(2) develop and update a curriculum utilizing existing training and educational programs and models in accordance with section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), for State, Tribal, and local first responders and officials, related to cybersecurity risks and incidents;

"(3) provide technical assistance services, training, and educational programs to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of acts of terrorism, in accordance with such section 2209;

"(4) conduct cross-sector cybersecurity training, education, and simulation exercises for entities, including State and local governments and Tribal organizations, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, in accordance with section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c));

"(5) help States, Tribal organizations, and communities develop cybersecurity information sharing programs, in accordance with section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), for the dissemination of homeland security information related to cybersecurity risks and incidents;

"(6) help incorporate cybersecurity risk and incident prevention and response into existing State, Tribal, and local emergency plans, including continuity of operations plans; and

"(7) assist State governments and Tribal organizations in developing cybersecurity plans.

"(c) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this Act, the Secretary shall take into consideration the following:

"(1) Prior experience conducting cybersecurity training, education, and exercises for State and local entities.

"(2) Geographic diversity of the members of any such consortium so as to maximize coverage of the different regions of the United States.

"(3) The participation in such consortium of one or more historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges that participate in the National Centers of Excellence in Cybersecurity program, as carried out by the Department of Homeland Security.

"(d) METRICS.—If the Secretary works with a consortium under subsection (a), the Secretary shall measure the effectiveness of the activities undertaken by the consortium under this Act.

"(e) OUTREACH.—The Secretary shall conduct outreach to universities and colleges, including, in particular, outreach to historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges, regarding opportunities to support efforts to address cybersecurity risks and incidents, by working with the Secretary under subsection (a).

"(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize a consortium to control or direct any law enforcement agency in the exercise of the duties of the law enforcement agency.

"(g) DEFINITIONS.—In this section—

"(1) the term 'community college' has the meaning given the term 'junior or community college' in section 312 of the Higher Education Act of 1965 (20 U.S.C. 1058);

"(2) the term 'consortium' means a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training and education in support of homeland security;

"(3) the terms 'cybersecurity risk' and 'incident' have the meanings given those terms in section 2209(a) of the Homeland Security Act of 2002 (6 U.S.C. 659(a)) [see 6 U.S.C. 650(7), (12)];

"(4) the term 'Department' means the Department of Homeland Security;

"(5) the term 'Hispanic-serving institution' has the meaning given the term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a);

"(6) the term 'historically Black college and university' has the meaning given the term 'part B institution' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061);

"(7) the term 'minority-serving institution' means an institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a));

"(8) the term 'Secretary' means the Secretary of Homeland Security;

"(9) The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States;

"(10) the term 'Tribal Colleges and Universities' has the meaning given the term in section 316 of the Higher Education Act of 1965 (20 U.S.C. 1059c); and

"(11) the term 'Tribal organization' has the meaning given the term in section 4(e) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e))."

RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM

Pub. L. 117–103, div. Y, §105, Mar. 15, 2022, 136 Stat. 1055, provided that:

"(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act [Mar. 15, 2022], the Director [of the Cybersecurity and Infrastructure Security Agency] shall establish a ransomware vulnerability warning pilot program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

"(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

"(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

"(2) utilize existing authorities to identify information systems that contain the security vulnerabilities identified in paragraph (1).

"(c) ENTITY NOTIFICATION.—

"(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

"(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures under that section.

"(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

"(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

"(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

"(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

"(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act."

[For definitions of terms used in section 105 of div. Y of Pub. L. 117–103, set out above, see section 681 of this title, as made applicable by section 102(1) of div. Y of Pub. L. 117–103, which is set out as a note under section 665j of this title, and see section 650 of this title, as made applicable by section 7143(f)(2) of div. G of Pub. L. 117–263, which is set out as a note under section 650 of this title.]

PILOT PROGRAM ON PUBLIC-PRIVATE PARTNERSHIPS WITH INTERNET ECOSYSTEM COMPANIES TO DETECT AND DISRUPT ADVERSARY CYBER OPERATIONS

Pub. L. 117–81, div. A, title XV, §1550, Dec. 27, 2021, 135 Stat. 2064, provided that:

"(a) PILOT REQUIRED.—Not later than one year after the date of the enactment of this Act [Dec. 27,

2021], the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and in coordination with the Secretary of Defense and the National Cyber Director, shall commence a pilot program to assess the feasibility and advisability of entering into public-private partnerships with internet ecosystem companies to facilitate, within the bounds of applicable provisions of law and such companies' terms of service, policies, procedures, contracts, and other agreements, actions by such companies to discover and disrupt use by malicious cyber actors of the platforms, systems, services, and infrastructure of such companies.

"(b) PUBLIC-PRIVATE PARTNERSHIPS.—

"(1) IN GENERAL.—In carrying out the pilot program under subsection (a), the Secretary shall seek to enter into one or more public-private partnerships with internet ecosystem companies.

"(2) VOLUNTARY PARTICIPATION.—

"(A) IN GENERAL.—Participation by an internet ecosystem company in a public-private partnership under the pilot program, including in any activity described in subsection (c), shall be voluntary.

"(B) PROHIBITION.—No funds appropriated by any Act may be used to direct, pressure, coerce, or otherwise require that any internet ecosystem company take any action on their platforms, systems, services, or infrastructure as part of the pilot program.

"(c) AUTHORIZED ACTIVITIES.—In carrying out the pilot program under subsection (a), the Secretary may—

"(1) provide assistance to a participating internet ecosystem company to develop effective know-your-customer processes and requirements;

"(2) provide information, analytics, and technical assistance to improve the ability of participating companies to detect and prevent illicit or suspicious procurement, payment, and account creation on their own platforms, systems, services, or infrastructure;

"(3) develop and socialize best practices for the collection, retention, and sharing of data by participating internet ecosystem companies to support discovery of malicious cyber activity, investigations, and attribution on the platforms, systems, services, or infrastructure of such companies;

"(4) provide to participating internet ecosystem companies actionable, timely, and relevant information, such as information about ongoing operations and infrastructure, threats, tactics, and procedures, and indicators of compromise, to enable such companies to detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of such companies;

"(5) provide recommendations for (but not design, develop, install, operate, or maintain) operational workflows, assessment and compliance practices, and training that participating internet ecosystem companies can implement to reliably detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of such companies;

"(6) provide recommendations for accelerating, to the greatest extent practicable, the automation of existing or implemented operational workflows to operate at line-rate in order to enable real-time mitigation without the need for manual review or action;

"(7) provide recommendations for (but not design, develop, install, operate, or maintain) technical capabilities to enable participating internet ecosystem companies to collect and analyze data on malicious activities occurring on the platforms, systems, services, or infrastructure of such companies to detect and disrupt operations of malicious cyber actors; and

"(8) provide recommendations regarding relevant mitigations for suspected or discovered malicious cyber activity and thresholds for action.

"(d) COMPETITION CONCERNS.—Consistent with section 1905 of title 18, United States Code, the Secretary shall ensure that any trade secret or proprietary information of a participating internet ecosystem company made known to the Federal Government pursuant to a public-private partnership under the pilot program remains private and protected unless explicitly authorized by such company.

"(e) IMPARTIALITY.—In carrying out the pilot program under subsection (a), the Secretary may not take any action that is intended primarily to advance the particular business interests of an internet ecosystem company but is authorized to take actions that advance the interests of the United States, notwithstanding differential impact or benefit to a given company's or given companies' business interests.

"(f) RESPONSIBILITIES.—

"(1) SECRETARY OF HOMELAND SECURITY.—The Secretary shall exercise primary responsibility for the pilot program under subsection (a), including organizing and directing authorized activities with participating Federal Government organizations and internet ecosystem companies to achieve the objectives of the pilot program.

"(2) NATIONAL CYBER DIRECTOR.—The National Cyber Director shall support prioritization and

cross-agency coordination for the pilot program, including ensuring appropriate participation by participating agencies and the identification and prioritization of key private sector entities and initiatives for the pilot program.

"(3) SECRETARY OF DEFENSE.—The Secretary of Defense shall provide support and resources to the pilot program, including the provision of technical and operational expertise drawn from appropriate and relevant officials and components of the Department of Defense, including the National Security Agency, United States Cyber Command, the Chief Information Officer, the Office of the Secretary of Defense, military department Principal Cyber Advisors, and the Defense Advanced Research Projects Agency.

"(g) PARTICIPATION OF OTHER FEDERAL GOVERNMENT COMPONENTS.—The Secretary may invite to participate in the pilot program required under subsection (a) the heads of such departments or agencies as the Secretary considers appropriate.

"(h) INTEGRATION WITH OTHER EFFORTS.—The Secretary shall ensure that the pilot program required under subsection (a) makes use of, builds upon, and, as appropriate, integrates with and does not duplicate other efforts of the Department of Homeland Security and the Department of Defense relating to cybersecurity, including the following:

"(1) The Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

"(2) The Cybersecurity Collaboration Center and Enduring Security Framework of the National Security Agency.

"(i) RULES OF CONSTRUCTION.—

"(1) LIMITATION ON GOVERNMENT ACCESS TO DATA.—Nothing in this section authorizes sharing of information, including information relating to customers of internet ecosystem companies or private individuals, from an internet ecosystem company to an agency, officer, or employee of the Federal Government unless otherwise authorized by another provision of law.

"(2) STORED COMMUNICATIONS ACT.—Nothing in this section may be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').

"(3) THIRD PARTY CUSTOMERS.—Nothing in this section may be construed to require a third party, such as a customer or managed service provider of an internet ecosystem company, to participate in the pilot program under subsection (a).

"(j) BRIEFINGS.—

"(1) INITIAL.—

"(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary, in coordination with the Secretary of Defense and the National Cyber Director, shall brief the appropriate committees of Congress on the pilot program required under subsection (a).

"(B) ELEMENTS.—The briefing required under subparagraph (A) shall include the following:

"(i) The plans of the Secretary for the implementation of the pilot program.

"(ii) Identification of key priorities for the pilot program.

"(iii) Identification of any potential challenges in standing up the pilot program or impediments, such as a lack of liability protection, to private sector participation in the pilot program.

"(iv) A description of the roles and responsibilities in the pilot program of each participating Federal entity.

"(2) ANNUAL.—

"(A) IN GENERAL.—Not later than two years after the date of the enactment of this Act and annually thereafter for three years, the Secretary, in coordination with the Secretary of Defense and the National Cyber Director, shall brief the appropriate committees of Congress on the progress of the pilot program required under subsection (a).

"(B) ELEMENTS.—Each briefing required under subparagraph (A) shall include the following:

"(i) Recommendations for addressing relevant policy, budgetary, and legislative gaps to increase the effectiveness of the pilot program.

"(ii) Recommendations, such as providing liability protection, for increasing private sector participation in the pilot program.

"(iii) A description of the challenges encountered in carrying out the pilot program, including any concerns expressed by internet ecosystem companies regarding participation in the pilot program.

"(iv) The findings of the Secretary with respect to the feasibility and advisability of

extending or expanding the pilot program.

"(v) Such other matters as the Secretary considers appropriate.

"(k) TERMINATION.—The pilot program required under subsection (a) shall terminate on the date that is five years after the date of the enactment of this Act [Dec. 27, 2021].

"(l) DEFINITIONS.—In this section:

"(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

"(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate; and

"(B) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives.

"(2) INTERNET ECOSYSTEM COMPANY.—The term 'internet ecosystem company' means a business incorporated in the United States that provides cybersecurity services, internet service, content delivery services, Domain Name Service, cloud services, mobile telecommunications services, email and messaging services, internet browser services, or such other services as the Secretary determines appropriate for the purposes of the pilot program under subsection (a).

"(3) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security."

K–12 CYBERSECURITY

Pub. L. 117–47, Oct. 8, 2021, 135 Stat. 397, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'K–12 Cybersecurity Act of 2021'.

"SEC. 2. FINDINGS.

"Congress finds the following:

"(1) K–12 educational institutions across the United States are facing cyber attacks.

"(2) Cyber attacks place the information systems of K–12 educational institutions at risk of possible disclosure of sensitive student and employee information, including—

"(A) grades and information on scholastic development;

"(B) medical records;

"(C) family records; and

"(D) personally identifiable information.

"(3) Providing K–12 educational institutions with resources to aid cybersecurity efforts will help K–12 educational institutions prevent, detect, and respond to cyber events.

"SEC. 3. K–12 EDUCATION CYBERSECURITY INITIATIVE.

"(a) DEFINITIONS.—In this section:

"(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given the term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) [see 6 U.S.C. 650].

"(2) DIRECTOR.—The term 'Director' means the Director of Cybersecurity and Infrastructure Security.

"(3) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

"(4) K–12 EDUCATIONAL INSTITUTION.—The term 'K–12 educational institution' means an elementary school or a secondary school, as those terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

"(b) STUDY.—

"(1) IN GENERAL.—Not later than 120 days after the date of enactment of this Act [Oct. 8, 2021], the Director, in accordance with subsection (g)(1), shall conduct a study on the specific cybersecurity risks facing K–12 educational institutions that—

"(A) analyzes how identified cybersecurity risks specifically impact K–12 educational institutions;

"(B) includes an evaluation of the challenges K–12 educational institutions face in—

"(i) securing—

"(I) information systems owned, leased, or relied upon by K–12 educational institutions; and

"(II) sensitive student and employee records; and

"(ii) implementing cybersecurity protocols;

"(C) identifies cybersecurity challenges relating to remote learning; and

"(D) evaluates the most accessible ways to communicate cybersecurity recommendations and

tools.

"(2) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Director shall provide a Congressional briefing on the study conducted under paragraph (1).

"(c) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after the completion of the study required under subsection (b)(1), the Director, in accordance with subsection (g)(1), shall develop recommendations that include cybersecurity guidelines designed to assist K–12 educational institutions in facing the cybersecurity risks described in subsection (b)(1), using the findings of the study.

"(d) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the completion of the development of the recommendations required under subsection (c), the Director shall develop an online training toolkit designed for officials at K–12 educational institutions to—

"(1) educate the officials about the cybersecurity recommendations developed under subsection (c); and

"(2) provide strategies for the officials to implement the recommendations developed under subsection (c).

"(e) PUBLIC AVAILABILITY.—The Director shall make available on the website of the Department of Homeland Security with other information relating to school safety the following:

"(1) The findings of the study conducted under subsection (b)(1).

"(2) The cybersecurity recommendations developed under subsection (c).

"(3) The online training toolkit developed under subsection (d).

"(f) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under [subsection] (c) by K–12 educational institutions shall be voluntary.

"(g) CONSULTATION.—

"(1) IN GENERAL.—In the course of the conduction of the study required under subsection (b)(1) and the development of the recommendations required under subsection (c), the Director shall consult with individuals and entities focused on cybersecurity and education, as appropriate, including—

"(A) teachers;

"(B) school administrators;

"(C) Federal agencies;

"(D) non-Federal cybersecurity entities with experience in education issues; and

"(E) private sector organizations.

"(2) INAPPLICABILITY OF FACA.—The Federal Advisory Committee Act ([former] 5 U.S.C App.) [see 5 U.S.C. 1001 et seq.] shall not apply to any consultation under paragraph (1)."

UNDER SECRETARY RESPONSIBLE FOR OVERSEEING CRITICAL INFRASTRUCTURE PROTECTION, CYBERSECURITY AND RELATED PROGRAMS AUTHORIZED TO SERVE AS DIRECTOR OF CYBERSECURITY AND INFRASTRUCTURE SECURITY

Pub. L. 115–278, §2(b)(1), Nov. 16, 2018, 132 Stat. 4175, provided that: "The individual serving as the Under Secretary appointed pursuant to section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H)) of the Department of Homeland Security on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Director of Cybersecurity and Infrastructure Security of the Department on and after such date."

§652a. Sector Risk Management Agencies

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and the Committee on Armed Services in the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services in the Senate.

(2) Critical infrastructure

The term "critical infrastructure" has the meaning given that term in section 5195c(e) of title 42.

(3) Department

The term "Department" means the Department of Homeland Security.

(4) Director

The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency of the Department.

(5) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(7) [1] Sector Risk Management Agency

The term "Sector Risk Management Agency" has the meaning given the term in section 650 of this title.

(b) Critical infrastructure sector designation

(1) Initial review

Not later than 180 days after January 1, 2021, the Secretary, in consultation with the heads of Sector Risk Management Agencies, shall—

(A) review the current framework for securing critical infrastructure, as described in section 652(c)(4) of this title and Presidential Policy Directive 21; and

(B) submit to the President and appropriate congressional committees a report that includes—

(i) information relating to—

(I) the analysis framework or methodology used to—

(aa) evaluate the current framework for securing critical infrastructure referred to in subparagraph (A); and

(bb) develop recommendations to—

(AA) revise the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) identify and designate any subsectors of such sectors;

(II) the data, metrics, and other information used to develop the recommendations required under clause (ii); and

(ii) recommendations relating to—

(I) revising—

(aa) the current framework for securing critical infrastructure referred to in subparagraph (A);

(bb) the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(cc) the identification and designation of any subsectors of such sectors; and

(II) any revisions to the list of designated Federal departments or agencies that serve as the Sector Risk Management Agency for a sector or subsector of such section, necessary to comply with paragraph (3)(B).

(2) Periodic evaluation by the Secretary

At least once every five years, the Secretary, in consultation with the Director and the heads of Sector Risk Management Agencies, shall—

(A) evaluate the current list of designated critical infrastructure sectors and subsectors of such sectors and the appropriateness of Sector Risk Management Agency designations, as set forth in Presidential Policy Directive 21, any successor or related document, or policy; and

(B) recommend, as appropriate, to the President—

(i) revisions to the current list of designated critical infrastructure sectors or subsectors of such sectors; and

(ii) revisions to the designation of any Federal department or agency designated as the Sector Risk Management Agency for a sector or subsector of such sector.

(3) Review and revision by the President

Not later than 180 days after the Secretary submits a recommendation pursuant to paragraph (1) or (2), the President shall—

(A) review the recommendation and revise, as appropriate, the designation of a critical infrastructure sector or subsector or the designation of a Sector Risk Management Agency; and

(B) submit to the appropriate congressional committees, the Majority and Minority Leaders of the Senate, and the Speaker and Minority Leader of the House of Representatives, a report that includes—

(i) an explanation with respect to the basis for accepting or rejecting the recommendations of the Secretary; and

(ii) information relating to the analysis framework, methodology, metrics, and data used to—

(I) evaluate the current framework for securing critical infrastructure referred to in paragraph (1)(A); and

(II) develop—

(aa) recommendations to revise—

(AA) the list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) the designation of any subsectors of such sectors; and

(bb) the recommendations of the Secretary.

(4) Publication

Any designation of critical infrastructure sectors shall be published in the Federal Register.

(c) Sector Risk Management Agencies

(1) Omitted

(2) Omitted

(3) References

Any reference to a Sector Specific Agency (including any permutations or conjugations thereof) in any law, regulation, map, document, record, or other paper of the United States shall be deemed to—

(A) be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector; and

(B) have the meaning given such term in section 650 of this title.

(4) Omitted

(d) Report and auditing

Not later than two years after January 1, 2021 and every four years thereafter for 12 years, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under section 665d of this title.

(Pub. L. 116–283, div. H, title XC, §9002, Jan. 1, 2021, 134 Stat. 4768; Pub. L. 117–263, div. G, title LXXI, §7143(d)(5), Dec. 23, 2022, 136 Stat. 3663.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Section is comprised of section 9002 of Pub. L. 116–283. Subsec. (c)(1) of section 9002 of Pub. L. 116–283 enacted section 665d of this title. Subsec. (c)(2) of section 9002 of Pub. L. 116–283 amended sections 195f, 321m, 651, 652, and 664 of this title. Subsec. (c)(4) of section 9002 of Pub. L. 116–283 amended the table of contents in section 1(b) of the Homeland Security Act of 2002.

AMENDMENTS

2022—Subsec. (a)(5). Pub. L. 117–263, §7143(d)(5)(A)(i), (ii), redesignated par. (6) as (5) and struck out former par. (5). Prior to amendment, text of par. (5) read as follows: "The term 'information sharing and analysis organization' has the meaning given that term in section 671(5) of this title."

Subsec. (a)(6), (7). Pub. L. 117–263, §7143(d)(5)(A)(ii), (iii), which redesignated par. (7) as (6) and then directed the general amendment of par. (7), was executed by making the redesignation and generally amending par. (6) as redesignated, to reflect the probable intent of Congress. As amended, such par. remained designated as (7). Prior to amendment, text of par. (7) read as follows: "The term 'sector risk management agency' has the meaning given the term 'Sector-Specific Agency' in section 651(5) of this title."

Subsec. (c)(3)(B). Pub. L. 117–263, §7143(d)(5)(B), which directed substitution of "given such term in section 650 of this title" for "given such term in section 651(5) of this title", was executed by making the substitution for "give such term in section 651(5) of this title", to reflect the probable intent of Congress.

Subsec. (d). Pub. L. 117–263, §7143(d)(5)(C), made technical amendment to reference in original act which appears in text as reference to section 665d of this title.

[1] *So in original. Probably should be "(6)".*

§653. Cybersecurity Division

(a) Establishment

(1) In general

There is established in the Agency a Cybersecurity Division.

(2) Executive Assistant Director

The Cybersecurity Division shall be headed by an Executive Assistant Director for Cybersecurity (in this section referred to as "the Executive Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department;

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) Reference

Any reference to the Assistant Secretary for Cybersecurity and Communications or Assistant Director for Cybersecurity in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Cybersecurity.

(b) Functions

The Executive Assistant Director shall—

(1) direct the cybersecurity efforts of the Agency;

(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44 and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(3) fully participate in the mechanisms required under section 652(c)(7) of this title; and

(4) carry out such other duties and powers as prescribed by the Director.

(Pub. L. 107–296, title XXII, §2203, as added Pub. L. 115–278, §2(a), Nov. 16, 2018, 132 Stat. 4174; amended Pub. L. 116–283, div. H, title XC, §9001(c)(1), Jan. 1, 2021, 134 Stat. 4766.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Cybersecurity Act of 2015, referred to in subsec. (b)(2), is div. N of Pub. L. 114–113, Dec. 18, 2015, 129 Stat. 2835. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

AMENDMENTS

2021—Subsec. (a)(2). Pub. L. 116–283, §9001(c)(1)(A)(i), in heading, substituted "Executive Assistant Director" for "Assistant Director" and, in introductory provisions, substituted "Executive Assistant Director for Cybersecurity" for "Assistant Director for Cybersecurity" and " 'the Executive Assistant Director' " for "the 'Assistant Director' ".

Subsec. (a)(3). Pub. L. 116–283, §9001(c)(1)(A)(ii), inserted "or Assistant Director for Cybersecurity" after "Assistant Secretary for Cybersecurity" and substituted "Executive Assistant Director for Cybersecurity." for "Assistant Director for Cybersecurity."

Subsec. (b). Pub. L. 116–283, §9001(c)(1)(B), substituted "Executive Assistant Director" for "Assistant Director" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CONTINUATION IN OFFICE

Pub. L. 116–283, div. H, title XC, §9001(c)(2), Jan. 1, 2021, 134 Stat. 4767, provided that: "The individual serving as the Assistant Director for Cybersecurity of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act [Jan. 1, 2021] may serve as the Executive Assistant Director for Cybersecurity on and after that date without the need for renomination or reappointment."

ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR FOR CYBERSECURITY

Pub. L. 115–278, §2(b)(3), Nov. 16, 2018, 132 Stat. 4175, provided that: "The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Cybersecurity on and after such date."

§654. Infrastructure Security Division

(a) Establishment

(1) In general

There is established in the Agency an Infrastructure Security Division.

(2) Executive Assistant Director

The Infrastructure Security Division shall be headed by an Executive Assistant Director for Infrastructure Security (in this section referred to as "the Executive Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department;

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) Reference

Any reference to the Assistant Secretary for Infrastructure Protection or Assistant Director for Infrastructure Security in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Infrastructure Security.

(b) Functions

The Executive Assistant Director shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards

Program established under subchapter XVI and the secure handling of ammonium nitrate program established under part J of subchapter VIII, or any successor programs;

(3) fully participate in the mechanisms required under section 652(c)(7) of this title; and

(4) carry out such other duties and powers as prescribed by the Director.

(Pub. L. 107–296, title XXII, §2204, as added Pub. L. 115–278, §2(a), Nov. 16, 2018, 132 Stat. 4174; amended Pub. L. 116–283, div. H, title XC, §9001(d)(1), Jan. 1, 2021, 134 Stat. 4767.)

EDITORIAL NOTES

AMENDMENTS

2021—Subsec. (a)(2). Pub. L. 116–283, §9001(d)(1)(A)(i), in heading, substituted "Executive Assistant Director" for "Assistant Director" and, in introductory provisions, substituted "Executive Assistant Director for Infrastructure Security" for "Assistant Director for Infrastructure Security" and "'the Executive Assistant Director' " for "the 'Assistant Director' ".

Subsec. (a)(3). Pub. L. 116–283, §9001(d)(1)(A)(ii), inserted "or Assistant Director for Infrastructure Security" after "Assistant Secretary for Infrastructure Protection" and substituted "Executive Assistant Director for Infrastructure Security." for "Assistant Director for Infrastructure Security."

Subsec. (b). Pub. L. 116–283, §9001(d)(1)(B), substituted "Executive Assistant Director" for "Assistant Director" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CONTINUATION IN OFFICE

Pub. L. 116–283, div. H, title XC, §9001(d)(2), Jan. 1, 2021, 134 Stat. 4767, provided that: "The individual serving as the Assistant Director for Infrastructure Security of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act [Jan. 1, 2021] may serve as the Executive Assistant Director for Infrastructure Security on and after that date without the need for renomination or reappointment."

ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY

Pub. L. 115–278, §2(b)(4), Nov. 16, 2018, 132 Stat. 4175, provided that: "The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Infrastructure Security on and after such date."

§655. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 652 of this title, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems;

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems; and

(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44.

(Pub. L. 107–296, title XXII, §2205, formerly title II, §223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, §2(e)(3)(A), Dec. 18,

2014, 128 Stat. 3086; renumbered title XXII, §2205, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(i), Nov. 16, 2018, 132 Stat. 4178, 4180; Pub. L. 117–263, div. G, title LXXI, §7143(c)(6), Dec. 23, 2022, 136 Stat. 3663.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 143 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Pub. L. 117–263 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security" in introductory provisions.

2018—Pub. L. 115–278, §2(g)(9)(A)(i)(I), substituted "section 652 of this title" for "section 121 of this title" and "Director of Cybersecurity and Infrastructure Security" for "Under Secretary appointed under section 113(a)(1)(H) of this title" in introductory provisions.

Par. (1)(B). Pub. L. 115–278, §2(g)(9)(A)(i)(II), struck out "and" at end.

2014—Pub. L. 113–283, §2(e)(3)(A)(i), (ii), inserted "Federal and" before "non-Federal" in section catchline and substituted "the Under Secretary appointed under section 113(a)(1)(H) of this title" for "the Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection" in introductory provisions.

Par. (3). Pub. L. 113–283, §2(e)(3)(A)(iii), (iv), added par. (3).

2007—Pub. L. 110–53 substituted "Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection" for "Under Secretary for Information Analysis and Infrastructure Protection" in introductory provisions.

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

§656. NET Guard

The Director of the Cybersecurity and Infrastructure Security Agency may establish a national technology guard, to be known as "NET Guard", comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

(Pub. L. 107–296, title XXII, §2206, formerly title II, §224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334; renumbered title XXII, §2206, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(ii), Nov. 16, 2018, 132 Stat. 4178, 4180; Pub. L. 117–263, div. G, title LXXI, §7143(c)(7), Dec. 23, 2022, 136 Stat. 3663.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 144 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Pub. L. 117–263 substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security".

2018—Pub. L. 115–278, §2(g)(9)(A)(ii), substituted "Director of Cybersecurity and Infrastructure Security" for "Assistant Secretary for Infrastructure Protection".

2007—Pub. L. 110–53 substituted "Assistant Secretary for Infrastructure Protection" for "Under Secretary for Information Analysis and Infrastructure Protection".

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

§657. Cyber Security Enhancement Act of 2002

(a) Short title

This section may be cited as the "Cyber Security Enhancement Act of 2002".

(b) Amendment of sentencing guidelines relating to certain computer crimes

(1) Directive to the United States Sentencing Commission

Pursuant to its authority under section 994(p) of title 28 and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18.

(2) Requirements

In carrying out this subsection, the Sentencing Commission shall—

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18.

(c) Study and report on computer crimes

Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18.

(d) Emergency disclosure exception

(1) Omitted

(2) Reporting of disclosures

A government entity that receives a disclosure under section 2702(b) of title 18 shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after November 25, 2002.

(Pub. L. 107–296, title XXII, §2207, formerly title II, §225, Nov. 25, 2002, 116 Stat. 2156; renumbered title XXII, §2207, Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 145 of this title prior to renumbering by Pub. L. 115–278.

Section is comprised of section 2207 of Pub. L. 107–296. Subsecs. (d)(1) and (e) to (j) of section 2207 of Pub. L. 107–296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

§658. Cybersecurity recruitment and retention

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term "appropriate committees of Congress" means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) Collective bargaining agreement

The term "collective bargaining agreement" has the meaning given that term in section 7103(a)(8) of title 5.

(3) Excepted service

The term "excepted service" has the meaning given that term in section 2103 of title 5.

(4) Preference eligible

The term "preference eligible" has the meaning given that term in section 2108 of title 5.

(5) Qualified position

The term "qualified position" means a position, designated by the Secretary for the purpose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

(6) Senior Executive Service

The term "Senior Executive Service" has the meaning given that term in section 2101a of title 5.

(b) General authority

(1) Establish positions, appoint personnel, and fix rates of pay

(A) General authority

The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

(I) senior level positions designated under section 5376 of title 5; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

(B) Construction with other laws

The authority of the Secretary under this subsection applies without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

(2) Basic pay

(A) Authority to fix rates of basic pay

In accordance with this section, the Secretary shall fix the rates of basic pay for any qualified position established under paragraph (1) in relation to the rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

(B) Prevailing rate systems

The Secretary may, consistent with section 5341 of title 5, adopt such provisions of that title as provide for prevailing rate systems of basic pay and may apply those provisions to qualified positions for employees in or under which the Department may employ individuals described by section 5342(a)(2)(A) of that title.

(3) Additional compensation, incentives, and allowances

(A) Additional compensation based on title 5 authorities

The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5.

(B) Allowances in nonforeign areas

An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) Plan for execution of authorities

Not later than 120 days after December 18, 2014, the Secretary shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

(5) Collective bargaining agreements

Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

(6) Required regulations

The Secretary, in coordination with the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

(c) Annual report

Not later than 1 year after December 18, 2014, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office within the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

(d) Three-year probationary period

The probationary period for all employees hired under the authority established in this section shall be 3 years.

(e) Incumbents of existing competitive service positions

(1) In general

An individual serving in a position on December 18, 2014, that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

(2) Subsequent conversion

After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

(f) Study and report

Not later than 120 days after December 18, 2014, the National Protection and Programs Directorate shall submit a report regarding the availability of, and benefits (including cost savings and security) of using, cybersecurity personnel and facilities outside of the National Capital Region (as defined in section 2674 of title 10) to serve the Federal and national need to—

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

(Pub. L. 107–296, title XXII, §2208, formerly title II, §226, as added Pub. L. 113–277, §3(a), Dec. 18, 2014, 128 Stat. 3005; renumbered title XXII, §2208, Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 147 of this title prior to renumbering by Pub. L. 115–278.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to National Protection and Programs Directorate of the Department of Homeland Security deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department, see section 652(a)(2) of this title, enacted Nov. 16, 2018.

§659. National cybersecurity and communications integration center

(a) Definition

The term "cybersecurity vulnerability" has the meaning given the term "security vulnerability" in section 650 of this title.

(b) Center

There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Director. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Executive Assistant Director for Cybersecurity.

(c) Functions

The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.];

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n), as appropriate; and

(C) sharing the analysis conducted under subparagraph (A) and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate, with Federal and non-Federal entities;

(6) upon request, providing operational and timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to

cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation, which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) share cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, mitigation protocols to counter cybersecurity vulnerabilities, as appropriate, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department;

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications;

(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices; and

(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 681 of this title) submitted by covered entities (as defined in section 681 of this title) and reports related to ransom payments (as defined in section 681 of this title) submitted by covered entities (as defined in section 681 of this title) in furtherance of the activities specified in sections 652(e), 653, and 681a of this title, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.

(d) Composition

(1) In general

The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community;

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) Information Sharing and Analysis Organizations, including information sharing and analysis centers;

(iii) owners and operators of critical information systems; and

(iv) private entities, including cybersecurity specialists;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector;

(E) an entity that collaborates with State and local governments, including an entity that collaborates with election officials, on cybersecurity risks and incidents, and has entered into a

voluntary information sharing relationship with the Center; and

(F) other appropriate representatives or entities, as determined by the Secretary.

(2) Incidents

In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) Principles

In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) Information Sharing and Analysis Organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(H) the Center designates an agency contact for non-Federal entities; and

(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015 [6 U.S.C. 1504].

(f) Cyber hunt and incident response teams

(1) In general

The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

(A) assistance to asset owners and operators in restoring services following a cyber incident;

(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

(C) mitigation strategies to prevent, deter, and protect against cybersecurity risks;

(D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as

appropriate; and

(E) such other capabilities as the Secretary determines appropriate.

(2) Associated metrics

The Center shall—

(A) define the goals and desired outcomes for each cyber hunt and incident response team; and

(B) develop metrics—

(i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A); and

(ii) that—

(I) are quantifiable and actionable; and

(II) the Center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response teams.

(3) Cybersecurity specialists

After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team.

(g) No right or benefit

(1) In general

The provision of assistance or information to, and inclusion in the Center, or any team or activity of the Center, of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Director.

(2) Certain assistance or information

The provision of certain assistance or information to, or inclusion in the Center, or any team or activity of the Center, of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(h) Automated information sharing

(1) In general

The Director, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.].

(2) Annual report

The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(i) Voluntary information sharing procedures

(1) Procedures

(A) In general

The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary

information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) National security

The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) Voluntary information sharing relationships

A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) Standard agreement

For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) Negotiated agreement

At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Director, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) Existing agreements

An agreement between the Center and a non-Federal entity that is entered into before December 18, 2015, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(j) Direct reporting

The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(k) Reports on international cooperation

Not later than 180 days after December 18, 2015, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(l) Outreach

Not later than 60 days after December 18, 2015, the Secretary, acting through the Director, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(m) Cybersecurity outreach

(1) In general

The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in

developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(2) Definitions

For purposes of this subsection, the terms "small business concern" and "small business development center" have the meaning given such terms, respectively, under section 632 of title 15.

(n) Coordinated vulnerability disclosure

The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(o) Protocols to counter certain cybersecurity vulnerabilities

The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.

(p) Subpoena authority

(1) Definition

In this subsection, the term "covered device or system"—

(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

(B) does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices.

(2) Authority

(A) In general

If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe such security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under subsection (c)(12).

(B) Limit on information

A subpoena issued pursuant to subparagraph (A) may seek information—

(i) only in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18; and

(ii) for not more than 20 covered devices or systems.

(C) Liability protections for disclosing providers

The provisions of section 2703(e) of title 18, shall apply to any subpoena issued pursuant to subparagraph (A).

(3) Coordination

(A) In general

If the Director exercises the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to interagency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after January 1, 2021.

(B) Contents

The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

(i) issued to carry out a function described in subsection (c)(12); and

(ii) subject to the limitations specified in this subsection.

(4) Noncompliance

If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued pursuant to this subsection, the Director may request that the Attorney General seek enforcement of such subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) Notice

Not later than seven days after the date on which the Director receives information obtained through a subpoena issued pursuant to this subsection, the Director shall notify any entity identified by information obtained pursuant to such subpoena regarding such subpoena and the identified vulnerability.

(6) Authentication

(A) In general

Any subpoena issued pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) Invalid if not authenticated

Any subpoena issued pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

(7) Procedures

Not later than 90 days after January 1, 2021, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued pursuant to this subsection, which shall address the following:

(A) The protection of and restriction on dissemination of nonpublic information obtained through such a subpoena, including a requirement that the Agency not disseminate nonpublic information obtained through such a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in accordance with paragraph (4), and may share with a Federal agency the nonpublic information of the entity at risk if—

(i) the Agency identifies or is notified of a cybersecurity incident involving such entity, which relates to the vulnerability which led to the issuance of such subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow such department or agency to take a law enforcement or national security action, consistent with the interagency procedures under paragraph (3)(A), or actions related to mitigating or otherwise resolving such incident;

(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests, consistent with such interagency procedures; and

(iv) the entity consents, except that the entity's consent shall not be required if another Federal department or agency identifies the entity to the Agency in connection with a suspected cybersecurity incident.

(B) The restriction on the use of information obtained through such a subpoena for a cybersecurity purpose.

(C) The retention and destruction of nonpublic information obtained through such a subpoena, including—

(i) destruction of such information that the Director determines is unrelated to critical infrastructure immediately upon providing notice to the entity pursuant to paragraph (5); and

(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through such a subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent.

(D) The processes for providing notice to each party that is subject to such a subpoena and each entity identified by information obtained under such a subpoena.

(E) The processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued pursuant to this subsection.

(F) The information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—

(i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and

(ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.

(8) Limitation on procedures

The internal procedures established pursuant to paragraph (7) may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to this chapter.

(9) Review of procedures

Not later than 1 year after January 1, 2021, the Privacy Officer of the Agency shall—

(A) review the internal procedures established pursuant to paragraph (7) to ensure that—

(i) such procedures are consistent with fair information practices; and

(ii) the operations of the Agency comply with such procedures; and

(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review under subparagraph (A).

(10) Publication of information

Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall publish information on the website of the Agency regarding the subpoena process under this subsection, including information regarding the following:

(A) Such internal procedures.

(B) The purpose for subpoenas issued pursuant to this subsection.

(C) The subpoena process.

(D) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.

(E) Policies and procedures on retention and sharing of data obtained by subpoenas.

(F) Guidelines on how entities contacted by the Director may respond to notice of a subpoena.

(11) Annual reports

The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas issued pursuant to this subsection, which shall include the following:

(A) A discussion of the following:

(i) The effectiveness of the use of such subpoenas to mitigate critical infrastructure security vulnerabilities.

(ii) The critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection.

(iii) The number of subpoenas so issued during the preceding year.

(iv) To the extent practicable, the number of vulnerable covered devices or systems mitigated under this subsection by the Agency during the preceding year.

(v) The number of entities notified by the Director under this subsection, and their responses, during the preceding year.

(B) For each subpoena issued pursuant to this subsection, the following:

(i) Information relating to the source of the security vulnerability detected, identified, or received by the Director.

(ii) Information relating to the steps taken to identify the entity at risk prior to issuing the subpoena.

(iii) A description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

(12) Publication of the annual reports

The Director shall publish a version of the annual report required under paragraph (11) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv), and (v) of subparagraph (A) of such paragraph.

(13) Prohibition on use of information for unauthorized purposes

Any information obtained pursuant to a subpoena issued under this subsection may not be provided to any other Federal department or agency for any purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.

(q) Industrial control systems

The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

(5) conduct such other efforts and assistance as the Secretary determines appropriate.

(r) Coordination on cybersecurity for SLTT entities

(1) [1] Coordination

The Center shall, upon request and to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

(A) conduct exercises with SLTT entities;

(B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

(i) cyber threat indicators;

(ii) defensive measures;

(iii) cybersecurity risks;
(iv) vulnerabilities; and
(v) incident response and management;

(C) in order to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable—
(i) cyber threat indicators;
(ii) defensive measures;
(iii) information about cybersecurity risks; and
(iv) information about incidents;

(D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;
(E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—
(i) information about tools;
(ii) information about products;
(iii) resources;
(iv) policies;
(v) guidelines;
(vi) controls; and
(vii) other cybersecurity standards and best practices and procedures related to information security, including, as appropriate, information produced by other Federal agencies;

(F) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;
(G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;
(H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and
(I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

(s) Report

Not later than 1 year after June 21, 2022, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the services and capabilities that the Agency directly and indirectly provides to SLTT entities.

(Pub. L. 107–296, title XXII, §2209, formerly title II, §227, formerly §226, as added Pub. L. 113–282, §3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered §227 and amended Pub. L. 114–113, div. N, title II, §§203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963; Pub. L. 114–328, div. A, title XVIII, §1841(b), Dec. 23, 2016, 130 Stat. 2663; renumbered title XXII, §2209, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(iii), Nov. 16, 2018, 132 Stat. 4178, 4180; Pub. L. 116–94, div. L, §102(a), Dec. 20, 2019, 133 Stat. 3089; Pub. L. 116–283, div. A, title XVII, §1716(a), Jan. 1, 2021, 134 Stat. 4094; Pub. L. 117–81, div. A, title XV, §§1541(a), 1542, 1548(c), Dec. 27, 2021, 135 Stat. 2054, 2056, 2063; Pub. L. 117–103, div. Y, §103(a)(1), Mar. 15, 2022, 136 Stat. 1038; Pub. L. 117–150, §2(2), June 21, 2022, 136 Stat. 1295; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(D), Dec. 23, 2022, 136 Stat. 3659.)

EDITORIAL NOTES

REFERENCES IN TEXT

Title I of the Cybersecurity Act of 2015, referred to in subsecs. (c)(1) and (h)(1), is title I of Pub. L. 114–113, div. N, Dec. 18, 2015, 129 Stat. 2936, also known as the Cybersecurity Information Sharing Act of 2015, which is classified generally to subchapter I of chapter 6 of this title. For complete classification of title I to the Code, see Short Title note set out under section 1501 of this title and Tables.

This chapter, referred to in subsec. (p)(8), was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out below and Tables.

CODIFICATION

Section was formerly classified to section 148 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7143(b)(2)(D)(i), added subsec. (a) and struck out former subsec. (a) which defined cybersecurity purpose, cybersecurity risk, cyber threat indicator, defensive measure, cybersecurity vulnerability, incident, information sharing and analysis organization, information system, security vulnerability, and sharing.

Subsec. (b). Pub. L. 117–263, §7143(b)(2)(D)(ii), inserted "Executive" before "Assistant Director for Cybersecurity".

Subsec. (c)(6). Pub. L. 117–150, §2(2)(A), inserted "operational and" before "timely".

Subsec. (c)(13). Pub. L. 117–103 added par. (13).

Subsec. (d)(1)(A)(iii). Pub. L. 117–263, §7143(b)(2)(D)(iii)(I), struck out ", as that term is defined under section 3003(4) of title 50" after "intelligence community".

Subsec. (d)(1)(B)(ii). Pub. L. 117–263, §7143(b)(2)(D)(iii)(II), substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations".

Subsec. (d)(1)(E). Pub. L. 117–150, §2(2)(B), inserted ", including an entity that collaborates with election officials," after "governments".

Subsec. (e)(1)(E)(ii)(II). Pub. L. 117–263, §7143(b)(2)(D)(iv), substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations".

Subsec. (p). Pub. L. 117–263, §7143(b)(2)(D)(v), redesignated subsec. (p) relating to coordination on cybersecurity for SLTT entities as (r).

Pub. L. 117–150, §2(2)(C), added subsec. (p) relating to coordination on cybersecurity for SLTT entities.

Subsec. (q). Pub. L. 117–263, §7143(b)(2)(D)(vi), redesignated subsec. (q) relating to report as (s).

Pub. L. 117–150, §2(2)(C), added subsec. (q) relating to report.

Subsec. (r). Pub. L. 117–263, §7143(b)(2)(D)(v), redesignated subsec. (p) relating to coordination on cybersecurity for SLTT entities as (r).

Subsec. (s). Pub. L. 117–263, §7143(b)(2)(D)(vi), redesignated subsec. (q) relating to report as (s).

2021—Subsec. (a). Pub. L. 117–81, §1542(1), added par. (4) and redesignated former pars. (4) to (8) (as previously added or redesignated by Pub. L. 116–283) as (5) to (9), respectively.

Pub. L. 116–283, §1716(a)(1), added pars. (1) and (7) and redesignated former pars. (1) to (5) as (2) to (6), respectively, and former par. (6) as (8).

Subsec. (c)(5)(B), (C). Pub. L. 117–81, §1542(2)(A), added subpar. (B), redesignated former subpar. (B) as (C), and inserted in subpar. (C) as redesignated "and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate," before "with Federal".

Subsec. (c)(6). Pub. L. 117–81, §1548(c), inserted ", which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions" after "mitigation, and remediation".

Subsec. (c)(7)(C). Pub. L. 117–81, §1542(2)(B), substituted "share" for "sharing".

Subsec. (c)(9). Pub. L. 117–81, §1542(2)(C), inserted "mitigation protocols to counter cybersecurity vulnerabilities, as appropriate," after "measures,".

Subsec. (c)(12). Pub. L. 116–283, §1716(a)(2), added par. (12).

Subsec. (e)(1)(I). Pub. L. 117–81, §1541(a)(1), added subpar. (I).

Subsec. (o). Pub. L. 117–81, §1542(4), added subsec. (o). Former subsec. (o) redesignated (p) relating to subpoena authority.

Pub. L. 116–283, §1716(a)(3), added subsec. (o).

Subsec. (p). Pub. L. 117–81, §1542(3), redesignated subsec. (o) as (p) relating to subpoena authority.

Subsec. (q). Pub. L. 117–81, §1541(a)(2), added subsec. (q) relating to industrial control systems.

2019—Subsec. (d)(1)(B)(iv). Pub. L. 116–94, §102(a)(1), inserted ", including cybersecurity specialists" after "entities".

Subsec. (f). Pub. L. 116–94, §102(a)(3), added subsec. (f). Former subsec. (f) redesignated (g).

Subsec. (g). Pub. L. 116–94, §102(a)(2), redesignated subsec. (f) as (g). Former subsec. (g) redesignated (h).

Subsec. (g)(1), (2). Pub. L. 116–94, §102(a)(4), inserted ", or any team or activity of the Center," after "Center".

Subsecs. (h) to (n). Pub. L. 116–94, §102(a)(2), redesignated subsecs. (g) to (m) as (h) to (n), respectively.

2018—Pub. L. 115–278, §2(g)(9)(A)(iii)(I), substituted "Director" for "Under Secretary appointed under section 113(a)(1)(H) of this title" wherever appearing.

Subsec. (a)(4). Pub. L. 115–278, §2(g)(9)(A)(iii)(II), substituted "section 671(5) of this title" for "section 131(5) of this title".

Subsec. (b). Pub. L. 115–278, §2(g)(9)(A)(iii)(III), inserted at end "The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity."

Subsec. (c)(11). Pub. L. 115–278, §2(g)(9)(A)(iii)(IV), substituted "Emergency Communications Division" for "Office of Emergency Communications".

2016—Subsecs. (l), (m). Pub. L. 114–328 added subsec. (l) and redesignated former subsec. (l) as (m).

2015—Subsec. (a)(1) to (5). Pub. L. 114–113, §203(1)(A), (B), added pars. (1) to (3), redesignated former pars. (3) and (4) as (4) and (5), respectively, and struck out former pars. (1) and (2), which defined "cybersecurity risk" and "incident", respectively.

Subsec. (a)(6). Pub. L. 114–113, §203(1)(C)–(E), added par. (6).

Subsec. (c)(1). Pub. L. 114–113, §203(2)(A), inserted "cyber threat indicators, defensive measures," before "cybersecurity risks" and ", including the implementation of title I of the Cybersecurity Act of 2015" before semicolon at end.

Subsec. (c)(3). Pub. L. 114–113, §203(2)(B), substituted "cyber threat indicators, defensive measures, cybersecurity risks," for "cybersecurity risks".

Subsec. (c)(5)(A). Pub. L. 114–113, §203(2)(C), substituted "cyber threat indicators, defensive measures, cybersecurity risks," for "cybersecurity risks".

Subsec. (c)(6). Pub. L. 114–113, §203(2)(D), substituted "cyber threat indicators, defensive measures, cybersecurity risks," for "cybersecurity risks" and struck out "and" at end.

Subsec. (c)(7)(C). Pub. L. 114–113, §203(2)(E), added subpar. (C).

Subsec. (c)(8) to (11). Pub. L. 114–113, §203(2)(F), added pars. (8) to (11).

Subsec. (d)(1)(B)(i). Pub. L. 114–113, §203(3)(A)(i), substituted ", local, and tribal" for "and local".

Subsec. (d)(1)(B)(ii). Pub. L. 114–113, §203(3)(A)(ii), substituted ", including information sharing and analysis centers;" for "; and".

Subsec. (d)(1)(B)(iv). Pub. L. 114–113, §203(3)(A)(iii), (iv), added cl. (iv).

Subsec. (d)(1)(E), (F). Pub. L. 114–113, §203(3)(B)–(D), added subpar. (E) and redesignated former subpar. (E) as (F).

Subsec. (e)(1)(A). Pub. L. 114–113, §203(4)(A)(i), inserted "cyber threat indicators, defensive measures, and" before "information".

Subsec. (e)(1)(B). Pub. L. 114–113, §203(4)(A)(ii), inserted "cyber threat indicators, defensive measures, and" before "information related".

Subsec. (e)(1)(F). Pub. L. 114–113, §203(4)(A)(iii), substituted "cyber threat indicators, defensive measures, cybersecurity risks," for "cybersecurity risks" and struck out "and" at end.

Subsec. (e)(1)(G). Pub. L. 114–113, §203(4)(A)(iv), substituted "cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and" for "cybersecurity risks and incidents".

Subsec. (e)(1)(H). Pub. L. 114–113, §203(4)(A)(v), added subpar. (H).

Subsec. (e)(2). Pub. L. 114–113, §203(4)(B), substituted "cyber threat indicators, defensive measures, cybersecurity risks," for "cybersecurity risks" and inserted "or disclosure" after "access".

Subsec. (e)(3). Pub. L. 114–113, §203(4)(C), inserted ", including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015" before period at end.

Subsecs. (g) to (l). Pub. L. 114–113, §203(5), added subsecs. (g) to (l).

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULES OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

Pub. L. 116–283, div. A, title XVII, §1716(b), Jan. 1, 2021, 134 Stat. 4098, provided that:

"(1) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this section or the amendments made by this section [amending this section] may be construed to grant the Secretary of Homeland Security, or the head of any another Federal agency or department, any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of the enactment of this Act [Jan. 1, 2021].

"(2) PRIVATE ENTITIES.—Nothing in this section or the amendments made by this section [amending this section] may be construed to require any private entity to—

"(A) request assistance from the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; or

"(B) implement any measure or recommendation suggested by the Director."

Pub. L. 113–282, §8, Dec. 18, 2014, 128 Stat. 3072, provided that:

"(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title] or the amendments made by this Act shall be construed to grant the Secretary [of Homeland Security] any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2014].

"(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

"(1) to request assistance from the Secretary; or

"(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary."

DEFINITIONS

Pub. L. 113–282, §2, Dec. 18, 2014, 128 Stat. 3066, provided that: "In this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title]—

"(1) the term 'Center' means the national cybersecurity and communications integration center under section 226 [renumbered 227 by section 223(a)(3) of Pub. L. 114–113 and renumbered 2209 by section 2(g)(2)(I) of Pub. L. 115–278] of the Homeland Security Act of 2002 [6 U.S.C. 659], as added by section 3;

"(2) the term 'critical infrastructure' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

"(3) the term 'cybersecurity risk' has the meaning given that term in section 226 [2209] of the Homeland Security Act of 2002, as added by section 3;

"(4) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5) [renumbered 2222(5) by section 2(g)(2)(H) of Pub. L. 115–278] of the Homeland Security Act of 2002 ([former] 6 U.S.C. 131(5)) [now 6 U.S.C. 671(5); see 6 U.S.C. 650(13)];

"(5) the term 'information system' has the meaning given that term in section 3502(8) of title 44, United States Code; and

"(6) the term 'Secretary' means the Secretary of Homeland Security."

[1] *So in original. There is no par. (2).*

§660. Cybersecurity plans

(a) Definitions

In this section, the term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency.

(b) Intrusion assessment plan

(1) Requirement

The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) Exception

The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) Cyber incident response plan

The Director of the Cybersecurity and Infrastructure Security Agency shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

(d) National Response Framework

The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(e) Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments

(1) In general

(A) Requirement

Not later than one year after December 27, 2021, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(B) Recommendations and requirements

The strategy required under subparagraph (A) shall provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents.

(2) Contents

The strategy required under paragraph (1) shall—

(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against,

detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

(i) incident exercises, information sharing and incident notification procedures;

(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40;

(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

(3) Considerations

In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, shall consider—

(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems owned or operated by State, local, Tribal, and territorial governments; and

(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies.

(4) Exemption

Chapter 35 of title 44 (commonly known as the "Paperwork Reduction Act") shall not apply to any action to implement this subsection.

(Pub. L. 107–296, title XXII, §2210, formerly title II, §228, as added and amended Pub. L. 114–113, div. N, title II, §§205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964; renumbered title XXII, §2210, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(iv), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–81, div. A, title XV, §§1545, 1546, Dec. 27, 2021, 135 Stat. 2057, 2059; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(E), (c)(8), Dec. 23, 2022, 136 Stat. 3660, 3663.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 149 of this title prior to renumbering by Pub. L. 115–278.

Former section 149 of this title, which was transferred and redesignated as subsec. (c) of this section by Pub. L. 114–113, div. N, title II, §223(a)(2), Dec. 18, 2015, 129 Stat. 2963, was based on Pub. L. 107–296, title II, §227, as added by Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7143(b)(2)(E)(i), substituted "section, the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency." for "section—" and struck out pars. (1) to (4) which defined agency information system, cybersecurity risk, information system, intelligence community, and national security system.

Subsec. (c). Pub. L. 117–263, §7143(c)(8), substituted "Director of the Cybersecurity and Infrastructure Security Agency" for "Director of Cybersecurity and Infrastructure Security".

Pub. L. 117–263, §7143(b)(2)(E)(ii), substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations (as defined in section 671(5) of this title)" and struck out "(as defined in section 659 of this title)" after "cybersecurity risks".

Subsec. (e)(1)(B). Pub. L. 117–263, §7143(b)(2)(E)(iii)(I), which directed striking out "(as such term is defined in section 659 of this title)", was executed by striking out "(as such term is defined in section 659 of this title)" after "cybersecurity risks" and after "incidents", to reflect the probable intent of Congress.

Subsec. (e)(3)(C). Pub. L. 117–263, §7143(b)(2)(E)(iii)(II), struck out "(as such term is defined in section 1501 of this title)" after "information systems".

2021—Subsec. (c). Pub. L. 117–81, §1546, substituted "update not less often than biennially" for "regularly update" and inserted "The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response." at end.

Subsec. (e). Pub. L. 117–81, §1545, added subsec. (e).

2018—Subsec. (a)(2). Pub. L. 115–278, §2(g)(9)(A)(iv)(I), substituted "section 659 of this title" for "section 148 of this title".

Subsec. (c). Pub. L. 115–278, §2(g)(9)(A)(iv), substituted "Director of Cybersecurity and Infrastructure Security" for "Under Secretary appointed under section 113(a)(1)(H) of this title", "section 671(5) of this title" for "section 131(5) of this title", and "section 659 of this title" for "section 148 of this title".

2015—Subsec. (c). Pub. L. 114–113, §223(a)(5), made technical amendment to reference in original act which appears in text as reference to section 148 of this title.

Pub. L. 114–113, §223(a)(2), transferred former section 149 of this title to subsec. (c) of this section. See Codification note above.

Subsec. (d). Pub. L. 114–113, §205, added subsec. (d).

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULES OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

Pub. L. 113–282, §7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: "Nothing in the amendment made by subsection (a) [enacting subsec. (c) of this section and section 150 of this title] or in subsection (b)(1) [formerly classified as a note under section 3543 of Title 44, Public Printing and Documents, see now section 2(d)(1) of Pub. L. 113–283, set out as a note under section 3553 of Title 44] shall be construed to alter any authority of a Federal agency or department."

§661. Cybersecurity strategy

(a) In general

Not later than 90 days after December 23, 2016, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

(b) Contents

The strategy required under subsection (a) shall include the following:

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs,

policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in section 659 of this title (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) Considerations

In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 347 of this title; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

(d) Implementation plan

Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) Congressional oversight

The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) Classified information

The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(g) Rule of construction

Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(Pub. L. 107–296, title XXII, §2211, formerly title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683; renumbered title XXII, §2211, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(v), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(F), Dec. 23, 2022, 136 Stat. 3660.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 149a of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (h). Pub. L. 117–263 struck out subsec. (h). Text read as follows: "In this section, the term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts."

2018—Subsec. (b)(2)(A). Pub. L. 115–278, §2(g)(9)(A)(v), substituted "section 659 of this title" for "the

section 148 of this title".

§662. Clearances

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; [1] relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(Pub. L. 107–296, title XXII, §2212, formerly title II, §229, formerly §228, as added Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered §229, Pub. L. 114–113, div. N, title II, §223(a)(1), Dec. 18, 2015, 129 Stat. 2963; renumbered title XXII, §2212, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(vi), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(G), Dec. 23, 2022, 136 Stat. 3660.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order 13549, referred to in text, is Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, which is set out as a note under section 3161 of Title 50, War and National Defense.

CODIFICATION

Section was formerly classified to section 150 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Pub. L. 117–263 substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations (as defined in section 671(5) of this title)".

2018—Pub. L. 115–278, §2(g)(9)(A)(vi), substituted "section 671(5) of this title" for "section 131(5) of this title".

[1] So in original. Probably should be "51609;".

§663. Federal intrusion detection and prevention system

(a) Definitions

In this section—

(1) the term "agency" has the meaning given the term in section 3502 of title 44;

(2) the term "agency information" means information collected or maintained by or on behalf of an agency; [1]

(3) the term "agency information system" has the meaning given the term in section 660 of this title; and [2]

(b) Requirement

(1) In general

Not later than 1 year after December 18, 2015, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) Regular improvement

The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) Activities

In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) Principles

In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) Private entities

(1) Conditions

A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than

to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) Limitation on liability

No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) Rule of construction

Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) Privacy Officer review

Not later than 1 year after December 18, 2015, the Privacy Officer appointed under section 142 of this title, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(Pub. L. 107–296, title XXII, §2213, formerly title II, §230, as added Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964; renumbered title XXII, §2213, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(vii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(H), Dec. 23, 2022, 136 Stat. 3660.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 208(b) of the E-Government Act of 2002, referred to in subsec. (c)(6), is section 208(b) of title II of Pub. L. 107–347, which is set out in a note under section 3501 of Title 44, Public Printing and Documents.

CODIFICATION

Section was formerly classified to section 151 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (a)(4). Pub. L. 117–263 struck out par. (4) which read as follows: "the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 659 of this title."

2018—Subsec. (a)(3). Pub. L. 115–278, §2(g)(9)(A)(vii)(I), substituted "section 660 of this title" for "section 149 of this title".

Subsec. (a)(4). Pub. L. 115–278, §2(g)(9)(A)(vii)(II), substituted "section 659 of this title" for "section 148 of this title".

STATUTORY NOTES AND RELATED SUBSIDIARIES

COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES

Pub. L. 117–81, div. A, title XV, §1544, Dec. 27, 2021, 135 Stat. 2057, provided that: "The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659]) to information systems (as such term is defined in such section 2209 [see 6 U.S.C. 650]) and industrial control systems, including supervisory control and data acquisition systems."

DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES

Pub. L. 115–390, title I, §101, Dec. 21, 2018, 132 Stat. 5173, provided that:

"(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a

policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

"(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

"(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

"(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

"(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

"(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

"(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

"(c) CONSULTATION.—

"(1) IN GENERAL.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

"(A) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) are protected from prosecution under section 1030 of title 18, United States Code, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

"(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

"(C) Non-governmental security researchers.

"(2) NONAPPLICABILITY OF FACA.—The Federal Advisory Committee Act ([former] 5 U.S.C. App.) [see 5 U.S.C. 1001 et seq.] shall not apply to any consultation under this section.

"(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

"(e) SUBMISSION TO CONGRESS.—

"(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act [Dec. 21, 2018], the Secretary of Homeland Security shall submit to the appropriate congressional committees a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

"(2) REPORT AND BRIEFING.—

"(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to the appropriate congressional committees a report on such policy and the remediation process required under subsection (b).

"(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to the appropriate congressional committees a briefing on the policy required under subsection (a) and the process required under subsection (b).

"(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (a) and the process required under subsection (b) for the period covered by the report or briefing, as the case may be:

"(i) The number of unique security vulnerabilities reported.

"(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

"(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

"(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

"(f) DEFINITIONS.—In this section:

"(1) The term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

"(2) The term 'information system' has the meaning given that term by section 3502 of title 44, United States Code.

"(3) The term 'appropriate information system' means an information system that the Secretary of

Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

"(4) The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives; and

"(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate."

DEPARTMENT OF HOMELAND SECURITY BUG BOUNTY PILOT PROGRAM

Pub. L. 115–390, title I, §102, Dec. 21, 2018, 132 Stat. 5175, provided that:

"(a) DEFINITIONS.—In this section:

"(1) The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(B) the Select Committee on Intelligence of the Senate;

"(C) the Committee on Homeland Security of the House of Representatives; and

"(D) Permanent Select Committee on Intelligence of the House of Representatives.

"(2) The term 'bug bounty program' means a program under which—

"(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

"(B) eligible individuals, organizations, and companies receive compensation in exchange for such reports.

"(3) The term 'Department' means the Department of Homeland Security.

"(4) The term 'eligible individual, organization, or company' means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

"(5) The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

"(6) The term 'pilot program' means the bug bounty pilot program required to be established under subsection (b)(1).

"(7) The term 'Secretary' means the Secretary of Homeland Security.

"(b) BUG BOUNTY PILOT PROGRAM.—

"(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act [Dec. 21, 2018], the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

"(2) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

"(A) designate appropriate information systems to be included in the pilot program;

"(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

"(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

"(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

"(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

"(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

"(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

"(3) CONTRACT AUTHORITY.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award 1 or more competitive contracts to an entity, as necessary, to manage the pilot program.

"(c) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

"(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

"(A) registered;

"(B) were determined eligible;

"(C) submitted security vulnerabilities; and

"(D) received compensation;

"(2) the number and severity of vulnerabilities reported as part of the pilot program;

"(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

"(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

"(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

"(6) the types of compensation provided under the pilot program; and

"(7) the lessons learned from the pilot program.

"(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Department $250,000 for fiscal year 2019 to carry out this section."

AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, §223(b), Dec. 18, 2015, 129 Stat. 2966, as amended by Pub. L. 115–278, §2(h)(1)(E), Nov. 16, 2018, 132 Stat. 4182, provided that:

"(1) IN GENERAL.—Except as provided in paragraph (2)—

"(A) not later than 1 year after the date of enactment of this Act [Dec. 18, 2015] or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

"(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 2213(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(2)], the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

"(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

"(3) DEFINITION.—Notwithstanding section 222 [6 U.S.C. 1521], in this subsection, the term 'agency information system' means an information system owned or operated by an agency.

"(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines."

[1] So in original. Probably should be followed by "and".

[2] So in original. The "; and" probably should be a period.

§664. National asset database

(a) Establishment

(1) National asset database

The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United

States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) Prioritized critical infrastructure list

In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) Use of database

The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) Maintenance of database

(1) In general

The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) Organization of information in database

The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7; and

(B) by the State and county of their location.

(3) Private sector integration

The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) Retention of classification

The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a Sector Risk Management Agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) Reports

(1) Report required

Not later than 180 days after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) Contents of report

Each such report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on such list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on such list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on such list or in such database.

(E) If appropriate, the extent to which such database and such list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any other information the Secretary deems relevant.

(3) Classified information

The report shall be submitted in unclassified form but may contain a classified annex.

(e) National Infrastructure Protection Consortium

The Secretary may establish a consortium to be known as the "National Infrastructure Protection Consortium". The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

(Pub. L. 107–296, title XXII, §2214, formerly title II, §210E, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372; renumbered title XXII, §2214, and amended Pub. L. 115–278, §2(g)(2)(G), (9)(A)(viii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 116–283, div. H, title XC, §9002(c)(2)(E), Jan. 1, 2021, 134 Stat. 4773.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 124l of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2021—Subsec. (c)(4). Pub. L. 116–283 substituted "Sector Risk Management Agency" for "sector-specific agency".

2018—Subsecs. (e), (f). Pub. L. 115–278, §2(g)(9)(A)(viii), redesignated subsec. (f) as (e) and struck out former subsec. (e). Prior to amendment, text of subsec. (e) read as follows: "By not later than two years after August 3, 2007, the Inspector General of the Department shall conduct a study of the implementation of this section."

§665. Duties and authorities relating to .gov internet domain

(a) Definition

In this section, the term "agency" has the meaning given the term in section 3502 of title 44.

(b) Availability of .gov internet domain

The Director shall make .gov internet domain name registration services, as well as any supporting services described in subsection (e), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (c);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (c); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(c) Requirements

The Director, with the approval of the Director of the Office of Management and Budget for agency .gov internet domain requirements and in consultation with the Director of the Office of Management and Budget for .gov internet domain requirements for entities that are not agencies, shall establish and publish on a publicly available website requirements for the registration and operation of .gov internet domains sufficient to—

(1) minimize the risk of .gov internet domains whose names could mislead or confuse users;

(2) establish that .gov internet domains may not be used for commercial or political campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the .gov internet domain with any other Department component or any other agency for any purpose other than the administration of the .gov internet domain, the services described in subsection (e), and the requirements for establishing a .gov inventory described in subsection (h).

(d) Executive branch

(1) In general

The Director of the Office of Management and Budget shall establish applicable processes and guidelines for the registration and acceptable use of .gov internet domains by agencies.

(2) Approval required

The Director shall obtain the approval of the Director of the Office of Management and Budget before registering a .gov internet domain name for an agency.

(3) Compliance

Each agency shall ensure that any website or digital service of the agency that uses a .gov internet domain is in compliance with the 21st Century IDEA Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

(e) Supporting services

(1) In general

The Director may provide services to the entities described in subsection (b)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered .gov internet domains.

(2) Rule of construction

Nothing in paragraph (1) shall be construed to—

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (b)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of .gov internet domains and the needs of .gov internet domain registrants.

(f) Fees

(1) In general

The Director may provide any service relating to the availability of the .gov internet domain program, including .gov internet domain name registration services described in subsection (b) and supporting services described in subsection (e), to entities described in subsection (b)(1) with or without reimbursement, including variable pricing.

(2) Limitation

The total fees collected for new .gov internet domain registrants or annual renewals of .gov internet domains shall not exceed the direct operational expenses of improving, maintaining, and operating the .gov internet domain, .gov internet domain services, and .gov internet domain supporting services.

(g) Consultation

The Director shall consult with the Director of the Office of Management and Budget, the Administrator of General Services, other civilian Federal agencies as appropriate, and entities representing State, local, Tribal, or territorial governments in developing the strategic direction of the .gov internet domain and in establishing requirements under subsection (c), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(h) .gov inventory

(1) In general

The Director shall, on a continuous basis—

(A) inventory all hostnames and services in active use within the .gov internet domain; and

(B) provide the data described in subparagraph (A) to domain registrants at no cost.

(2) Requirements

In carrying out paragraph (1)—

(A) data may be collected through analysis of public and non-public sources, including commercial data sets;

(B) the Director shall share with Federal and non-Federal domain registrants all unique hostnames and services discovered within the zone of their registered domain;

(C) the Director shall share any data or information collected or used in the management of the .gov internet domain name registration services relating to Federal executive branch registrants with the Director of the Office of Management and Budget for the purpose of fulfilling the duties of the Director of the Office of Management and Budget under section 3553 of title 44;

(D) the Director shall publish on a publicly available website discovered hostnames that describe publicly accessible agency websites, to the extent consistent with the security of Federal information systems but with the presumption of disclosure;

(E) the Director may publish on a publicly available website any analysis conducted and data collected relating to compliance with Federal mandates and industry best practices, to the extent consistent with the security of Federal information systems but with the presumption of disclosure; and

(F) the Director shall—

(i) collect information on the use of non-.gov internet domain suffixes by agencies for their official online services;

(ii) collect information on the use of non-.gov internet domain suffixes by State, local, Tribal, and territorial governments; and

(iii) publish the information collected under clause (i) on a publicly available website to the extent consistent with the security of the Federal information systems, but with the presumption of disclosure.

(3) National security coordination

(A) In general

In carrying out this subsection, the Director shall inventory, collect, and publish hostnames and services in a manner consistent with the protection of national security information.

(B) Limitation

The Director may not inventory, collect, or publish hostnames or services under this subsection if the Director, in coordination with other heads of agencies, as appropriate, determines that the collection or publication would—

(i) disrupt a law enforcement investigation;

(ii) endanger national security or intelligence activities;

(iii) impede national defense activities or military operations; or

(iv) hamper security remediation actions.

(4) Strategy

Not later than 180 days after December 27, 2020, the Director shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives a strategy to utilize the information collected under this subsection for countering malicious cyber activity.

(Pub. L. 107–296, title XXII, §2215, as added Pub. L. 116–260, div. U, title IX, §904(b)(1)(B), Dec. 27, 2020, 134 Stat. 2298; Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(ii), (B), Dec. 27, 2021, 135 Stat. 2060, 2061; Pub. L. 117–263, div. G, title LXXI, §7143(a)(1), Dec. 23, 2022, 136 Stat. 3654.)

EDITORIAL NOTES

REFERENCES IN TEXT

The 21st Century IDEA Act, referred to in subsec. (d)(3), is Pub. L. 115–336, Dec. 20, 2018, 132 Stat. 5025, also known as the 21st Century Integrated Digital Experience Act, which is set out as a note under section 3501 of Title 44, Public Printing and Documents.

CODIFICATION

Other sections 2215 of Pub. L. 107–296 were renumbered sections 2216, 2217, and 2218 and are classified, respectively, to sections 665b, 665c, and 665d of this title.

AMENDMENTS

2022—Pub. L. 117–263 made amendment identical to that made by Pub. L. 117–81, §1547(b)(1)(B). See 2021 Amendment note below.

2021—Pub. L. 117–81, §1547(b)(1)(B), made technical amendment to the directory language of section 904(b)(1) of Pub. L. 116–260.

Pub. L. 117–81, §1547(b)(1)(A)(ii), reenacted section catchline.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress,

Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

EFFECTIVE DATE OF 2022 AMENDMENT

Amendment by Pub. L. 117–263 effective as if enacted as part of title IX of div. U of Pub. L. 116–260, see section 7143(a)(2) of Pub. L. 117–263, set out as a note under section 652 of this title.

FINDINGS

Pub. L. 116–260, div. U, title IX, §902, Dec. 27, 2020, 134 Stat. 2297, provided that: "Congress finds that—

"(1) the .gov internet domain reflects the work of United States innovators in inventing the internet and the role that the Federal Government played in guiding the development and success of the early internet;

"(2) the .gov internet domain is a unique resource of the United States that reflects the history of innovation and global leadership of the United States;

"(3) when online public services and official communications from any level and branch of government use the .gov internet domain, they are easily recognized as official and difficult to impersonate;

"(4) the citizens of the United States deserve online public services that are safe, recognizable, and trustworthy;

"(5) the .gov internet domain should be available at no cost or a negligible cost to any Federal, State, local, or territorial government-operated or publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, for use in their official services, operations, and communications;

"(6) the .gov internet domain provides a critical service to those Federal, State, local, Tribal, and territorial governments; and

"(7) the .gov internet domain should be operated transparently and in the spirit of public accessibility, privacy, and security."

[For definition of "State" as used in section 902 of Pub. L. 116–260, set out above, see section 903 of Pub. L. 116–260, set out as a note below.]

PURPOSE OF .GOV INTERNET DOMAIN PROGRAM

Pub. L. 116–260, div. U, title IX, §904(a), Dec. 27, 2020, 134 Stat. 2298, provided that: "The purpose of the .gov internet domain program is to—

"(1) legitimize and enhance public trust in government entities and their online services;

"(2) facilitate trusted electronic communication and connections to and from government entities;

"(3) provide simple and secure registration of .gov internet domains;

"(4) improve the security of the services hosted within these .gov internet domains, and of the .gov namespace in general; and

"(5) enable the discoverability of government services to the public and to domain registrants."

[For definition of "online service" as used in section 904(a) of Pub. L. 116–260, set out above, see section 903 of Pub. L. 116–260, set out as a note below.]

REFERENCE GUIDE

Pub. L. 116–260, div. U, title IX, §904(b)(2)(B), Dec. 27, 2020, 134 Stat. 2301, provided that: "Not later than 1 year after the date of enactment of this Act [Dec. 27, 2020], the Director, in consultation with the Administrator and entities representing State, local, Tribal, or territorial governments, shall develop and publish on a publicly available website a reference guide for migrating online services to the .gov internet domain, which shall include—

"(i) process and technical information on how to carry out a migration of common categories of online services, such as web and email services;

"(ii) best practices for cybersecurity pertaining to registration and operation of a .gov internet domain; and

"(iii) references to contract vehicles and other private sector resources vetted by the Director that may assist in performing the migration."

[For definitions of terms used in section 904(b)(2)(B) of Pub. L. 116–260, set out above, see section 903 of Pub. L. 116–260, set out as a note below.]

TRANSITION

Pub. L. 116–260, div. U, title IX, §907, Dec. 27, 2020, 134 Stat. 2303, provided that:

"(a) There shall be transferred to the Director the .gov internet domain program, as operated by the General Services Administration under title 41, Code of Federal Regulations, on the date on which the Director begins operational administration of the .gov internet domain program, in accordance with subsection (c).

"(b) Not later than 30 days after the date of enactment of this Act [probably means "this title", approved Dec. 27, 2020], the Director shall submit a plan for the operational and contractual transition of the .gov internet domain program to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform [now Committee on Oversight and Accountability], and the Committee on House Administration of the House of Representatives.

"(c) Not later than 120 days after the date of enactment of this Act, the Director shall begin operationally administering the .gov internet domain program, and shall publish on a publicly available website the requirements for domain registrants as described in section 2215(b) of the Homeland Security Act of 2002 [6 U.S.C. 665(b)], as added by section 904(b) of this Act.

"(d) On the date on which the Director begins operational administration of the .gov internet domain program, in accordance with subsection (c), the Administrator shall rescind the requirements in part 102–173 of title 41, Code of Federal Regulations.

"(e) During the 5-year period beginning on the date of enactment of this Act [Dec. 27, 2020], any fee charged to entities that are not agencies for new .gov internet domain registrants or annual renewals of .gov internet domains shall be not more than the amount of the fee charged for such registration or renewal as of October 1, 2019."

[For definition of "Director" as used in section 907 of Pub. L. 116–260, set out above, see section 903 of Pub. L. 116–260, set out as a note below.]

DEFINITIONS

Pub. L. 116–260, div. U, title IX, §903, Dec. 27, 2020, 134 Stat. 2298, provided that: "In this Act [probably means "this title", see Short Title of 2020 Amendment note set out under section 101 of this title]—

"(1) the term 'Administrator' means the Administrator of General Services;

"(2) the term 'agency' has the meaning given the term in section 3502 of title 44, United States Code;

"(3) the term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency;

"(4) the term 'online service' means any internet-facing service, including a website, email, a virtual private network, or a custom application; and

"(5) the term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States."

§665a. Intelligence and cybersecurity diversity fellowship program

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term "appropriate committees of Congress" means—

(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) Excepted service

The term "excepted service" has the meaning given that term in section 2103 of title 5.

(3) Historically Black college or university

The term "historically Black college or university" has the meaning given the term "part B institution" in section 1061 of title 20.

(4) Institution of higher education

The term "institution of higher education" has the meaning given that term in section 1001 of title 20.

(5) Minority-serving institution

The term "minority-serving institution" means an institution of higher education described in section 1067q(a) of title 20.

(b) Program

The Secretary shall carry out an intelligence and cybersecurity diversity fellowship program (in this section referred to as the "Program") under which an eligible individual may—

(1) participate in a paid internship at the Department that relates to intelligence, cybersecurity, or some combination thereof;

(2) receive tuition assistance from the Secretary; and

(3) upon graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), receive an offer of employment to work in an intelligence or cybersecurity position of the Department that is in the excepted service.

(c) Eligibility

To be eligible to participate in the Program, an individual shall—

(1) be a citizen of the United States; and

(2) as of the date of submitting the application to participate in the Program—

(A) have a cumulative grade point average of at least 3.2 on a 4.0 scale;

(B) be a socially disadvantaged individual (as that term in [1] defined in section 124.103 of title 13, Code of Federal Regulations, or successor regulation); and

(C) be a sophomore, junior, or senior at an institution of higher education.

(d) Direct hire authority

If an individual who receives an offer of employment under subsection (b)(3) accepts such offer, the Secretary shall appoint, without regard to provisions of subchapter I of chapter 33 of title 5 (except for section 3328 of such title) such individual to the position specified in such offer.

(e) Reports

(1) Reports

Not later than 1 year after December 27, 2020, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program.

(2) Matters

Each report under paragraph (1) shall include, with respect to the most recent year, the following:

(A) A description of outreach efforts by the Secretary to raise awareness of the Program among institutions of higher education in which eligible individuals are enrolled.

(B) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(C) The number of individuals participating in the Program, listed by the institution of higher education in which the individual is enrolled at the time of participation, and information on the nature of such participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(D) The number of individuals who accepted an offer of employment under the Program and an identification of the element within the Department to which each individual was appointed.

(Pub. L. 107–296, title XIII, §1333, as added Pub. L. 116–260, div. W, title IV, §404(a), Dec. 27, 2020, 134 Stat. 2378.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of title XIII of Pub. L. 107–296, and not as part of title XXII of 107–296 which comprises this subchapter.

[1] *So in original. Probably should be "is".*

§665b. Joint cyber planning office

(a) Establishment of Office

There is established in the Agency an office for joint cyber planning (in this section referred to as the "Office") to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) Planning and execution

In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

(1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;

(2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;

(3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(4) ensure that plans for cyber defense operations, as appropriate, are responsive to potential adversary activity conducted in response to United States offensive cyber operations;

(5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

(7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) Composition

The Office shall be composed of—

(1) a central planning staff; and

(2) appropriate representatives of Federal departments and agencies, including—

(A) the Department;

(B) United States Cyber Command;

(C) the National Security Agency;

(D) the Federal Bureau of Investigation;

(E) the Department of Justice; and

(F) the Office of the Director of National Intelligence.

(d) Consultation

In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

(1) State, local, federally-recognized Tribal, and territorial governments;

(2) Information Sharing and Analysis Organizations, including information sharing and analysis

centers;

(3) owners and operators of critical information systems;

(4) private entities; and

(5) other appropriate representatives or entities, as determined by the Secretary.

(e) Interagency agreements

The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) Definitions

In this section, the term "cyber defense operation" means the defensive activities performed for a cybersecurity purpose.

(Pub. L. 107–296, title XXII, §2216, formerly §2215, as added Pub. L. 116–283, div. A, title XVII, §1715(a), Jan. 1, 2021, 134 Stat. 4092; renumbered §2216 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(iii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(I), Dec. 23, 2022, 136 Stat. 3660.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 2216 of Pub. L. 107–296 was renumbered section 2219 and is classified to section 665e of this title.

AMENDMENTS

2022—Subsec. (d)(2). Pub. L. 117–263, §7143(b)(2)(I)(i), substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations".

Subsec. (f). Pub. L. 117–263, §7143(b)(2)(I)(ii), substituted "section, the term 'cyber defense operation' means the defensive activities performed for a cybersecurity purpose." for "section:" and struck out pars. (1) to (4) which defined cyber defense operation, cybersecurity purpose, cybersecurity risk, incident, and information sharing and analysis organization.

2021—Pub. L. 117–81 reenacted section catchline.

§665c. Cybersecurity State Coordinator

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity

incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(c) Feedback

The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(Pub. L. 107–296, title XXII, §2217, formerly §2215, as added Pub. L. 116–283, div. A, title XVII, §1717(a)(1)(B), Jan. 1, 2021, 134 Stat. 4099; renumbered §2217 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(iv), Dec. 27, 2021, 135 Stat. 2061.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 2217 of Pub. L. 107–296 was renumbered section 2220 and is classified to section 665f of this title.

AMENDMENTS

2021—Pub. L. 117–81 reenacted section catchline.

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Pub. L. 116–283, div. A, title XVII, §1717(a)(4), Jan. 1, 2021, 134 Stat. 4100, provided that: "Nothing in this subsection [enacting this section, amending section 652 of this title, and enacting provisions set out as a note below] or the amendments made by this subsection may be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents."

COORDINATION PLAN

Pub. L. 116–283, div. A, title XVII, §1717(a)(2), Jan. 1, 2021, 134 Stat. 4100, provided that: "Not later than 60 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall establish and submit to the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security in the House of Representatives a plan describing the reporting structure and coordination processes and procedures of Cybersecurity State Coordinators within the Cybersecurity and Infrastructure Security Agency under section 2215 of the Homeland Security Act of 2002 [Pub. L. 107–296], as added by paragraph (1)(B) [6 U.S.C. 665c]."

§665d. Sector Risk Management Agencies

(a) In general

Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

(1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and

(2) support programs and associated activities of such sector or subsector of such sector.

(b) Implementation

In carrying out this section, Sector Risk Management Agencies shall—

(1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

(2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

(3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(c) Responsibilities

Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of such sector and authorities under applicable law to—

(1) support sector risk management, in coordination with the Director, including—

(A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

(B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

(2) assess sector risk, in coordination with the Director, including—

(A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

(B) supporting national risk assessment efforts led by the Department;

(3) sector coordination, including—

(A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

(B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

(C) participating in cross-sector coordinating councils, as appropriate;

(4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

(A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through Information Sharing and Analysis Organizations and the national cybersecurity and communications integration center established pursuant to section 659 of this title;

(B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(5) supporting incident management, including—

(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

(6) contributing to emergency preparedness efforts, including—

(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

(B) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and

(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.

(Pub. L. 107–296, title XXII, §2218, formerly §2215, as added Pub. L. 116–283, div. H, title XC, §9002(c)(1), Jan. 1, 2021, 134 Stat. 4770; renumbered §2218 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(v), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(J), Dec. 23, 2022, 136 Stat. 3660.)

EDITORIAL NOTES

PRIOR PROVISIONS

A prior section 2218 of Pub. L. 107–296 was renumbered section 2220A and is classified to section 665g of this title.

AMENDMENTS

2022—Subsec. (c)(4)(A). Pub. L. 117–263 substituted "Information Sharing and Analysis Organizations" for "information sharing and analysis organizations".

2021—Pub. L. 117–81 reenacted section catchline.

§665e. Cybersecurity Advisory Committee

(a) Establishment

The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the "Advisory Committee").

(b) Duties

(1) In general

The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) Recommendations

(A) In general

The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) Recommendations of subcommittees

Recommendations agreed upon by subcommittees established under subsection (d) for any

year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) Periodic reports

The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) Annual report

(A) In general

The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) Publication

Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5.

(5) Feedback

Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) Congressional notification

Not less frequently than once per year after January 1, 2021, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) Governance rules

The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) Membership

(1) Appointment

(A) In general

Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020,[1] the Director shall appoint the members of the Advisory Committee.

(B) Composition

The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) Representation

(i) In general

The membership of the Advisory Committee shall satisfy the following criteria:

(I) Consist of subject matter experts.

(II) Be geographically balanced.

(III) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(aa) Defense.
(bb) Education.
(cc) Financial services and insurance.
(dd) Healthcare.
(ee) Manufacturing.
(ff) Media and entertainment.
(gg) Chemicals.
(hh) Retail.
(ii) Transportation.
(jj) Energy.
(kk) Information Technology.
(ll) Communications.
(mm) Other relevant fields identified by the Director.

(ii) Prohibition

Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) Publication of membership list

The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) Term of office

(A) Terms

The term of each member of the Advisory Committee shall be two years, except that a member may continue to serve until a successor is appointed.

(B) Removal

The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

(C) Reappointment

A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) Prohibition on compensation

The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) Meetings

(A) In general

The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) Public meetings

At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) Attendance

The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) Member access to classified information

(A) In general

Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted

from reviewing, discussing, or possessing classified information.

(B) Access

Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) Protections

A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) Rule of construction

Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) Chairperson

The Advisory Committee shall select, from among the members of the Advisory Committee—

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) Subcommittees

(1) In general

The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

(2) Meetings and reporting

Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) Subject matter experts

The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

(Pub. L. 107–296, title XXII, §2219, formerly §2216, as added Pub. L. 116–283, div. A, title XVII, §1718(a), Jan. 1, 2021, 134 Stat. 4102; renumbered §2219 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(vi), Dec. 27, 2021, 135 Stat. 2061.)

EDITORIAL NOTES

REFERENCES IN TEXT

The date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, referred to in subsec. (c)(1)(A), probably means the date of enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116–283, which was approved Jan. 1, 2021. No act named the Cybersecurity Advisory Committee Authorization Act of 2020 has been enacted. However, a bill, S. 4024, entitled "Cybersecurity Advisory Committee Authorization Act of 2020" was introduced to Senate on June 22, 2020.

Executive Order No. 13526, referred to in subsec. (c)(5)(B), is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, set out as a note under section 3161 of Title 50, War and National Defense.

AMENDMENTS

2021—Pub. L. 117–81 reenacted section catchline.

[1] *See References in Text note below.*

§665f. Cybersecurity education and training programs

(a) Establishment

(1) In general

The Cybersecurity Education and Training Assistance Program (referred to in this section as "CETAP") is established within the Agency.

(2) Purpose

The purpose of CETAP shall be to support the effort of the Agency in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

(A) providing foundational cybersecurity awareness and literacy;

(B) encouraging cybersecurity career exploration; and

(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) Requirements

In carrying out CETAP, the Director shall—

(1) ensure that the program—

(A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

(D) provides direct student engagement opportunities through camps and other programming;

(E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(F) integrates with existing post-secondary education and workforce development programs at the Department;

(G) promotes and supports national standards for elementary and secondary cyber education;

(H) partners with cybersecurity and education stakeholder groups to expand outreach; and

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

(2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) Briefings

(1) In general

Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) Contents

Each briefing conducted under paragraph (1) shall include—

(A) estimated figures on the number of students reached and teachers engaged;

(B) information on outreach and engagement efforts, including the activities described in

subsection (b)(1)(E);

(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;

(D) information on new curricula offerings and teacher training platforms; and

(E) information on coordination with post-secondary education and workforce development programs at the Department.

(d) Mission promotion

The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

(e) Grants and cooperative agreements

The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 1001 of title 20), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

(1) carry out the purposes of CETAP; and

(2) enhance CETAP to address the national shortfall of cybersecurity professionals.

(Pub. L. 107–296, title XXII, §2220, formerly §2217, as added Pub. L. 116–283, div. A, title XVII, §1719(c), Jan. 1, 2021, 134 Stat. 4106; renumbered §2220 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(vii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, §7104, Dec. 23, 2022, 136 Stat. 3622.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (c)(2)(C) to (E). Pub. L. 117–263, §7104(b), added subpar. (C) and redesignated former subpars. (C) and (D) as (D) and (E), respectively.

Subsec. (e). Pub. L. 117–263, §7104(a), added subsec. (e).

2021—Pub. L. 117–81 reenacted section catchline.

§665g. State and Local Cybersecurity Grant Program

(a) Definitions

In this section:

(1) Cybersecurity Plan

The term "Cybersecurity Plan" means a plan submitted by an eligible entity under subsection (e)(1).

(2) Eligible entity

The term "eligible entity" means a—

(A) State; or

(B) Tribal government.

(3) Multi-entity group

The term "multi-entity group" means a group of 2 or more eligible entities desiring a grant under this section.

(4) Online service

The term "online service" means any internet-facing service, including a website, email, virtual private network, or custom application.

(5) Rural area

The term "rural area" has the meaning given the term in section 5302 of title 49.

(6) State and Local Cybersecurity Grant Program

The term "State and Local Cybersecurity Grant Program" means the program established under subsection (b).

(7) Tribal government

The term "Tribal government" means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 5131 of title 25.

(b) Establishment

(1) In general

There is established within the Department a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments.

(2) Application

An eligible entity desiring a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(c) Administration

The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 604 and 605 of this title.

(d) Use of funds

An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate, shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity;

(3) pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;

(4) assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or

(5) fund any other appropriate activity determined by the Secretary, acting through the Director.

(e) Cybersecurity plans

(1) In general

An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for review in accordance with subsection (i).

(2) Required elements

A Cybersecurity Plan of an eligible entity shall—

(A) incorporate, to the extent practicable—

(i) any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments; and

(ii) if the eligible entity is a State, consultation and feedback from local governments and associations of local governments within the jurisdiction of the eligible entity;

(B) describe, to the extent practicable, how the eligible entity will—

(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

(ii) monitor, audit, and,[1] track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(iii) enhance the preparation, response, and resiliency of information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, against cybersecurity risks and cybersecurity threats;

(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(v) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, such as—

(I) the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

(II) cyber chain supply chain risk management best practices identified by the National Institute of Standards and Technology; and

(III) knowledge bases of adversary tools and tactics;

(vi) promote the delivery of safe, recognizable, and trustworthy online services by the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including through the use of the .gov internet domain;

(vii) ensure continuity of operations of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident;

(viii) use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

(ix) if the eligible entity is a State, ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local governments within the jurisdiction of the eligible entity in the event of an incident involving those communications or data networks;

(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and—

(I) if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including by expanding information sharing agreements with the Department; and

(II) the Department;

(xii) leverage cybersecurity services offered by the Department;

(xiii) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats in consultation with—

(I) if the eligible entity is a State, local governments and associations of local governments within the jurisdiction of the eligible entity; and

(II) as applicable—

(aa) eligible entities that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an Information Sharing and Analysis Organization; and

(bb) countries that neighbor the jurisdiction of the eligible entity;

(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the jurisdiction of the eligible entity; and

(xvi) distribute funds, items, services, capabilities, or activities to local governments under subsection (n)(2)(A), including the fraction of that distribution the eligible entity plans to distribute to rural areas under subsection (n)(2)(B);

(C) assess the capabilities of the eligible entity relating to the actions described in subparagraph (B);

(D) describe, as appropriate and to the extent practicable, the individual responsibilities of the eligible entity and local governments within the jurisdiction of the eligible entity in implementing the plan;

(E) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(F) describe the metrics the eligible entity will use to measure progress towards—

(i) implementing the plan; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(3) Discretionary elements

In drafting a Cybersecurity Plan, an eligible entity may—

(A) consult with the Multi-State Information Sharing and Analysis Center;

(B) include a description of cooperative programs developed by groups of local governments within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

(C) include a description of programs provided by the eligible entity to support local governments and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

(f) Multi-entity grants

(1) In general

The Secretary may award grants under this section to a multi-entity group to support multi-entity efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities that comprise the multi-entity group.

(2) Satisfaction of other requirements

In order to be eligible for a multi-entity grant under this subsection, each eligible entity that comprises a multi-entity group shall have—

(A) a Cybersecurity Plan that has been reviewed by the Secretary in accordance with subsection (i); and

(B) a cybersecurity planning committee established in accordance with subsection (g).

(3) Application

(A) In general

A multi-entity group applying for a multi-entity grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) Multi-entity project plan

An application for a grant under this section of a multi-entity group under subparagraph (A) shall include a plan describing—

(i) the division of responsibilities among the eligible entities that comprise the multi-entity group;

(ii) the distribution of funding from the grant among the eligible entities that comprise the multi-entity group; and

(iii) how the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) Planning committees

(1) In general

An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

(A) assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(B) approve the Cybersecurity Plan of the eligible entity; and

(C) assist with the determination of effective funding priorities for a grant under this section in accordance with subsections (d) and (j).

(2) Composition

A committee of an eligible entity established under paragraph (1) shall—

(A) be comprised of representatives from—

(i) the eligible entity;

(ii) if the eligible entity is a State, counties, cities, and towns within the jurisdiction of the eligible entity; and

(iii) institutions of public education and health within the jurisdiction of the eligible entity; and

(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(3) Cybersecurity expertise

Not less than one-half of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

(4) Rule of construction regarding existing planning committees

Nothing in this subsection shall be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that—

(A) meets the requirements of this subsection; or

(B) may be expanded or leveraged to meet the requirements of this subsection, including

through the formation of a cybersecurity planning subcommittee.

(5) Rule of construction regarding control of information systems of eligible entities

Nothing in this subsection shall be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems owned or operated by, or on behalf of, the eligible entity.

(h) Special rule for Tribal governments

With respect to any requirement under subsection (e) or (g), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe an alternative substantively similar requirement for Tribal governments if the Secretary finds that the alternative requirement is necessary for the effective delivery and administration of grants to Tribal governments under this section.

(i) Review of plans

(1) Review as condition of grant

(A) In general

Subject to paragraph (3), before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall—

(i) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and

(ii) determine that the Cybersecurity Plan reviewed under clause (i) satisfies the requirements under paragraph (2).

(B) Duration of determination

In the case of a determination under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the 2-year period beginning on the date of the determination.

(C) Annual renewal

Not later than 2 years after the date on which the Secretary determines under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), and annually thereafter, the Secretary, acting through the Director, shall—

(i) determine whether the Cybersecurity Plan and any revisions continue to meet the criteria described in paragraph (2); and

(ii) renew the determination if the Secretary, acting through the Director, makes a positive determination under clause (i).

(2) Plan requirements

In reviewing a Cybersecurity Plan of an eligible entity under this subsection, the Secretary, acting through the Director, shall ensure that the Cybersecurity Plan—

(A) satisfies the requirements of subsection (e)(2); and

(B) has been approved by—

(i) the cybersecurity planning committee of the eligible entity established under subsection (g); and

(ii) the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity.

(3) Exception

Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary for review before September 30, 2023, if the eligible entity certifies to the Secretary that—

(A) the activities that will be supported by the grant are—

(i) integral to the development of the Cybersecurity Plan of the eligible entity; or

(ii) necessary to assist with activities described in subsection (d)(4), as confirmed by the Director; and

(B) the eligible entity will submit to the Secretary a Cybersecurity Plan for review under this subsection by September 30, 2023.

(4) Rule of construction

Nothing in this subsection shall be construed to provide authority to the Secretary to—

(A) regulate the manner by which an eligible entity or local government improves the cybersecurity of the information systems owned or operated by, or on behalf of, the eligible entity or local government; or

(B) condition the receipt of grants under this section on—

(i) participation in a particular Federal program; or

(ii) the use of a specific product or technology.

(j) Limitations on uses of funds

(1) In general

Any entity that receives funds from a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any recipient cost-sharing contribution;

(C) to pay a ransom;

(D) for recreational or social purposes; or

(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

(2) Compliance oversight

In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this section uses the grant for the purposes for which the grant is awarded.

(3) Rule of construction

Nothing in paragraph (1)(A) shall be construed to prohibit the use of funds from a grant under this section awarded to a State, local, or Tribal government for otherwise permissible uses under this section on the basis that the State, local, or Tribal government has previously used State, local, or Tribal funds to support the same or similar uses.

(k) Opportunity to amend applications

In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct any defects in those applications before making final awards, including by allowing applicants to revise a submitted Cybersecurity Plan.

(l) Apportionment

For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among eligible entities as follows:

(1) Baseline amount

The Secretary shall first apportion—

(A) 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands;

(B) 1 percent of such amounts to each of the remaining States; and

(C) 3 percent of such amounts to Tribal governments.

(2) Remainder

The Secretary shall apportion the remainder of such amounts to States as follows:

(A) 50 percent of such remainder in the ratio that the population of each State, bears to the

population of all States; and

(B) 50 percent of such remainder in the ratio that the population of each State that resides in rural areas, bears to the population of all States that resides in rural areas.

(3) Apportionment among Tribal governments

In determining how to apportion amounts to Tribal governments under paragraph (1)(C), the Secretary shall consult with the Secretary of the Interior and Tribal governments.

(4) Multi-entity grants

An amount received from a multi-entity grant awarded under subsection (f)(1) by a State or Tribal government that is a member of the multi-entity group shall qualify as an apportionment for the purpose of this subsection.

(m) Federal share

(1) In general

The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

(A) in the case of a grant to an eligible entity—

(i) for fiscal year 2022, 90 percent;

(ii) for fiscal year 2023, 80 percent;

(iii) for fiscal year 2024, 70 percent; and

(iv) for fiscal year 2025, 60 percent; and

(B) in the case of a grant to a multi-entity group—

(i) for fiscal year 2022, 100 percent;

(ii) for fiscal year 2023, 90 percent;

(iii) for fiscal year 2024, 80 percent; and

(iv) for fiscal year 2025, 70 percent.

(2) Waiver

(A) In general

The Secretary may waive or modify the requirements of paragraph (1) if an eligible entity or multi-entity group demonstrates economic hardship.

(B) Guidelines

The Secretary shall establish and publish guidelines for determining what constitutes economic hardship for the purposes of this subsection.

(C) Considerations

In developing guidelines under subparagraph (B), the Secretary shall consider, with respect to the jurisdiction of an eligible entity—

(i) changes in rates of unemployment in the jurisdiction from previous years;

(ii) changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) from previous years; and

(iii) any other factors the Secretary considers appropriate.

(3) Waiver for Tribal governments

Notwithstanding paragraph (2), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may waive or modify the requirements of paragraph (1) for 1 or more Tribal governments if the Secretary determines that the waiver is in the public interest.

(n) Responsibilities of grantees

(1) Certification

Each eligible entity or multi-entity group that receives a grant under this section shall certify to

the Secretary that the grant will be used—

(A) for the purpose for which the grant is awarded; and

(B) in compliance with subsections (d) and (j).

(2) Availability of funds to local governments and rural areas

(A) In general

Subject to subparagraph (C), not later than 45 days after the date on which an eligible entity or multi-entity group receives a grant under this section, the eligible entity or multi-entity group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local governments within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multi-entity group—

(i) not less than 80 percent of funds available under the grant;

(ii) with the consent of the local governments, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

(iii) with the consent of the local governments, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

(B) Availability to rural areas

In obligating funds, items, services, capabilities, or activities to local governments under subparagraph (A), the eligible entity or eligible entities that comprise the multi-entity group shall ensure that rural areas within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group receive not less than—

(i) 25 percent of the amount of the grant awarded to the eligible entity;

(ii) items, services, capabilities, or activities having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or

(iii) grant funds combined with other items, services, capabilities, or activities having the total value of not less than 25 percent of the grant awarded to the eligible entity.

(C) Exceptions

This paragraph shall not apply to—

(i) any grant awarded under this section that solely supports activities that are integral to the development or revision of the Cybersecurity Plan of the eligible entity; or

(ii) the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

(3) Certifications regarding distribution of grant funds to local governments

An eligible entity or multi-entity group shall certify to the Secretary that the eligible entity or multi-entity group has made the distribution to local governments required under paragraph (2).

(4) Extension of period

(A) In general

An eligible entity or multi-entity group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

(B) Approval

The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

(5) Direct funding

If an eligible entity does not make a distribution to a local government required under paragraph

(2) in a timely fashion, the local government may petition the Secretary to request the Secretary to provide funds directly to the local government.

(6) Limitation on construction

A grant awarded under this section may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities.

(7) Consultation in allocating funds

An eligible entity applying for a grant under this section shall agree to consult the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity in allocating funds from a grant awarded under this section.

(8) Penalties

In addition to other remedies available to the Secretary, if an eligible entity violates a requirement of this subsection, the Secretary may—

(A) terminate or reduce the amount of a grant awarded under this section to the eligible entity; or

(B) distribute grant funds previously awarded to the eligible entity—

(i) in the case of an eligible entity that is a State, directly to the appropriate local government as a replacement grant in an amount determined by the Secretary; or

(ii) in the case of an eligible entity that is a Tribal government, to another Tribal government or Tribal governments as a replacement grant in an amount determined by the Secretary.

(o) Consultation with State, local, and Tribal representatives

In carrying out this section, the Secretary shall consult with State, local, and Tribal representatives with professional experience relating to cybersecurity, including representatives of associations representing State, local, and Tribal governments, to inform—

(1) guidance for applicants for grants under this section, including guidance for Cybersecurity Plans;

(2) the study of risk-based formulas required under subsection (q)(4);

(3) the development of guidelines required under subsection (m)(2)(B); and

(4) any modifications described in subsection (q)(2)(D).

(p) Notification to Congress

Not later than 3 business days before the date on which the Department announces the award of a grant to an eligible entity under this section, including an announcement to the eligible entity, the Secretary shall provide to the appropriate congressional committees notice of the announcement.

(q) Reports, study, and review

(1) Annual reports by grant recipients

(A) In general

Not later than 1 year after the date on which an eligible entity receives a grant under this section for the purpose of implementing the Cybersecurity Plan of the eligible entity, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in—

(i) implementing the Cybersecurity Plan of the eligible entity; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(B) Absence of plan

Not later than 1 year after the date on which an eligible entity that does not have a Cybersecurity Plan receives funds under this section, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to—

(i) develop or revise a Cybersecurity Plan; or

(ii) assist with the activities described in subsection (d)(4).

(2) Annual reports to Congress

Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

(A) the use of grants awarded under this section;

(B) the proportion of grants used to support cybersecurity in rural areas;

(C) the effectiveness of the State and Local Cybersecurity Grant Program;

(D) any necessary modifications to the State and Local Cybersecurity Grant Program; and

(E) any progress made toward—

(i) developing, implementing, or revising Cybersecurity Plans; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, State, local, or Tribal governments as a result of the award of grants under this section.

(3) Public availability

(A) In general

The Secretary, acting through the Director, shall make each report submitted under paragraph (2) publicly available, including by making each report available on the website of the Agency.

(B) Redactions

In making each report publicly available under subparagraph (A), the Director may make redactions that the Director, in consultation with each eligible entity, determines necessary to protect classified or other information exempt from disclosure under section 552 of title 5 (commonly referred to as the "Freedom of Information Act").

(4) Study of risk-based formulas

(A) In general

Not later than September 30, 2024, the Secretary, acting through the Director, shall submit to the appropriate congressional committees a study and legislative recommendations on the potential use of a risk-based formula for apportioning funds under this section, including—

(i) potential components that could be included in a risk-based formula, including the potential impact of those components on support for rural areas under this section;

(ii) potential sources of data and information necessary for the implementation of a risk-based formula;

(iii) any obstacles to implementing a risk-based formula, including obstacles that require a legislative solution;

(iv) if a risk-based formula were to be implemented for fiscal year 2026, a recommended risk-based formula for the State and Local Cybersecurity Grant Program; and

(v) any other information that the Secretary, acting through the Director, determines necessary to help Congress understand the progress towards, and obstacles to, implementing a risk-based formula.

(B) Inapplicability of Paperwork Reduction Act

The requirements of chapter 35 of title 44 (commonly referred to as the "Paperwork Reduction Act"), shall not apply to any action taken to carry out this paragraph.

(5) Tribal cybersecurity needs report

Not later than 2 years after November 15, 2021, the Secretary, acting through the Director, shall submit to Congress a report that—

(A) describes the cybersecurity needs of Tribal governments, which shall be determined in consultation with the Secretary of the Interior and Tribal governments; and

(B) includes any recommendations for addressing the cybersecurity needs of Tribal governments, including any necessary modifications to the State and Local Cybersecurity Grant Program to better serve Tribal governments.

(6) GAO review

Not later than 3 years after November 15, 2021, the Comptroller General of the United States shall conduct a review of the State and Local Cybersecurity Grant Program, including—

(A) the grant selection process of the Secretary; and

(B) a sample of grants awarded under this section.

(r) Authorization of appropriations

(1) In general

There are authorized to be appropriated for activities under this section—

(A) for fiscal year 2022, $200,000,000;

(B) for fiscal year 2023, $400,000,000;

(C) for fiscal year 2024, $300,000,000; and

(D) for fiscal year 2025, $100,000,000.

(2) Transfers authorized

(A) In general

During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to paragraph (1) or other amounts appropriated to carry out the State and Local Cybersecurity Grant Program for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.

(B) Additional appropriations

Any funds transferred under subparagraph (A) shall be in addition to any funds appropriated to the Department or the components described in subparagraph (A) for salaries, expenses, and other administrative costs.

(s) Termination

(1) In general

Subject to paragraph (2), the requirements of this section shall terminate on September 30, 2026.

(2) Exception

The reporting requirements under subsection (q) shall terminate on the date that is 1 year after the date on which the final funds from a grant under this section are expended or returned.

(Pub. L. 107–296, title XXII, §2220A, formerly §2218, as added Pub. L. 117–58, div. G, title VI, §70612(a), Nov. 15, 2021, 135 Stat. 1272; renumbered §2220A and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(viii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(K), Dec. 23, 2022, 136 Stat. 3660; Pub. L. 119–75, div. I, §5009, Feb. 3, 2026, 140 Stat. 630.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Food and Nutrition Act of 2008, referred to in subsec. (m)(2)(C)(ii), is Pub. L. 88–525, Aug. 31, 1964,

78 Stat. 703, which is classified generally to chapter 51 (§2011 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 7 and Tables.

AMENDMENTS

2026—Subsec. (s)(1). Pub. L. 119–75 substituted "September 30, 2026" for "September 30, 2025".

2022—Subsec. (a). Pub. L. 117–263, §7143(b)(2)(K)(i), redesignated pars. (3), (4), and (8) to (12) as (1) to (7), respectively, and struck out former pars. (1), (2), and (5) to (7) which defined appropriate committees of Congress, cyber threat indicator, incident, information sharing and analysis organization, and information system, respectively.

Subsec. (e)(2)(B)(xiv)(II)(aa). Pub. L. 117–263, §7143(b)(2)(K)(ii), substituted "Information Sharing and Analysis Organization" for "information sharing and analysis organization".

Subsec. (p). Pub. L. 117–263, §7143(b)(2)(K)(iii), substituted "appropriate congressional committees" for "appropriate committees of Congress".

Subsec. (q)(4)(A). Pub. L. 117–263, §7143(b)(2)(K)(iv), which directed amendment of subsec. (q)(4) by substituting "appropriate congressional committees" for "appropriate committees of Congress" "in the matter preceding clause (i)", was executed by making the substitution in the introductory provisions of subsec. (q)(4)(A), to reflect the probable intent of Congress.

2021—Pub. L. 117–81 reenacted section catchline.

[1] So in original. The comma probably should not appear.

§665h. National Cyber Exercise Program

(a) Establishment of program

(1) In general

There is established in the Agency the National Cyber Exercise Program (referred to in this section as the "Exercise Program") to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) Requirements

(A) In general

The Exercise Program shall be—

(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(B) Model exercise selection

The Exercise Program shall—

(i) include a selection of model exercises that government and private entities can readily adapt for use; and

(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) Consultation

In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

(b) Definitions

In this section:

(1) State

The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) Private entity

The term "private entity" has the meaning given such term in section 1501 of this title.

(c) Rule of construction

Nothing in this section shall be construed to affect the authorities or responsibilities of the Administrator of the Federal Emergency Management Agency pursuant to section 748 of this title.

(Pub. L. 107–296, title XXII, §2220B, as added Pub. L. 117–81, div. A, title XV, §1547(a), Dec. 27, 2021, 135 Stat. 2059.)

§665i. CyberSentry program

(a) Establishment

There is established in the Agency a program, to be known as "CyberSentry", to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, upon request and subject to the consent of such owner or operator.

(b) Activities

The Director, through CyberSentry, shall—

(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such owner or operator;

(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such vulnerabilities;

(4) produce aggregated, anonymized analytic products, based on threat hunting and continuous monitoring and detection activities and partnerships, with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022.

(c) Privacy review

Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency under section 652(h) of this title shall—

(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

(2) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report certifying compliance with all applicable privacy laws as referred to in paragraph (1), or identifying any instances of noncompliance with such privacy laws.

(d) Report to Congress

Not later than one year after December 27, 2021, the Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing and written report on implementation of this section.

(e) Savings

Nothing in this section may be construed to permit the Federal Government to gain access to information of a remote computing service provider to the public or an electronic service provider to the public, the disclosure of which is not permitted under section 2702 of title 18.

(f) Definition

In this section, the term "industrial control system" means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (DCSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

(g) Termination

The authority to carry out a program under this section shall terminate on the date that is seven years after December 27, 2021.

(Pub. L. 107–296, title XXII, §2220C, as added Pub. L. 117–81, div. A, title XV, §1548(a), Dec. 27, 2021, 135 Stat. 2061; amended Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(L), Dec. 23, 2022, 136 Stat. 3661.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1501 of the National Defense Authorization Act for Fiscal Year 2022, referred to in subsec. (b)(5), is section 1501 of Pub. L. 117–81, div. A, title XV, Dec. 27, 2021, 135 Stat. 2020, related to development of taxonomy of cyber capabilities, which is not classified to the Code.

CODIFICATION

Section 1548(a) of Pub. L. 117–81, which directed that this section be added at the end of title XXII of the Homeland Security Act of 2002, was executed by adding this section at the end of this part as if the directory language had added the section at the end of subtitle A of title XXII of the Act, to reflect the probable intent of Congress.

AMENDMENTS

2022—Subsec. (f). Pub. L. 117–263 added subsec. (f) and struck out former subsec. (f) which defined cybersecurity risk, industrial control system, and information system.

§665j. Ransomware threat mitigation activities

(a) Joint Ransomware Task Force

(1) In general

Not later than 180 days after March 15, 2022, the Director, in consultation with the National

Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) Composition

The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) Responsibilities

The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify [1] metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

(b) Rule of construction

Nothing in this section shall be construed to provide any additional authority to any Federal agency.

(Pub. L. 117–103, div. Y, §106, Mar. 15, 2022, 136 Stat. 1056.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

Pub. L. 117–103, div. Y, §102, Mar. 15, 2022, 136 Stat. 1038, provided that: "In this division [see Short Title of 2022 Amendment note set out under section 101 of this title]:

"(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms 'covered cyber incident', 'covered entity', 'cyber incident', 'information system', 'ransom payment', 'ransomware attack', and 'security vulnerability' have the meanings given those terms in section 2240 of the Homeland Security Act of 2002 [6 U.S.C. 681], as added by section 103 of this division [see also 6 U.S.C. 650].

"(2) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure

Security Agency."

[1] *So in original.*

§665k. Federal Clearinghouse on School Safety Evidence-based Practices

(a) Establishment

(1) In general

The Secretary, in coordination with the Secretary of Education, the Attorney General, and the Secretary of Health and Human Services, shall establish a Federal Clearinghouse on School Safety Evidence-based Practices (in this section referred to as the "Clearinghouse") within the Department.

(2) Purpose

The Clearinghouse shall serve as a Federal resource to identify and publish online through SchoolSafety.gov, or any successor website, evidence-based practices and recommendations to improve school safety for use by State and local educational agencies, institutions of higher education, State and local law enforcement agencies, health professionals, and the general public.

(3) Personnel

(A) Assignments

The Clearinghouse shall be assigned such personnel and resources as the Secretary considers appropriate to carry out this section.

(B) Detailees

The Secretary of Education, the Attorney General, and the Secretary of Health and Human Services may detail personnel to the Clearinghouse.

(4) Exemptions

(A) Paperwork Reduction Act

Chapter 35 of title 44 (commonly known as the "Paperwork Reduction Act"), shall not apply to any rulemaking or information collection required under this section.

(B) Federal Advisory Committee Act

The Federal Advisory Committee Act (5 U.S.C. App.) [1] shall not apply for the purposes of carrying out this section.

(b) Clearinghouse contents

(1) Consultation

In identifying the evidence-based practices and recommendations for the Clearinghouse, the Secretary shall—

(A) consult with appropriate Federal, State, local, Tribal, private sector, and nongovernmental organizations, including civil rights and disability rights organizations; and

(B) consult with the Secretary of Education to ensure that evidence-based practices published by the Clearinghouse are aligned with evidence-based practices to support a positive and safe learning environment for all students.

(2) Criteria for evidence-based practices and recommendations

The evidence-based practices and recommendations of the Clearinghouse shall—

(A) include comprehensive evidence-based school safety measures;

(B) include the evidence or research rationale supporting the determination of the Clearinghouse that the evidence-based practice or recommendation under subparagraph (A) has been shown to have a significant effect on improving the health, safety, and welfare of persons

in school settings, including—

(i) relevant research that is evidence-based, as defined in section 7801 of title 20, supporting the evidence-based practice or recommendation;

(ii) findings and data from previous Federal or State commissions recommending improvements to the safety posture of a school; or

(iii) other supportive evidence or findings relied upon by the Clearinghouse in determining evidence-based practices and recommendations, as determined in consultation with the officers described in subsection (a)(3)(B);

(C) include information on Federal programs for which implementation of each evidence-based practice or recommendation is an eligible use for the program;

(D) be consistent with Federal civil rights laws, including title II of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.); and

(E) include options for developmentally appropriate recommendations for use in educational settings with respect to children's ages and physical, social, sensory, and emotionally developmental statuses.

(3) Past commission recommendations

The Clearinghouse shall present, as determined in consultation with the officers described in subsection (a)(3)(B), Federal, State, local, Tribal, private sector, and nongovernmental organization issued best practices and recommendations and identify any best practice or recommendation of the Clearinghouse that was previously issued by any such organization or commission.

(c) Assistance and training

The Secretary may produce and publish materials on the Clearinghouse to assist and train educational agencies and law enforcement agencies on the implementation of the evidence-based practices and recommendations.

(d) Continuous improvement

The Secretary shall—

(1) collect for the purpose of continuous improvement of the Clearinghouse—

(A) Clearinghouse data analytics;

(B) user feedback on the implementation of resources, evidence-based practices, and recommendations identified by the Clearinghouse; and

(C) any evaluations conducted on implementation of the evidence-based practices and recommendations of the Clearinghouse; and

(2) in coordination with the Secretary of Education, the Secretary of Health and Human Services, and the Attorney General—

(A) regularly assess and identify Clearinghouse evidence-based practices and recommendations for which there are no resources available through Federal Government programs for implementation; and

(B) establish an external advisory board, which shall be comprised of appropriate State, local, Tribal, private sector, and nongovernmental organizations, including organizations representing parents of elementary and secondary school students, representative [2] from civil rights organizations, representatives of disability rights organizations, representatives of educators, representatives of law enforcement, and nonprofit school safety and security organizations, to—

(i) provide feedback on the implementation of evidence-based practices and recommendations of the Clearinghouse; and

(ii) propose additional recommendations for evidence-based practices for inclusion in the Clearinghouse that meet the requirements described in subsection (b)(2)(B).

(e) Parental assistance

The Clearinghouse shall produce materials in accessible formats to assist parents and legal guardians of students with identifying relevant Clearinghouse resources related to supporting the implementation of Clearinghouse evidence-based practices and recommendations.

(Pub. L. 107–296, title XXII, §2220D, as added Pub. L. 117–159, div. A, title III, §13302(a), June 25, 2022, 136 Stat. 1334.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (a)(4)(B), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

The Americans with Disabilities Act of 1990, referred to in subsec. (b)(2)(D), is Pub. L. 101–336, July 26, 1990, 104 Stat. 327. Title II of the Act is classified generally to subchapter II (§12131 et seq.) of chapter 126 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 12101 of Title 42 and Tables.

The Rehabilitation Act of 1973, referred to in subsec. (b)(2)(D), is Pub. L. 93–112, Sept. 26, 1973, 87 Stat. 355, which is classified generally to chapter 16 (§701 et seq.) of Title 29, Labor. For complete classification of this Act to the Code, see Short Title note set out under section 701 of Title 29 and Tables.

The Civil Rights Act of 1964, referred to in subsec. (b)(2)(D), is Pub. L. 88–352, July 2, 1964, 78 Stat. 241. Title VI of the Act is classified generally to subchapter V (§2000d et seq.) of chapter 21 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 2000a of Title 42 and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

LUKE AND ALEX SCHOOL SAFETY ACT OF 2022

Pub. L. 117–159, div. A, title III, subtitle C, June 25, 2022, 136 Stat. 1334, provided that:

"SEC. 13301. SHORT TITLE.

"This subtitle may be cited as the 'Luke and Alex School Safety Act of 2022'.

"SEC. 13302. FEDERAL CLEARINGHOUSE ON SCHOOL SAFETY EVIDENCE-BASED PRACTICES.

"(a) IN GENERAL.—[Enacted this section.]

"(b) TECHNICAL AMENDMENTS.—[Amended table of contents of the Homeland Security Act of 2002.]

"SEC. 13303. NOTIFICATION OF CLEARINGHOUSE.

"(a) NOTIFICATION BY THE SECRETARY OF EDUCATION.—The Secretary of Education shall provide written notification of the publication of the Federal Clearinghouse on School Safety Evidence-based Practices (referred to in this section and section 13304 as the 'Clearinghouse'), as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

"(1) every State and local educational agency; and

"(2) other Department of Education partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Education.

"(b) NOTIFICATION BY THE SECRETARY OF HOMELAND SECURITY.—The Secretary of Homeland Security shall provide written notification of the publication of the Clearinghouse, as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

"(1) every State homeland security advisor;

"(2) every State department of homeland security; and

"(3) other Department of Homeland Security partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Homeland Security.

"(c) NOTIFICATION BY THE SECRETARY OF HEALTH AND HUMAN SERVICES.—The Secretary of Health and Human Services shall provide written notification of the publication of the Clearinghouse, as

required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

"(1) every State department of public health; and

"(2) other Department of Health and Human Services partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Health and Human Services.

"(d) NOTIFICATION BY THE ATTORNEY GENERAL.—The Attorney General shall provide written notification of the publication of the Clearinghouse, as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

"(1) every State department of justice; and

"(2) other Department of Justice partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Attorney General.

"SEC. 13304. GRANT PROGRAM REVIEW.

"(a) FEDERAL GRANTS AND RESOURCES.—Not later than 1 year after the date of enactment of this Act [June 25, 2022], the Clearinghouse or the external advisory board established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by this subtitle, shall—

"(1) review grant programs and identify any grant program that may be used to implement evidence-based practices and recommendations of the Clearinghouse;

"(2) identify any evidence-based practices and recommendations of the Clearinghouse for which there is not a Federal grant program that may be used for the purposes of implementing the evidence-based practice or recommendation as applicable to the agency; and

"(3) periodically report any findings under paragraph (2) to the appropriate committees of Congress.

"(b) STATE GRANTS AND RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—

"(1) each agency responsible for school safety in the State, or any State that does not have such an agency designated;

"(2) any grant program that may be used for the purposes of implementing evidence-based practices and recommendations of the Clearinghouse; and

"(3) any resources other than grant programs that may be used to assist in implementation of evidence-based practices and recommendations of the Clearinghouse.

"SEC. 13305. RULES OF CONSTRUCTION.

"(a) WAIVER OF REQUIREMENTS.—Nothing in this subtitle or the amendments made by this subtitle shall be construed to create, satisfy, or waive any requirement under—

"(1) title II of the Americans With [sic] Disabilities Act of 1990 (42 U.S.C. 12131 et seq.);

"(2) the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.);

"(3) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.);

"(4) title IX of the Education Amendments of 1972 (20 U.S.C. 1681 et seq.); or

"(5) the Age Discrimination Act of 1975 (42 U.S.C. 6101 et seq.).

"(b) PROHIBITION ON FEDERALLY DEVELOPED, MANDATED, OR ENDORSED CURRICULUM .—Nothing in this subtitle or the amendments made by this subtitle shall be construed to authorize any officer or employee of the Federal Government to engage in an activity otherwise prohibited under section 103(b) of the Department of Education Organization Act (20 U.S.C. 3403(b))."

[1] *See References in Text note below.*

[2] *So in original. Probably should be "representatives".*

§665*l*. School and daycare protection

(a) In general

Not later than 180 days after December 23, 2022, and annually thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report regarding the following:

(1) The Department of Homeland Security's activities, policies, and plans to enhance the security of early childhood education programs, elementary schools, and secondary schools during the preceding year that includes information on the Department's activities through the Federal School Safety Clearinghouse.

(2) Information on all structures or efforts within the Department intended to bolster coordination among departmental components and offices involved in carrying out paragraph (1) and, with respect to each structure or effort, specificity on which components and offices are involved and which component or office leads such structure or effort.

(3) A detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out these activities.

(b) Briefing

Not later than 30 days after the submission of each report required under subsection (a), the Secretary of Homeland Security shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing regarding such report and the status of efforts to carry out plans included in such report for the preceding year.

(c) Definitions

In this section, the terms "early childhood education program", "elementary school", and "secondary school" have the meanings given such terms in section 7801 of title 20.

(Pub. L. 117–263, div. G, title LXXI, §7103, Dec. 23, 2022, 136 Stat. 3621.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§665m. President's Cup Cybersecurity Competition

(a) In general

The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the "Director") of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the "Department of Homeland Security Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition" (in this section referred to as the "competition") for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

(b) Eligibility

To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5) and shall comply with any rules promulgated by the Director regarding the competition.

(c) Competition administration

The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(d) Competition parameters

Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraphs (1), (2), or (3), as determined necessary by the Director.

(e) Use of funds

(1) In general

In order to further the goals and objectives of the competition, the Director may use amounts made available to the Director for the competition for reasonable expenses for the following:

(A) Advertising, marketing, and promoting the competition.

(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition.

(C) Promotional items, including merchandise and apparel.

(D) Consistent with section 4503 of title 5, necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(E) Monetary and nonmonetary awards for competition participants, including members of the uniformed services, subject to subsection (f).

(2) Application

This subsection shall apply to amounts appropriated on or after December 23, 2022.

(f) Prize limitation

(1) Awards by the Director

The Director may make one or more awards per competition, except that the amount or value of each shall not exceed $10,000.

(2) Awards by the Secretary of Homeland Security

The Secretary of Homeland Security may make one or more awards per competition, except the amount or the value of each shall not exceed $25,000.

(3) Regular pay

A monetary award under this section shall be in addition to the regular pay of the recipient.

(4) Overall yearly award limit

The total amount or value of awards made under this Act [1] during a fiscal year may not exceed $100,000.

(g) Reporting requirements

The Director shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following with respect to each competition conducted in the preceding year:

(1) A description of available amounts.

(2) A description of authorized expenditures.

(3) Information relating to participation.

(4) Information relating to lessons learned, and how such lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(Pub. L. 117–263, div. G, title LXXI, §7121, Dec. 23, 2022, 136 Stat. 3638.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (f)(4), is Pub. L. 117–263, Dec. 23, 2022, 136 Stat. 2395, known as the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, but probably means H.R. 6824, 117th Cong., 2d Sess. (as reported to the Senate), known as the President's Cup Cybersecurity Competition Act, which consisted only of the section containing the short title and this section. The reference to "this Act" from the original was not updated when the text of H.R. 6824 was incorporated into Pub. L. 117–263.

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

[1] So in original. Probably should refer to "this section". See References in Text note below.

§665n. Industrial Control Systems Cybersecurity Training Initiative

(a) Establishment

(1) In general

The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the "Initiative") is established within the Agency.

(2) Purpose

The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

(b) Requirements

In carrying out the Initiative, the Director shall—

(1) ensure the Initiative includes—

(A) virtual and in-person trainings and courses provided at no cost to participants;

(B) trainings and courses available at different skill levels, including introductory level courses;

(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and

(D) appropriate consideration regarding the availability of trainings and courses in different regions of the United States; and [1]

(2) engage in—

(A) collaboration with the National Laboratories of the Department of Energy in accordance with section 189 of this title;

(B) consultation with Sector Risk Management Agencies;[2]

(C) as appropriate, consultation with private sector entities with relevant expertise, such as vendors of industrial control systems technologies; and

(3) consult, to the maximum extent practicable, with commercial training providers and academia to minimize the potential for duplication of other training opportunities.

(c) Reports

(1) In general

Not later than one year after December 23, 2022, and annually thereafter, the Director shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the Initiative.

(2) Contents

Each report submitted under paragraph (1) shall include the following:

(A) A description of the courses provided under the Initiative.

(B) A description of outreach efforts to raise awareness of the availability of such courses.

(C) The number of participants in each course.

(D) Voluntarily provided information on the demographics of participants in such courses, including by sex, race, and place of residence.

(E) Information on the participation in such courses of workers from each critical infrastructure sector.

(F) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

(G) Recommendations regarding how to strengthen the state of industrial control systems cybersecurity education and training.

(Pub. L. 107–296, title XXII, §2220E, as added Pub. L. 117–263, div. G, title LXXI, §7122(a), Dec. 23, 2022, 136 Stat. 3640.)

[1] So in original. The word "and" probably should not appear.

[2] So in original. Probably should be followed by "and".

PART B—CRITICAL INFRASTRUCTURE INFORMATION

EDITORIAL NOTES

CODIFICATION

Subtitle B of title XXII of Pub. L. 107–296, comprising this part, was originally added as subtitle B of title II of Pub. L. 107–296, and was classified to part B (§131 et seq.) of subchapter II of this chapter. Subtitle B of title II of Pub. L. 107–296 was subsequently redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

§671. Definitions

In this part:

(1) Agency

The term "agency" has the meaning given it in section 551 of title 5.

(2) Covered Federal agency

The term "covered Federal agency" means the Department of Homeland Security.

(3) Critical infrastructure information

The term "critical infrastructure information" has the meaning given the term in section 650 of this title.

(4) Critical infrastructure protection program

The term "critical infrastructure protection program" means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) Protected system

The term "protected system"—

(A) means any service, physical or computer-based system, process, or procedure that

directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(6) Voluntary

(A) In general

The term "voluntary", in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) Exclusions

The term "voluntary"—

(i) in the case of any action brought under the securities laws as is defined in section 78c(a)(47) of title 15—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 78l(i) of title 15; and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(Pub. L. 107–296, title XXII, §2222, formerly title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961; renumbered title XXII, §2222, and amended Pub. L. 115–278, §2(g)(2)(H), (9)(B)(i), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(M), Dec. 23, 2022, 136 Stat. 3661.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 131 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Par. (3). Pub. L. 117–263, §7143(b)(2)(M)(i), added par. (3) and struck out former par. (3) which defined critical infrastructure information.

Pars. (5) to (8). Pub. L. 117–263, §7143(b)(2)(M)(ii), (iii), redesignated pars. (6) and (7) as (5) and (6), respectively, and struck out former pars. (5) and (8) which defined Information Sharing and Analysis Organization and cybersecurity risk and incident, respectively.

2018—Par. (8). Pub. L. 115–278, §2(g)(9)(B)(i), substituted "section 659 of this title" for "section 148 of this title".

2015—Par. (5)(A). Pub. L. 114–113, §204(1)(A), inserted ", including information related to cybersecurity risks and incidents," after "critical infrastructure information" and ", including cybersecurity risks and incidents," after "related to critical infrastructure".

Par. (5)(B). Pub. L. 114–113, §204(1)(B), inserted ", including cybersecurity risks and incidents," after "critical infrastructure information" and ", including cybersecurity risks and incidents," after "related to critical infrastructure".

Par. (5)(C). Pub. L. 114–113, §204(1)(C), inserted ", including cybersecurity risks and incidents," after "critical infrastructure information".

Par. (8). Pub. L. 114–113, §204(2), added par. (8).

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

For short title of this part as the "Critical Infrastructure Information Act of 2002", see section 2221 of Pub. L. 107–296, set out as a note under section 101 of this title.

PROHIBITION ON NEW REGULATORY AUTHORITY

Pub. L. 114–113, div. N, title II, §210, Dec. 18, 2015, 129 Stat. 2962, provided that: "Nothing in this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title] or the amendments made by this subtitle may be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2015]."

DEFINITIONS

Pub. L. 114–113, div. N, title II, §202, Dec. 18, 2015, 129 Stat. 2956, as amended by Pub. L. 115–278, §2(h)(1)(A), Nov. 16, 2018, 132 Stat. 4181, provided that: "In this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title]:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(B) the Committee on Homeland Security of the House of Representatives.

"(2) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given those terms in section 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659] [see now 6 U.S.C. 650].

"(3) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms 'cyber threat indicator' and 'defensive measure' have the meanings given those terms in section 102 [6 U.S.C. 1501].

"(4) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

"(5) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security."

§672. Designation of critical infrastructure protection program

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

(Pub. L. 107–296, title XXII, §2223, formerly title II, §213, Nov. 25, 2002, 116 Stat. 2152; renumbered title XXII, §2223, Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 132 of this title prior to renumbering by Pub. L. 115–278.

§673. Protection of voluntarily shared critical infrastructure information

(a) Protection

(1) In general

Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5 (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this part, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.[1]

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) Express statement

For purposes of paragraph (1), the term "express statement", with respect to information or records, means—

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) Limitation

No communication of critical infrastructure information to a covered Federal agency made pursuant to this part shall be considered to be an action subject to the requirements of chapter 10 of title 5.

(c) Independently obtained information

Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law. For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5.

(d) Treatment of voluntary submittal of information

The voluntary submittal to the Government of information or records that are protected from disclosure by this part shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) Procedures

(1) In general

The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after November 25, 2002.

(2) Elements

The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this part;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) Penalties

Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this part coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) Authority to issue warnings

The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) Authority to delegate

The President may delegate authority to a critical infrastructure protection program, designated under section 672 of this title, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 4558 of title 50.

(Pub. L. 107–296, title XXII, §2224, formerly title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 112–199, title I, §111, Nov. 27, 2012, 126 Stat. 1472; renumbered title XXII, §2224, and amended Pub. L. 115–278, §2(g)(2)(H), (9)(B)(ii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–286, §4(a)(18), Dec. 27, 2022, 136 Stat. 4307.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Critical Infrastructure Information Act of 2002, referred to in subsec. (a)(2)(A), is subtitle B (§2221 et seq.) of title XXII of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2150, which is classified generally to this part. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

Section was formerly classified to section 133 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–286 substituted "chapter 10 of title 5." for "the Federal Advisory Committee Act."

2018—Subsec. (h). Pub. L. 115–278, §2(g)(9)(B)(ii), substituted "section 672 of this title" for "section 132 of this title".

2012—Subsec. (c). Pub. L. 112–199 inserted at end "For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5."

2004—Subsec. (a)(1)(D)(ii)(II). Pub. L. 108–271 substituted "Government Accountability Office" for "General Accounting Office".

STATUTORY NOTES AND RELATED SUBSIDIARIES

EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–199 effective 30 days after Nov. 27, 2012, see section 202 of Pub. L. 112–199, set out as a note under section 1204 of Title 5, Government Organization and Employees.

[1] *So in original. The period probably should be a semicolon.*

§674. No private right of action

Nothing in this part may be construed to create a private right of action for enforcement of any provision of this chapter.

(Pub. L. 107–296, title XXII, §2225, formerly title II, §215, Nov. 25, 2002, 116 Stat. 2155; renumbered title XXII, §2225, Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

Section was formerly classified to section 134 of this title prior to renumbering by Pub. L. 115–278.

PART C—DECLARATION OF A SIGNIFICANT INCIDENT

§677. Sense of Congress

It is the sense of Congress that—

(1) the purpose of this part is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and

(2) the authorities established under this part are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.

(Pub. L. 107–296, title XXII, §2231, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1267.)

§677a. Definitions

For the purposes of this part:

(1) Asset response activity

The term "asset response activity" means an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—

(A) furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;

(B) assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;

(C) developing courses of action to mitigate the risks assessed under subparagraph (B);

(D) facilitating information sharing and operational coordination with entities performing threat response activities; and

(E) providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

(2) Declaration

The term "declaration" means a declaration of the Secretary under section 677b(a)(1) of this title.

(3) Director

The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(4) Federal agency

The term "Federal agency" has the meaning given the term "agency" in section 3502 of title 44.

(5) Fund

The term "Fund" means the Cyber Response and Recovery Fund established under section 677c(a) of this title.

(6) Incident

The term "incident" has the meaning given the term in section 3552 of title 44.

(7) Renewal

The term "renewal" means a renewal of a declaration under section 677b(d) of this title.

(8) Significant incident

The term "significant incident"—

(A) means an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—

(i) the national security interests, foreign relations, or economy of the United States; or

(ii) the public confidence, civil liberties, or public health and safety of the people of the

United States; and

(B) does not include an incident or a portion of a group of related incidents that occurs on—
(i) a national security system (as defined in section 3552 of title 44); or
(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44.

(Pub. L. 107–296, title XXII, §2232, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1267.)

§677b. Declaration

(a) In general

(1) Declaration

The Secretary, in consultation with the National Cyber Director, may make a declaration of a significant incident in accordance with this section for the purpose of enabling the activities described in this part if the Secretary determines that—

(A) a specific significant incident—
(i) has occurred; or
(ii) is likely to occur imminently; and

(B) otherwise available resources, other than the Fund, are likely insufficient to respond effectively to, or to mitigate effectively, the specific significant incident described in subparagraph (A).

(2) Prohibition on delegation

The Secretary may not delegate the authority provided to the Secretary under paragraph (1).

(b) Asset response activities

Upon a declaration, the Director shall coordinate—

(1) the asset response activities of each Federal agency in response to the specific significant incident associated with the declaration; and

(2) with appropriate entities, which may include—

(A) public and private entities and State and local governments with respect to the asset response activities of those entities and governments; and

(B) Federal, State, local, and Tribal law enforcement agencies with respect to investigations and threat response activities of those law enforcement agencies; and

(3) Federal, State, local, and Tribal emergency management and response agencies.

(c) Duration

Subject to subsection (d), a declaration shall terminate upon the earlier of—

(1) a determination by the Secretary that the declaration is no longer necessary; or

(2) the expiration of the 120-day period beginning on the date on which the Secretary makes the declaration.

(d) Renewal

The Secretary, without delegation, may renew a declaration as necessary.

(e) Publication

(1) In general

Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.

(2) Prohibition

A declaration or renewal published under paragraph (1) may not include the name of any

affected individual or private company.

(f) Advance actions

(1) In general

The Secretary—

(A) shall assess the resources available to respond to a potential declaration; and

(B) may take actions before and while a declaration is in effect to arrange or procure additional resources for asset response activities or technical assistance the Secretary determines necessary, which may include entering into standby contracts with private entities for cybersecurity services or incident responders in the event of a declaration.

(2) Expenditure of funds

Any expenditure from the Fund for the purpose of paragraph (1)(B) shall be made from amounts available in the Fund, and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purpose.

(Pub. L. 107–296, title XXII, §2233, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1268.)

§677c. Cyber Response and Recovery Fund

(a) In general

There is established a Cyber Response and Recovery Fund, which shall be available for—

(1) the coordination of activities described in section 677b(b) of this title;

(2) response and recovery support for the specific significant incident associated with a declaration to Federal, State, local, and Tribal, entities and public and private entities on a reimbursable or non-reimbursable basis, including through asset response activities and technical assistance, such as—

(A) vulnerability assessments and mitigation;

(B) technical incident mitigation;

(C) malware analysis;

(D) analytic support;

(E) threat detection and hunting; and

(F) network protections;

(3) as the Director determines appropriate, grants for, or cooperative agreements with, Federal, State, local, and Tribal public and private entities to respond to, and recover from, the specific significant incident associated with a declaration, such as—

(A) hardware or software to replace, update, improve, harden, or enhance the functionality of existing hardware, software, or systems; and

(B) technical contract personnel support; and

(4) advance actions taken by the Secretary under section 677b(f)(1)(B) of this title.

(b) Deposits and expenditures

(1) In general

Amounts shall be deposited into the Fund from—

(A) appropriations to the Fund for activities of the Fund; and

(B) reimbursement from Federal agencies for the activities described in paragraphs (1), (2), and (4) of subsection (a), which shall only be from amounts made available in advance in appropriations Acts for such reimbursement.

(2) Expenditures

Any expenditure from the Fund for the purposes of this part shall be made from amounts

available in the Fund from a deposit described in paragraph (1), and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purposes.

(c) Supplement not supplant

Amounts in the Fund shall be used to supplement, not supplant, other Federal, State, local, or Tribal funding for activities in response to a declaration.

(d) Reporting

The Secretary shall require an entity that receives amounts from the Fund to submit a report to the Secretary that details the specific use of the amounts.

(Pub. L. 107–296, title XXII, §2234, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1270.)

§677d. Notification and reporting

(a) Notification

Upon a declaration or renewal, the Secretary shall immediately notify the National Cyber Director and appropriate congressional committees and include in the notification—

(1) an estimation of the planned duration of the declaration;

(2) with respect to a notification of a declaration, the reason for the declaration, including information relating to the specific significant incident or imminent specific significant incident, including—

(A) the operational or mission impact or anticipated impact of the specific significant incident on Federal and non-Federal entities;

(B) if known, the perpetrator of the specific significant incident; and

(C) the scope of the Federal and non-Federal entities impacted or anticipated to be impacted by the specific significant incident;

(3) with respect to a notification of a renewal, the reason for the renewal;

(4) justification as to why available resources, other than the Fund, are insufficient to respond to or mitigate the specific significant incident; and

(5) a description of the coordination activities described in section 677b(b) of this title that the Secretary anticipates the Director to perform.

(b) Report to Congress

Not later than 180 days after the date of a declaration or renewal, the Secretary shall submit to the appropriate congressional committees a report that includes—

(1) the reason for the declaration or renewal, including information and intelligence relating to the specific significant incident that led to the declaration or renewal;

(2) the use of any funds from the Fund for the purpose of responding to the incident or threat described in paragraph (1);

(3) a description of the actions, initiatives, and projects undertaken by the Department and State and local governments and public and private entities in responding to and recovering from the specific significant incident described in paragraph (1);

(4) an accounting of the specific obligations and outlays of the Fund; and

(5) an analysis of—

(A) the impact of the specific significant incident described in paragraph (1) on Federal and non-Federal entities;

(B) the impact of the declaration or renewal on the response to, and recovery from, the specific significant incident described in paragraph (1); and

(C) the impact of the funds made available from the Fund as a result of the declaration or renewal on the recovery from, and response to, the specific significant incident described in

paragraph (1).

(c) Classification

Each notification made under subsection (a) and each report submitted under subsection (b)—

(1) shall be in an unclassified form with appropriate markings to indicate information that is exempt from disclosure under section 552 of title 5 (commonly known as the "Freedom of Information Act"); and

(2) may include a classified annex.

(d) Consolidated report

The Secretary shall not be required to submit multiple reports under subsection (b) for multiple declarations or renewals if the Secretary determines that the declarations or renewals substantively relate to the same specific significant incident.

(e) Exemption

The requirements of subchapter I of chapter 35 of title 44 (commonly known as the "Paperwork Reduction Act") shall not apply to the voluntary collection of information by the Department during an investigation of, a response to, or an immediate post-response review of, the specific significant incident leading to a declaration or renewal.

(Pub. L. 107–296, title XXII, §2235, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1270.)

§677e. Rule of construction

Nothing in this part shall be construed to impair or limit the ability of the Director to carry out the authorized activities of the Cybersecurity and Infrastructure Security Agency.

(Pub. L. 107–296, title XXII, §2236, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1272.)

§677f. Authorization of appropriations

There are authorized to be appropriated to the Fund $20,000,000 for fiscal year 2022 and each fiscal year thereafter until September 30, 2028, which shall remain available until September 30, 2028.

(Pub. L. 107–296, title XXII, §2237, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1272.)

§677g. Sunset

The authorities granted to the Secretary or the Director under this part shall expire on the date that is 7 years after November 15, 2021.

(Pub. L. 107–296, title XXII, §2238, as added Pub. L. 117–58, div. G, title VI, §70602(a), Nov. 15, 2021, 135 Stat. 1272.)

PART D—CYBER INCIDENT REPORTING

§681. Definitions

In this part:

(1) Center

The term "Center" means the center established under section 659 of this title.

(2) Council

The term "Council" means the Cyber Incident Reporting Council described in section 681f of this title.

(3) Covered cyber incident

The term "covered cyber incident" means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title.

(4) Covered entity

The term "covered entity" means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title.

(5) Cyber incident

The term "cyber incident"—

(A) has the meaning given the term "incident" in section 659 [1] of this title; and

(B) does not include an occurrence that imminently, but not actually, jeopardizes—

(i) information on information systems; or

(ii) information systems.

(6) Cyber threat

The term "cyber threat" has the meaning given the term "cybersecurity threat" in section 650 of this title.

(7) Federal entity

The term "Federal entity" has the meaning given the term in section 1501 of this title.

(8) Ransom payment

The term "ransom payment" means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

(9) Significant cyber incident

The term "significant cyber incident" means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

(10) Virtual currency

The term "virtual currency" means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

(11) Virtual currency address

The term "virtual currency address" means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

(Pub. L. 107–296, title XXII, §2240, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1039; amended Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(N), Dec. 23, 2022, 136 Stat. 3661.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 659 of this title, referred to in par. (5)(A), was subsequently amended, and section 659(a) no longer

defines the term "incident". Reference to term, "incident", as defined in this chapter deemed to be a reference to that term as defined in section 650(12) of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

AMENDMENTS

2022—Par. (2). Pub. L. 117–263, §7143(b)(2)(N)(i), (ii), redesignated par. (3) as (2) and struck out former par. (2). Prior to amendment, text of par. (2) read as follows: "The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto."

Pars. (3) to (5). Pub. L. 117–263, §7143(b)(2)(N)(ii), redesignated pars. (4) to (6) as (3) to (5), respectively. Former par. (3) redesignated (2).

Par. (6). Pub. L. 117–263, §7143(b)(2)(N)(ii), (iii), redesignated par. (7) as (6) and substituted "section 650 of this title" for "section 651 of this title". Former par. (6) redesignated (5).

Par. (7). Pub. L. 117–263, §7143(b)(2)(N)(iv), added par. (7). Former par. (7) redesignated (6).

Par. (8). Pub. L. 117–263, §7143(b)(2)(N)(iv), (vi), redesignated par. (13) as (8) and struck out former par. (8). Prior to amendment, text of par. (8) read as follows: "The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', and 'security vulnerability' have the meanings given those terms in section 1501 of this title."

Par. (9). Pub. L. 117–263, §7143(b)(2)(N)(v), (vi), redesignated par. (16) as (9) and struck out former par. (9). Prior to amendment, text of par. (9) read as follows: "The terms 'incident' and 'sharing' have the meanings given those terms in section 659 of this title."

Par. (10). Pub. L. 117–263, §7143(b)(2)(N)(v), (vi), redesignated par. (18) as (10) and struck out former par. (10). Prior to amendment, text of par. (10) read as follows: "The term 'Information Sharing and Analysis Organization' has the meaning given the term in section 671 of this title."

Par. (11). Pub. L. 117–263, §7143(b)(2)(N)(v), (vi), redesignated par. (19) as (11) and struck out former par. (11). Prior to amendment, text of par. (11) read as follows: "The term 'information system'—

"(A) has the meaning given the term in section 3502 of title 44; and

"(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers."

Par. (12). Pub. L. 117–263, §7143(b)(2)(N)(v), struck out par. (12). Text read as follows: "The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center."

Par. (13). Pub. L. 117–263, §7143(b)(2)(N)(vi), redesignated par. (13) as (8).

Par. (14). Pub. L. 117–263, §7143(b)(2)(N)(v), struck out par. (14). Text read as follows: "The term 'ransomware attack'—

"(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is—

"(i) not genuine; or

"(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system."

Par. (15). Pub. L. 117–263, §7143(b)(2)(N)(v), struck out par. (15). Text read as follows: "The term 'Sector Risk Management Agency' has the meaning given the term in section 651 of this title."

Par. (16). Pub. L. 117–263, §7143(b)(2)(N)(vi), redesignated par. (16) as (9).

Par. (17). Pub. L. 117–263, §7143(b)(2)(N)(v), struck out par. (17). Text read as follows: "The term 'supply chain compromise' means an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle."

Pars. (18), (19). Pub. L. 117–263, §7143(b)(2)(N)(vi), redesignated pars. (18) and (19) as (10) and (11), respectively.

[1] *See References in Text note below.*

§681a. Cyber incident review

(a) Activities

The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

(3) leverage information gathered about cyber incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 681e of this title;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under section [1] 681b(a) and 681c of this title involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

(9) proactively identify opportunities, consistent with the protections in section 681e of this title, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

(10) in accordance with section 681e of this title and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom

payment report, voluntarily submitted information pursuant to section 681c of this title, or information received pursuant to a request for information or subpoena under section 681d of this title, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

(b) Interagency sharing

The President or a designee of the President—

(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

(2) shall determine the appropriate Federal agencies under subsection (a)(10).

(c) Periodic briefing

Not later than 60 days after the effective date of the final rule required under section 681b(b) of this title, and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

(1) include the total number of reports submitted under sections 681b and 681c of this title during the preceding month, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 681b and 681c of this title, including—

(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

(3) include a summary of the known uses of the information in reports submitted under sections 681b and 681c of this title; and

(4) include an unclassified portion, but may include a classified component.

(Pub. L. 107–296, title XXII, §2241, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1040.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Cybersecurity Information Sharing Act of 2015, referred to in subsec. (a)(1), is title I of div. N of Pub. L. 114–113, Dec. 18, 2015, 129 Stat. 2936, which is classified generally to subchapter I (§1501 et seq.) of chapter 6 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

[1] *So in original. Probably should be "sections".*

§681b. Required reporting of certain cyber incidents

(a) In general

(1) Covered cyber incident reports

(A) In general

A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

(B) Limitation

The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

(2) Ransom payment reports

(A) In general

A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

(B) Application

The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

(3) Supplemental reports

A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until such date that such covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

(4) Preservation of information

Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

(5) Exceptions

(A) Reporting of covered cyber incident with ransom payment

If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

(B) Substantially similar reported information

(i) In general

Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements of section 681g(a) of this title, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

(ii) Limitation

The exemption in clause (i) shall take effect with respect to a covered entity once an agency agreement and sharing mechanism is in place between the Agency and the respective Federal agency, pursuant to section 681g(a) of this title.

(iii) Rules of construction

Nothing in this paragraph shall be construed to—

(I) exempt a covered entity from the reporting requirements under paragraph (3) unless the supplemental report also meets the requirements of clauses (i) and (ii) of this paragraph; [1]

(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant to section 681g of this title; or

(III) prevent an entity from communicating with the Agency.

(C) Domain name system

The requirements under paragraphs (1), (2) and (3) shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

(6) Manner, timing, and form of reports

Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

(7) Effective date

Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

(b) Rulemaking

(1) Notice of proposed rulemaking

Not later than 24 months after March 15, 2022, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

(2) Final rule

Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

(3) Subsequent rulemakings

(A) In general

The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

(B) Procedures

Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, including the issuance of a notice of proposed rulemaking under section 553 of such title.

(c) Elements

The final rule issued pursuant to subsection (b) shall be composed of the following elements:

(1) A clear description of the types of entities that constitute covered entities, based on—

(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

(A) at a minimum, require the occurrence of—

(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against [2]

(I) an information system or network; or

(II) an operational technology system or process; or

(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

(B) consider—

(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;

(ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and

(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

(C) exclude—

(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and

(ii) the threat of disruption as extortion, as described in section 681(14)(A) [3] of this title.

(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the covered entity shall comply with the requirements in this part in reporting the covered cyber incident or ransom payment.

(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

(A) A description of the covered cyber incident, including—

(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such cyber incident;

(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

(iii) the estimated date range of such incident; and

(iv) the impact to the operations of the covered entity.

(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.

(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

(E) The name and other information that clearly identifies the covered entity impacted by the covered cyber incident, including, as applicable, the State of incorporation or formation of the

covered entity, trade names, legal names, or other identifiers.

(F) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this part.

(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

(A) A description of the ransomware attack, including the estimated date range of the attack.

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

(D) The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.

(E) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that covered entity to assist with compliance with the requirements of this part.

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

(I) The amount of the ransom payment.

(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4), the period of time for which the data is required to be preserved, and allowable uses, processes, and procedures.

(7) Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—

(A) be established by the Director in consultation with the Council;

(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable;

(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and

(D) provide a clear description of what constitutes substantial new or different information.

(8) Procedures for—

(A) entities, including third parties pursuant to subsection (d)(1), to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the Agency to carry out—

(i) the enforcement provisions of section 681d of this title, including with respect to the issuance, service, withdrawal, referral process, and enforcement of subpoenas, appeals and due process procedures;

(ii) other available enforcement mechanisms including acquisition, suspension and

debarment procedures; and

(iii) other aspects of noncompliance;

(C) implementing the exceptions provided in subsection (a)(5); and

(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 1504(b) of this title and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

(9) Other procedural measures directly necessary to implement subsection (a).

(d) Third party report submission and ransom payment

(1) Report submission

A covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).

(2) Ransom payment

If a covered entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

(3) Duty to report

Third-party reporting under this subparagraph [4] does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

(4) Responsibility to advise

Any third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this section.

(e) Outreach to covered entities

(1) In general

The Agency shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

(2) Elements

The outreach and education campaign under paragraph (1) shall include the following:

(A) An overview of the final rule issued pursuant to subsection (b).

(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken under section 681d of this title when a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

(F) An overview of the privacy and civil liberties requirements in this part.

(3) Coordination

In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

(A) the Critical Infrastructure Partnership Advisory Council established under section 451 of this title;

(B) Information Sharing and Analysis Organizations;

(C) trade associations;

(D) information sharing and analysis centers;

(E) sector coordinating councils; and

(F) any other entity as determined appropriate by the Director.

(f) Exemption

Sections 3506(c), 3507, 3508, and 3509 of title 44 shall not apply to any action to carry out this section.

(g) Rule of construction

Nothing in this section shall affect the authorities of the Federal Government to implement the requirements of Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), including changes to the Federal Acquisition Regulations and remedies to include suspension and debarment.

(h) Savings provision

Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

(Pub. L. 107–296, title XXII, §2242, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1042.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 681(14)(A) of this title, referred to in subsec. (c)(2)(C)(ii), was repealed by section 7143(b)(2)(N)(v) of Pub. L. 117–263. See section 650(22)(A) of this title. References to terms defined in this chapter deemed to be references to those terms as defined in section 650 of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

Executive Order 14028, referred to in subsec. (g), is Ex. Ord. No. 14028, May 12, 2021, 86 F.R. 26633, which is set out as a note under section 3551 of Title 44, Public Printing and Documents.

[1] So in original. Probably should be "subparagraph".

[2] So in original. Probably should be followed by a dash.

[3] See References in Text note below.

[4] So in original. Probably should be "subsection".

§681c. Voluntary reporting of other cyber incidents

(a) In general

Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) of section 681b(a) of this title, but may enhance the situational awareness of cyber threats.

(b) Voluntary provision of additional information in required reports

Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 681b(a) of this title information that is not required to be included, but may enhance the situational awareness of cyber threats.

(c) Application of section 681e of this title

Section 681e of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b) as it applies to reports and information submitted under section 681b of this title.

(Pub. L. 107–296, title XXII, §2243, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1049; amended Pub. L. 117–263, div. G, title LXXI, §7143(e)(1), Dec. 23, 2022, 136 Stat. 3664.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (c). Pub. L. 117–263 added subsec. (c) and struck out former subsec. (c). Prior to amendment, text read as follows: "The protections under section 681e of this title applicable to reports made under section 681b of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b)."

§681d. Noncompliance with required reporting

(a) Purpose

In the event that a covered entity that is required to submit a report under section 681b(a) of this title fails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

(b) Initial request for information

(1) In general

If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 681a(a) of this title, that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 681b(a) of this title, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) Treatment

Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 681b of this title [1] including that section 681e of this title shall apply to such information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 681b of this title.

(c) Enforcement

(1) In general

If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from

which such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 681b of this title and any implementing regulations, and assess potential impacts to national security, economic security, or public health and safety.

(2) Civil action

(A) In general

If a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

(B) Venue

An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

(C) Contempt of court

A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

(3) Non-delegation

The authority of the Director to issue a subpoena under this subsection may not be delegated.

(4) Authentication

(A) In general

Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) Invalid if not authenticated

Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

(d) Provision of certain information to Attorney General

(1) In general

Notwithstanding section 681e(a)(5) of this title and paragraph (b)(2) of this section, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution.

(2) Consultation

The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

(e) Considerations

When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

(1) the complexity in determining if a covered cyber incident has occurred; and

(2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

(f) Exclusions

This section shall not apply to a State, local, Tribal, or territorial government entity.

(g) Report to Congress

The Director shall submit to Congress an annual report on the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b);

(2) issued a subpoena pursuant to subsection (c); or

(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

(h) Publication of the annual report

The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b); or

(2) issued a subpoena pursuant to subsection (c).

(i) Anonymization of reports

The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

(Pub. L. 107–296, title XXII, §2244, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1049; amended Pub. L. 117–263, div. G, title LXXI, §7143(e)(2), Dec. 23, 2022, 136 Stat. 3664.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (b)(2). Pub. L. 117–263 inserted "including that section 681e of this title shall apply to such information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 681b of this title" after "section 681b of this title".

[1] *So in original. Probably should be followed by a comma.*

§681e. Information shared with or provided to the Federal Government

(a) Disclosure, retention, and use

(1) Authorized activities

Information provided to the Agency pursuant to section 681b or 681c of this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(A) a cybersecurity purpose;

(B) the purpose of identifying—

(i) a cyber threat, including the source of the cyber threat; or

(ii) a security vulnerability;

(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out

of a cyber incident reported pursuant to section 681b or 681c of this title or any of the offenses listed in section 1504(d)(5)(A)(v) of this title.

(2) Agency actions after receipt

(A) Rapid, confidential sharing of cyber threat indicators

Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

(B) Principles for sharing security vulnerabilities

With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

(3) Privacy and civil liberties

Information contained in covered cyber incident and ransom payment reports submitted to the Agency pursuant to section 681b of this title shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 1504 of this title and in a manner that protects personal information from unauthorized use or unauthorized disclosure.

(4) Digital security

The Agency shall ensure that reports submitted to the Agency pursuant to section 681b of this title, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

(5) Prohibition on use of information in regulatory actions

(A) In general

A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this part to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

(B) Clarification

A report submitted to the Agency pursuant to section 681b or 681c of this title may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.

(b) Protections for reporting entities and information

Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 681b of this title, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 681c of this title, shall—

(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

(2) be exempt from disclosure under section 552(b)(3) of title 5 (commonly known as the "Freedom of Information Act"), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

(4) not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) Liability protections

(1) In general

No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 681b(a) of this title that is submitted in conformance with this part and the rule promulgated under section 681b(b) of this title, except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 681d(c)(2) of this title.

(2) Scope

The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

(3) Restrictions

Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this part or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this part shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

(d) Sharing with non-Federal entities

The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 681b of this title available to critical infrastructure owners and operators and the general public.

(e) Stored Communications Act

Nothing in this part shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18 (commonly known as the "Stored Communications Act").

(Pub. L. 107–296, title XXII, §2245, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1051.)

§681f. Cyber Incident Reporting Council

(a) Responsibility of the Secretary

The Secretary shall lead an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations.

(b) Rule of construction

Nothing in subsection (a) shall be construed to provide any additional regulatory authority to any Federal entity.

(Pub. L. 107–296, title XXII, §2246, as added Pub. L. 117–103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1054.)

§681g. Federal sharing of incident reports

(a) Cyber incident reporting sharing

(1) In general

Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Department of Homeland Security (including the Cybersecurity and Infrastructure Security Agency) and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 681a(b) of this title, as added by section 103 of this division.

(2) Rule of construction

The requirements described in paragraph (1) and section 681e(d) of this title, as added by section 103 of this division, may not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure or provision of information within the executive branch.

(3) Protection of information

The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this division or the amendments made by this division.

(4) Effective date

This subsection shall take effect on the effective date of the final rule issued pursuant to section 681b(b) of this title, as added by section 103 of this division.

(5) Agency agreements

(A) In general

The Agency and any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives incident reports from entities, including due to ransomware attacks, shall, as appropriate, enter into a documented agreement to establish policies, processes, procedures, and mechanisms to ensure reports are shared with the Agency pursuant to paragraph (1).

(B) Availability

To the maximum extent practicable, each documented agreement required under subparagraph (A) shall be made publicly available.

(C) Requirement

The documented agreements required by subparagraph (A) shall require reports be shared from Federal agencies with the Agency in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments established in section 681b of this title, as added by section 103 of this division.

(b) Harmonizing reporting requirements

The Secretary of Homeland Security, acting through the Director, shall, in consultation with the Cyber Incident Reporting Council described in section 681f of this title, as added by section 103 of this division, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with appropriate Federal partners and regulatory authorities that receive reports relating to incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of the Agency to gain timely situational awareness of a covered cyber incident or ransom payment.

(Pub. L. 117–103, div. Y, §104, Mar. 15, 2022, 136 Stat. 1054.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 103 of this division, referred to in text, is section 103 of div. Y of Pub. L. 117–103, which enacted this part and amended section 659 of this title.

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of terms used in this section, see section 102 of div. Y of Pub. L. 117–103, which is set out as a note under section 665j of this title.

CHAPTER 2—NATIONAL EMERGENCY MANAGEMENT

Sec.

701. Definitions.

SUBCHAPTER I—PERSONNEL PROVISIONS

PART A—FEDERAL EMERGENCY MANAGEMENT AGENCY PERSONNEL

711. Surge Capacity Force.

PART B—EMERGENCY MANAGEMENT CAPABILITIES

721. Evacuation preparedness technical assistance.
722. Urban Search and Rescue Response System.
723. Metropolitan Medical Response Grant Program.
724. Logistics.
725. Prepositioned equipment program.
726. Basic life supporting first aid and education.
727. Improvements to information technology systems.
728. Disclosure of certain information to law enforcement agencies.

SUBCHAPTER II—COMPREHENSIVE PREPAREDNESS SYSTEM

PART A—NATIONAL PREPAREDNESS SYSTEM

741. Definitions.
742. National preparedness.
743. National preparedness goal.

744. Establishment of national preparedness system.
745. National planning scenarios.
746. Target capabilities and preparedness priorities.
747. Equipment and training standards.
748. Training and exercises.
748a. Prioritization of facilities.
749. Comprehensive assessment system.
750. Remedial action management program.
751. Federal response capability inventory.
752. Reporting requirements.
753. Federal preparedness.
754. Use of existing resources.

PART B—ADDITIONAL PREPAREDNESS

761. Emergency Management Assistance Compact grants.
762. Emergency management performance grants program.
763. Transfer of Noble Training Center.
763a. Training for Federal Government, foreign governments, or private entities.
764. National exercise simulation center.
765. Real property transactions.

PART C—MISCELLANEOUS AUTHORITIES

771. National Disaster Recovery Strategy.
772. National Disaster Housing Strategy.
773. Individuals with disabilities guidelines.
774. Reunification.
775. National Emergency Family Registry and Locator System.
776. Individuals and households pilot program.
777. Public assistance pilot program.

PART D—PREVENTION OF FRAUD, WASTE, AND ABUSE

791. Advance contracting.
792. Repealed.
793. Oversight and accountability of Federal disaster expenditures.
794. Limitation on length of certain noncompetitive contracts.
795. Fraud, waste, and abuse controls.
796. Registry of disaster response contractors.
797. Fraud prevention training program.

PART E—AUTHORIZATION OF APPROPRIATIONS

811. Authorization of appropriations.

PART F—GLOBAL CATASTROPHIC RISK MANAGEMENT

821. Definitions.
822. Assessment of global catastrophic risk.
823. Report required.
824. Enhanced catastrophic incident annex.
825. Rules of construction.

§701. Definitions

In this title— [1]

(1) the term "Administrator" means the Administrator of the Agency;

(2) the term "Agency" means the Federal Emergency Management Agency;

(3) the term "appropriate committees of Congress" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) those committees of the House of Representatives that the Speaker of the House of

Representatives determines appropriate;

(4) the term "catastrophic incident" means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area;

(5) the term "Department" means the Department of Homeland Security;

(6) the terms "emergency" and "major disaster" have the meanings given the terms in section 5122 of title 42;

(7) the term "emergency management" means the governmental function that coordinates and integrates all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters;

(8) the term "emergency response provider" has the meaning given the term in section 101 of this title;

(9) the term "Federal coordinating officer" means a Federal coordinating officer as described in section 5143 of title 42;

(10) the term "individual with a disability" has the meaning given the term in section 12102 of title 42;

(11) the terms "local government" and "State" have the meaning given the terms in section 101 of this title;

(12) the term "National Incident Management System" means a system to enable effective, efficient, and collaborative incident management;

(13) the term "National Response Plan" means the National Response Plan or any successor plan prepared under section 314(a)(6) of this title;

(14) the term "Secretary" means the Secretary of Homeland Security;

(15) the term "surge capacity" means the ability to rapidly and substantially increase the provision of search and rescue capabilities, food, water, medicine, shelter and housing, medical care, evacuation capacity, staffing (including disaster assistance employees), and other resources necessary to save lives and protect property during a catastrophic incident; and

(16) the term "tribal government" means the government of an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation.

(Pub. L. 109–295, title VI, §602, Oct. 4, 2006, 120 Stat. 1394.)

EDITORIAL NOTES

REFERENCES IN TEXT

This title, referred to in text, is title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1355, known as the Post-Katrina Emergency Management Reform Act of 2006. For complete classification of title VI to the Code, see Short Title note set out below and Tables.

Section 314(a)(6) of this title, referred to in par. (13), was in the original "section 502(a)(6) of the Homeland Security Act 2002" and was translated as meaning section 502 of Pub. L. 107–296 prior to its redesignation as section 504 by Pub. L. 109–295, §611(8), and not section 506 of Pub. L. 107–296 which was redesignated section 502 by Pub. L. 109–295, §611(9), and is classified to section 312 of this title, to reflect the probable intent of Congress.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Any reference to the Administrator of the Federal Emergency Management Agency in title VI of Pub. L. 109–295 or an amendment by title VI to be considered to refer and apply to the Director of the Federal Emergency Management Agency until Mar. 31, 2007, see section 612(f)(2) of Pub. L. 109–295, set out as a note under section 313 of this title.

EFFECTIVE DATE

Pub. L. 109–295, title VI, §614, Oct. 4, 2006, 120 Stat. 1411, provided that:

"(a) IN GENERAL.—Except as provided in subsection (b), this title [see Tables for classification] and the amendments made by this title shall take effect on the date of enactment of this Act [Oct. 4, 2006].

"(b) EXCEPTIONS.—The following shall take effect on March 31, 2007:

"(1) The amendments made by section 611(11) [enacting section 313 of this title].

"(2) The amendments made by section 611(12) [amending section 314 of this title].

"(3) Sections 505, 507, 508, and 514 of the Homeland Security Act of 2002 [sections 315, 317, 318, and 321c of this title], as amended by section 611(13) of this Act.

"(4) The amendments made by subsection (a) [sic].

"(5) The amendments made by subsection (b)(1) [sic]."

SHORT TITLE OF 2022 AMENDMENT

Pub. L. 117–263, div. G, title LXXIII, §7301, Dec. 23, 2022, 136 Stat. 3684, provided that: "This subtitle [subtitle A (§§7301–7309) of title LXXIII of div. G of Pub. L. 117–263, enacting part F of subchapter II of this chapter] may be cited as the 'Global Catastrophic Risk Management Act of 2022'."

SHORT TITLE OF 2020 AMENDMENT

Pub. L. 116–272, §1, Dec. 31, 2020, 134 Stat. 3349, provided that: "This Act [amending section 791 of this title and enacting provisions set out as notes under section 791 of this title] may be cited as the 'Federal Advance Contracts Enhancement Act' or the 'FACE Act'."

SHORT TITLE OF 2019 AMENDMENT

Pub. L. 116–64, §1, Oct. 9, 2019, 133 Stat. 1122, provided that: "This Act [amending section 748 of this title] may be cited as the 'Terrorist and Foreign Fighter Travel Exercise Act of 2019'."

SHORT TITLE

Pub. L. 109–295, title VI, §601, Oct. 4, 2006, 120 Stat. 1394, provided that: "This title [see Tables for classification] may be cited as the 'Post-Katrina Emergency Management Reform Act of 2006'."

CLARIFICATION OF CONGRESSIONAL INTENT

Pub. L. 110–53, title XXII, §2202, Aug. 3, 2007, 121 Stat. 541, provided that: "The Federal departments and agencies (including independent agencies) identified under the provisions of this title [enacting provisions set out as notes under section 194 of this title and section 247d–3a of Title 42, The Public Health and Welfare, and amending provisions set out as a note under section 309 of Title 47, Telecommunications] and title III of this Act [enacting sections 579 and 580 of this title and amending sections 194 and 572 of this title] and title VI of Public Law 109–295 [see Short Title note set out above] shall carry out their respective duties and responsibilities in a manner that does not impede the implementation of requirements specified under this title and title III of this Act and title VI of Public Law 109–295. Notwithstanding the obligations under section 1806 of Public Law 109–295 [probably means Pub. L. 107–296; 6 U.S.C. 576], the provisions of this title and title III of this Act and title VI of Public Law 109–295 shall not preclude or obstruct any such department or agency from exercising its other authorities related to emergency communications matters."

NATIONAL WEATHER SERVICE

Pub. L. 109–295, title VI, §613, Oct. 4, 2006, 120 Stat. 1411, provided that: "Nothing in this title [see Tables for classification] shall alter or otherwise affect the authorities and activities of the National Weather Service to protect life and property, including under the Act of October 1, 1890 (26 Stat. 653-55) [15 U.S.C. 312 et seq.]."

REFERENCES IN PUB. L. 109–295

Pub. L. 109–295, title VI, §699A, Oct. 4, 2006, 120 Stat. 1463, provided that: "Except as expressly provided otherwise, any reference to 'this Act' contained in this title [see Tables for classification] shall be treated as referring only to the provisions of this title."

[1] *See References in Text note below.*

SUBCHAPTER I—PERSONNEL PROVISIONS

PART A—FEDERAL EMERGENCY MANAGEMENT AGENCY PERSONNEL

§711. Surge Capacity Force

(a) Establishment

(1) In general

Not later than 6 months after October 4, 2006, the Administrator shall prepare and submit to the appropriate committees of Congress a plan to establish and implement a Surge Capacity Force for deployment of individuals to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

(2) Authority

(A) In general

Except as provided in subparagraph (B), the plan shall provide for individuals in the Surge Capacity Force to be trained and deployed under the authorities set forth in the Robert T. Stafford Disaster Relief and Emergency Assistance Act [42 U.S.C. 5121 et seq.].

(B) Exception

If the Administrator determines that the existing authorities are inadequate for the training and deployment of individuals in the Surge Capacity Force, the Administrator shall report to Congress as to the additional statutory authorities that the Administrator determines necessary.

(b) Employees designated to serve

The plan shall include procedures under which the Secretary shall designate employees of the Department who are not employees of the Agency and shall, in conjunction with the heads of other Executive agencies, designate employees of those other Executive agencies, as appropriate, to serve on the Surge Capacity Force.

(c) Capabilities

The plan shall ensure that the Surge Capacity Force—

(1) includes a sufficient number of individuals credentialed in accordance with section 320 of this title that are capable of deploying rapidly and efficiently after activation to prepare for, respond to, and recover from natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; and

(2) includes a sufficient number of full-time, highly trained individuals credentialed in accordance with section 320 of this title to lead and manage the Surge Capacity Force.

(d) Training

The plan shall ensure that the Administrator provides appropriate and continuous training to members of the Surge Capacity Force to ensure such personnel are adequately trained on the Agency's programs and policies for natural disasters, acts of terrorism, and other man-made disasters.

(e) No impact on agency personnel ceiling

Surge Capacity Force members shall not be counted against any personnel ceiling applicable to the Federal Emergency Management Agency.

(f) Expenses

The Administrator may provide members of the Surge Capacity Force with travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under

subchapter I of chapter 57 of title 5 for the purpose of participating in any training that relates to service as a member of the Surge Capacity Force.

(g) Immediate implementation of Surge Capacity Force involving Federal employees

As soon as practicable after October 4, 2006, the Administrator shall develop and implement—

(1) the procedures under subsection (b); and

(2) other elements of the plan needed to establish the portion of the Surge Capacity Force consisting of individuals designated under those procedures.

(Pub. L. 109–295, title VI, §624, Oct. 4, 2006, 120 Stat. 1419.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a)(2)(A), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

PART B—EMERGENCY MANAGEMENT CAPABILITIES

§721. Evacuation preparedness technical assistance

The Administrator, in coordination with the heads of other appropriate Federal agencies, shall provide evacuation preparedness technical assistance to State, local, and tribal governments, including the preparation of hurricane evacuation studies and technical assistance in developing evacuation plans, assessing storm surge estimates, evacuation zones, evacuation clearance times, transportation capacity, and shelter capacity.

(Pub. L. 109–295, title VI, §632, Oct. 4, 2006, 120 Stat. 1421.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

GUIDANCE ON EVACUATION ROUTES

Pub. L. 115–254, div. D, §1209, Oct. 5, 2018, 132 Stat. 3441, provided that:

"(a) IN GENERAL.—

"(1) IDENTIFICATION.—The Administrator [of the Federal Emergency Management Agency], in coordination with the Administrator of the Federal Highway Administration, shall develop and issue guidance for State, local, and Indian tribal governments regarding the identification of evacuation routes.

"(2) GUIDANCE.—The Administrator of the Federal Highway Administration, in coordination with the Administrator, shall revise existing guidance or issue new guidance as appropriate for State, local, and Indian tribal governments regarding the design, construction, maintenance, and repair of evacuation routes.

"(b) CONSIDERATIONS.—

"(1) IDENTIFICATION.—In developing the guidance under subsection (a)(1), the Administrator shall consider—

"(A) whether evacuation routes have resisted impacts and recovered quickly from disasters, regardless of cause;

"(B) the need to evacuate special needs populations, including—

"(i) individuals with a physical or mental disability;

"(ii) individuals in schools, daycare centers, mobile home parks, prisons, nursing homes and other long-term care facilities, and detention centers;

"(iii) individuals with limited-English proficiency;

"(iv) the elderly; and

"(v) individuals who are tourists, seasonal workers, or homeless;

"(C) the sharing of information and other public communications with evacuees during evacuations;

"(D) the sheltering of evacuees, including the care, protection, and sheltering of animals;

"(E) the return of evacuees to their homes; and

"(F) such other items the Administrator considers appropriate.

"(2) DESIGN, CONSTRUCTION, MAINTENANCE, AND REPAIR.—In revising or issuing guidance under subsection (a)(2), the Administrator of the Federal Highway Administration shall consider—

"(A) methods that assist evacuation routes to—

"(i) withstand likely risks to viability, including flammability and hydrostatic forces;

"(ii) improve durability, strength (including the ability to withstand tensile stresses and compressive stresses), and sustainability; and

"(iii) provide for long-term cost savings;

"(B) the ability of evacuation routes to effectively manage contraflow operations;

"(C) for evacuation routes on public lands, the viewpoints of the applicable Federal land management agency regarding emergency operations, sustainability, and resource protection; and

"(D) such other items the Administrator of the Federal Highway Administration considers appropriate.

"(c) STUDY.—The Administrator, in coordination with the Administrator of the Federal Highway Administration and State, local, territorial, and Indian tribal governments, may—

"(1) conduct a study of the adequacy of available evacuation routes to accommodate the flow of evacuees; and

"(2) submit recommendations on how to help with anticipated evacuation route flow, based on the study conducted under paragraph (1), to—

"(A) the Federal Highway Administration;

"(B) the [Federal Emergency Management] Agency;

"(C) State, local, territorial, and Indian tribal governments; and

"(D) Congress."

[For definition of "State", as used in section 1209 of Pub. L. 115–254, set out above, see section 1203 of Pub. L. 115–254, set out as a note under section 5122 of Title 42, The Public Health and Welfare.]

§722. Urban Search and Rescue Response System

(a) In general

There is in the Agency a system known as the Urban Search and Rescue Response System.

(b) Authorization of appropriations

There is authorized to be appropriated to carry out the system for fiscal year 2008, an amount equal to the amount appropriated for the system for fiscal year 2007 and an additional $20,000,000.

(Pub. L. 109–295, title VI, §634, Oct. 4, 2006, 120 Stat. 1421.)

§723. Metropolitan Medical Response Grant Program

(a) In general

There is a Metropolitan Medical Response Program.

(b) Purposes

The program shall include each purpose of the program as it existed on June 1, 2006.

(c) Authorization of appropriations

There is authorized to be appropriated to carry out the program for fiscal year 2008, an amount equal to the amount appropriated for the program for fiscal year 2007 and an additional $30,000,000.

(Pub. L. 109–295, title VI, §635, Oct. 4, 2006, 120 Stat. 1421.)

§724. Logistics

The Administrator shall develop an efficient, transparent, and flexible logistics system for procurement and delivery of goods and services necessary for an effective and timely response to natural disasters, acts of terrorism, and other man-made disasters and for real-time visibility of items at each point throughout the logistics system.

(Pub. L. 109–295, title VI, §636, Oct. 4, 2006, 120 Stat. 1422.)

§725. Prepositioned equipment program

(a) In general

The Administrator shall establish a prepositioned equipment program to preposition standardized emergency equipment in at least 11 locations to sustain and replenish critical assets used by State, local, and tribal governments in response to (or rendered inoperable by the effects of) natural disasters, acts of terrorism, and other man-made disasters.

(b) Notice

The Administrator shall notify State, local, and tribal officials in an area in which a location for the prepositioned equipment program will be closed not later than 60 days before the date of such closure.

(Pub. L. 109–295, title VI, §637, Oct. 4, 2006, 120 Stat. 1422.)

§726. Basic life supporting first aid and education

The Administrator shall enter into agreements with organizations to provide funds to emergency response providers to provide education and training in life supporting first aid to children.

(Pub. L. 109–295, title VI, §639, Oct. 4, 2006, 120 Stat. 1423.)

§727. Improvements to information technology systems

(a) Measures to improve information technology systems

The Administrator, in coordination with the Chief Information Officer of the Department, shall take appropriate measures to update and improve the information technology systems of the Agency, including measures to—

(1) ensure that the multiple information technology systems of the Agency (including the National Emergency Management Information System, the Logistics Information Management System III, and the Automated Deployment Database) are, to the extent practicable, fully compatible and can share and access information, as appropriate, from each other;

(2) ensure technology enhancements reach the headquarters and regional offices of the Agency in a timely fashion, to allow seamless integration;

(3) develop and maintain a testing environment that ensures that all system components are properly and thoroughly tested before their release;

(4) ensure that the information technology systems of the Agency have the capacity to track disaster response personnel, mission assignments task orders, commodities, and supplies used in response to a natural disaster, act of terrorism, or other man-made disaster;

(5) make appropriate improvements to the National Emergency Management Information System to address shortcomings in such system on October 4, 2006; and

(6) provide training, manuals, and guidance on information technology systems to personnel, including disaster response personnel, to help ensure employees can properly use information technology systems.

(b) Report

Not later than 270 days after October 4, 2006, the Administrator shall submit to the appropriate committees of Congress a report describing the implementation of this section, including a description of any actions taken, improvements made, and remaining problems and a description of any additional funding needed to make necessary and appropriate improvements to the information technology systems of the Agency.

(Pub. L. 109–295, title VI, §640, Oct. 4, 2006, 120 Stat. 1423.)

§728. Disclosure of certain information to law enforcement agencies

In the event of circumstances requiring an evacuation, sheltering, or mass relocation, the Administrator may disclose information in any individual assistance database of the Agency in accordance with section 552a(b) of title 5 (commonly referred to as the "Privacy Act") to any law enforcement agency of the Federal Government or a State, local, or tribal government in order to identify illegal conduct or address public safety or security issues, including compliance with sex offender notification laws.

(Pub. L. 109–295, title VI, §640a, Oct. 4, 2006, 120 Stat. 1424.)

SUBCHAPTER II—COMPREHENSIVE PREPAREDNESS SYSTEM

PART A—NATIONAL PREPAREDNESS SYSTEM

§741. Definitions

In this part:

(1) Capability

The term "capability" means the ability to provide the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be achieved with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome.

(2) Credentialed; credentialing

The terms "credentialed" and "credentialing" have the meanings given those terms in section 311 of this title.

(3) Hazard

The term "hazard" has the meaning given that term under section 5195a(a)(1) of title 42.

(4) Mission assignment

The term "mission assignment" means a work order issued to a Federal agency by the Agency, directing completion by that agency of a specified task and setting forth funding, other managerial controls, and guidance.

(5) National preparedness goal

The term "national preparedness goal" means the national preparedness goal established under section 743 of this title.

(6) National preparedness system

The term "national preparedness system" means the national preparedness system established under section 744 of this title.

(7) National training program

The term "national training program" means the national training program established under section 748(a) of this title.

(8) Operational readiness

The term "operational readiness" means the capability of an organization, an asset, a system, or equipment to perform the missions or functions for which it is organized or designed.

(9) Performance measure

The term "performance measure" means a quantitative or qualitative characteristic used to gauge the results of an outcome compared to its intended purpose.

(10) Performance metric

The term "performance metric" means a particular value or characteristic used to measure the outcome that is generally expressed in terms of a baseline and a target.

(11) Prevention

The term "prevention" means any activity undertaken to avoid, prevent, or stop a threatened or actual act of terrorism.

(12) Resources

The term "resources" has the meaning given that term in section 311 of this title.

(13) Type

The term "type" means a classification of resources that refers to the capability of a resource.

(14) Typed; typing

The terms "typed" and "typing" have the meanings given those terms in section 311 of this title.

(Pub. L. 109–295, title VI, §641, Oct. 4, 2006, 120 Stat. 1424; Pub. L. 110–53, title IV, §401(b), Aug. 3, 2007, 121 Stat. 302.)

EDITORIAL NOTES

AMENDMENTS

2007—Pars. (2) to (14). Pub. L. 110–53 added pars. (2) and (12) to (14) and redesignated former pars. (2) to (10) as (3) to (11), respectively.

§742. National preparedness

In order to prepare the Nation for all hazards, including natural disasters, acts of terrorism, and other man-made disasters, the President, consistent with the declaration of policy under section 5195 of title 42 and title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by this Act, shall develop a national preparedness goal and a national preparedness system.

(Pub. L. 109–295, title VI, §642, Oct. 4, 2006, 120 Stat. 1425.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Homeland Security Act of 2002, referred to in text, is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135. Title V of the Act is classified generally to subchapter V (§311 et seq.) of chapter 1 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

This Act, referred to in text, means title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1394, known as the Post-Katrina Emergency Management Reform Act of 2006. For complete classification of this Act to the Code, see Short Title and References in Pub. L. 109–295 notes set out under section 701 of this title and Tables.

§743. National preparedness goal

(a) Establishment

The President, acting through the Administrator, shall complete, revise, and update, as necessary, a national preparedness goal that defines the target level of preparedness to ensure the Nation's ability to prevent, respond to, recover from, and mitigate against natural disasters, acts of terrorism, and other man-made disasters.

(b) National Incident Management System and National Response Plan

The national preparedness goal, to the greatest extent practicable, shall be consistent with the National Incident Management System and the National Response Plan.

(Pub. L. 109–295, title VI, §643, Oct. 4, 2006, 120 Stat. 1425.)

§744. Establishment of national preparedness system

(a) Establishment

The President, acting through the Administrator, shall develop a national preparedness system to enable the Nation to meet the national preparedness goal.

(b) Components

The national preparedness system shall include the following components:

(1) Target capabilities and preparedness priorities.
(2) Equipment and training standards.
(3) Training and exercises.
(4) Comprehensive assessment system.
(5) Remedial action management program.
(6) Federal response capability inventory.
(7) Reporting requirements.
(8) Federal preparedness.

(c) National planning scenarios

The national preparedness system may include national planning scenarios.

(Pub. L. 109–295, title VI, §644, Oct. 4, 2006, 120 Stat. 1425.)

§745. National planning scenarios

(a) In general

The Administrator, in coordination with the heads of appropriate Federal agencies and the National Advisory Council, may develop planning scenarios to reflect the relative risk requirements presented by all hazards, including natural disasters, acts of terrorism, and other man-made disasters, in order to provide the foundation for the flexible and adaptive development of target capabilities and the identification of target capability levels to meet the national preparedness goal.

(b) Development

In developing, revising, and replacing national planning scenarios, the Administrator shall ensure that the scenarios—

(1) reflect the relative risk of all hazards and illustrate the potential scope, magnitude, and complexity of a broad range of representative hazards; and

(2) provide the minimum number of representative scenarios necessary to identify and define the tasks and target capabilities required to respond to all hazards.

(Pub. L. 109–295, title VI, §645, Oct. 4, 2006, 120 Stat. 1425.)

§746. Target capabilities and preparedness priorities

(a) Establishment of guidelines on target capabilities

Not later than 180 days after October 4, 2006, the Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall complete, revise, and update, as necessary, guidelines to define risk-based target capabilities for Federal, State, local, and tribal government preparedness that will enable the Nation to prevent, respond to, recover from, and mitigate against all hazards, including natural disasters, acts of terrorism, and other man-made disasters.

(b) Distribution of guidelines

The Administrator shall ensure that the guidelines are provided promptly to the appropriate committees of Congress and the States.

(c) Objectives

The Administrator shall ensure that the guidelines are specific, flexible, and measurable.

(d) Terrorism risk assessment

With respect to analyzing and assessing the risk of acts of terrorism, the Administrator shall consider—

(1) the variables of threat, vulnerability, and consequences related to population (including transient commuting and tourist populations), areas of high population density, critical infrastructure, coastline, and international borders; and

(2) the most current risk assessment available from the Chief Intelligence Officer of the Department of the threats of terrorism against the United States.

(e) Preparedness priorities

In establishing the guidelines under subsection (a), the Administrator shall establish preparedness priorities that appropriately balance the risk of all hazards, including natural disasters, acts of terrorism, and other man-made disasters, with the resources required to prevent, respond to, recover from, and mitigate against the hazards.

(f) Mutual aid agreements

The Administrator may provide support for the development of mutual aid agreements within States.

(Pub. L. 109–295, title VI, §646, Oct. 4, 2006, 120 Stat. 1426.)

§747. Equipment and training standards

(a) Equipment standards

(1) In general

The Administrator, in coordination with the heads of appropriate Federal agencies and the National Advisory Council, shall support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for the performance, use, and validation of equipment used by Federal, State, local, and tribal governments and nongovernmental emergency response providers.

(2) Requirements

The national voluntary consensus standards shall—

(A) be designed to achieve equipment and other capabilities consistent with the national preparedness goal, including the safety and health of emergency response providers;

(B) to the maximum extent practicable, be consistent with existing national voluntary consensus standards;

(C) take into account, as appropriate, threats that may not have been contemplated when the existing standards were developed; and

(D) focus on maximizing operability, interoperability, interchangeability, durability, flexibility, efficiency, efficacy, portability, sustainability, and safety.

(b) Training standards

The Administrator shall—

(1) support the development, promulgation, and regular updating, as necessary, of national voluntary consensus standards for training; and

(2) ensure that the training provided under the national training program is consistent with the standards.

(c) Consultation with standards organizations

In carrying out this section, the Administrator shall consult with representatives of relevant public and private sector national voluntary consensus standards development organizations.

(Pub. L. 109–295, title VI, §647, Oct. 4, 2006, 120 Stat. 1426.)

§748. Training and exercises

(a) National training program

(1) In general

Beginning not later than 180 days after October 4, 2006, the Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national training program to implement the national preparedness goal, National Incident Management System, National Response Plan, and other related plans and strategies.

(2) Training partners

In developing and implementing the national training program, the Administrator shall—

(A) work with government training facilities, academic institutions, private organizations, and other entities that provide specialized, state-of-the-art training for emergency managers or emergency response providers; and

(B) utilize, as appropriate, training courses provided by community colleges, State and local public safety academies, State and private universities, and other facilities.

(b) National exercise program

(1) In general

Beginning not later than 180 days after October 4, 2006, the Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national exercise program to test and evaluate the national preparedness goal, National Incident Management System, National Response Plan, and other related plans and strategies.

(2) Requirements

The national exercise program—

(A) shall be—

(i) as realistic as practicable, based on current risk assessments, including credible and emerging threats, vulnerabilities, and consequences, and designed to stress the national preparedness system;

(ii) designed, as practicable, to simulate the partial or complete incapacitation of a State, local, or tribal government;

(iii) carried out, as appropriate, with a minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

(iv) designed to provide for the systematic evaluation of readiness and enhance operational understanding of the incident command system and relevant mutual aid agreements;

(v) designed to address the unique requirements of populations with special needs, including the elderly; and

(vi) designed to promptly develop after-action reports and plans for quickly incorporating lessons learned into future operations; and

(B) shall include a selection of model exercises that State, local, and tribal governments can readily adapt for use and provide assistance to State, local, and tribal governments with the design, implementation, and evaluation of exercises (whether a model exercise program or an exercise designed locally) that—

(i) conform to the requirements under subparagraph (A);

(ii) are consistent with any applicable State, local, or tribal strategy or plan; and

(iii) provide for systematic evaluation of readiness.

(3) National level exercises

The Administrator shall periodically, but not less than biennially, perform national exercises for the following purposes:

(A) To test and evaluate the capability of Federal, State, local, and tribal governments to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction.

(B) To test and evaluate the readiness of Federal, State, local, and tribal governments to respond and recover in a coordinated and unified manner to catastrophic incidents.

(Pub. L. 109–295, title VI, §648, Oct. 4, 2006, 120 Stat. 1427; Pub. L. 110–53, title IV, §§402, 403, Aug. 3, 2007, 121 Stat. 302, 303; Pub. L. 116–64, §3, Oct. 9, 2019, 133 Stat. 1123.)

EDITORIAL NOTES

AMENDMENTS

2019—Subsec. (b)(2)(A)(i). Pub. L. 116–64 inserted "and emerging" after "credible".

2007—Subsec. (b)(2)(A)(iv) to (vi). Pub. L. 110–53, §402, added cls. (iv) to (vi) and struck out former cls. (iv) and (v) which read as follows:

"(iv) designed to provide for systematic evaluation of readiness; and

"(v) designed to address the unique requirements of populations with special needs; and".

Subsec. (b)(2)(B). Pub. L. 110–53, §403, in introductory provisions, substituted "shall include a selection of model exercises that State, local, and tribal governments can readily adapt for use and provide assistance to State, local, and tribal governments with the design, implementation, and evaluation of exercises (whether a model exercise program or an exercise designed locally)" for "shall provide assistance to State, local, and tribal governments with the design, implementation, and evaluation of exercises".

§748a. Prioritization of facilities

Not later than 180 days after October 5, 2018, the Administrator shall provide guidance and training on an annual basis to State, local, and Indian tribal governments, first responders, and utility companies on—

(1) the need to prioritize assistance to hospitals, nursing homes, and other long-term care facilities to ensure that such health care facilities remain functioning or return to functioning as soon as practicable during power outages caused by natural hazards, including severe weather events;

(2) how hospitals, nursing homes and other long-term care facilities should adequately prepare for power outages during a major disaster or emergency, as those terms are defined in section 5122 of title 42; and

(3) how State, local, and Indian tribal governments, first responders, utility companies,

hospitals, nursing homes, and other long-term care facilities should develop a strategy to coordinate emergency response plans, including the activation of emergency response plans, in anticipation of a major disaster, including severe weather events.

(Pub. L. 115–254, div. D, §1208, Oct. 5, 2018, 132 Stat. 3441.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Disaster Recovery Reform Act of 2018 and also as part of the FAA Reauthorization Act of 2018, and not as part of the Post-Katrina Emergency Management Reform Act of 2006 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of "Administrator" and "State" as used in this section, see section 1203 of Pub. L. 115–254, set out as a note under section 5122 of Title 42, The Public Health and Welfare.

§749. Comprehensive assessment system

(a) Establishment

The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a comprehensive system to assess, on an ongoing basis, the Nation's prevention capabilities and overall preparedness, including operational readiness.

(b) Performance metrics and measures

The Administrator shall ensure that each component of the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies, and the reports required under section 752 of this title is developed, revised, and updated with clear and quantifiable performance metrics, measures, and outcomes.

(c) Contents

The assessment system established under subsection (a) shall assess—

(1) compliance with the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies;

(2) capability levels at the time of assessment against target capability levels defined pursuant to the guidelines established under section 746(a) of this title;

(3) resource needs to meet the desired target capability levels defined pursuant to the guidelines established under section 746(a) of this title; and

(4) performance of training, exercises, and operations.

(Pub. L. 109–295, title VI, §649, Oct. 4, 2006, 120 Stat. 1428.)

§750. Remedial action management program

The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

(1) analyze training, exercises, and real-world events to identify and disseminate lessons learned and best practices;

(2) generate and disseminate, as appropriate, after action reports to participants in exercises and real-world events; and

(3) conduct remedial action tracking and long-term trend analysis.

(Pub. L. 109–295, title VI, §650, Oct. 4, 2006, 120 Stat. 1428.)

§751. Federal response capability inventory

(a) In general

In accordance with section 5196(h)(1)(C) of title 42, the Administrator shall accelerate the completion of the inventory of Federal response capabilities.

(b) Contents

For each Federal agency with responsibilities under the National Response Plan, the inventory shall include—

(1) for each capability—

(A) the performance parameters of the capability;

(B) the timeframe within which the capability can be brought to bear on an incident; and

(C) the readiness of the capability to respond to all hazards, including natural disasters, acts of terrorism, and other man-made disasters;

(2) a list of personnel credentialed in accordance with section 320 of this title;

(3) a list of resources typed in accordance with section 320 of this title; and

(4) emergency communications assets maintained by the Federal Government and, if appropriate, State, local, and tribal governments and the private sector.

(c) Department of Defense

The Administrator, in coordination with the Secretary of Defense, shall develop a list of organizations and functions within the Department of Defense that may be used, pursuant to the authority provided under the National Response Plan and sections 5170a, 5170b, and 5192 of title 42, to provide support to civil authorities during natural disasters, acts of terrorism, and other man-made disasters.

(d) Database

The Administrator shall establish an inventory database to allow—

(1) real-time exchange of information regarding—

(A) capabilities;

(B) readiness;

(C) the compatibility of equipment;

(D) credentialed personnel; and

(E) typed resources;

(2) easy identification and rapid deployment of capabilities, credentialed personnel, and typed resources during an incident; and

(3) the sharing of the inventory described in subsection (a) with other Federal agencies, as appropriate.

(Pub. L. 109–295, title VI, §651, Oct. 4, 2006, 120 Stat. 1429; Pub. L. 110–53, title IV, §405, Aug. 3, 2007, 121 Stat. 303.)

EDITORIAL NOTES

AMENDMENTS

2007—Subsec. (b). Pub. L. 110–53, §405(1)(A), substituted "For each Federal agency with responsibilities under the National Response Plan, the inventory" for "The inventory" in introductory provisions.

Subsec. (b)(2) to (4). Pub. L. 110–53, §405(1)(B)–(D), added pars. (2) and (3) and redesignated former par. (2) as (4).

Subsec. (d)(1). Pub. L. 110–53, §405(2)(A), substituted "regarding—" for "regarding capabilities, readiness, or the compatibility of equipment;" in introductory provisions and added subpars. (A) to (E).

Subsec. (d)(2). Pub. L. 110–53, §405(2)(B), inserted "of capabilities, credentialed personnel, and typed

resources" after "rapid deployment".

Subsec. (d)(3). Pub. L. 110–53, §405(2)(C), substituted "the inventory described in subsection (a)" for "inventories".

§752. Reporting requirements

(a) Federal preparedness report

(1) In general

Not later than 12 months after October 4, 2006, and annually thereafter, the Administrator, in coordination with the heads of appropriate Federal agencies, shall submit to the appropriate committees of Congress a report on the Nation's level of preparedness for all hazards, including natural disasters, acts of terrorism, and other man-made disasters.

(2) Contents

Each report shall include—

(A) an assessment of how Federal assistance supports the national preparedness system;

(B) the results of the comprehensive assessment carried out under section 749 of this title;

(C) a review of the inventory described in section 751 of this title, including the number and type of credentialed personnel in each category of personnel trained and ready to respond to a natural disaster, act of terrorism, or other man-made disaster;

(D) an assessment of resource needs to meet preparedness priorities established under section 746(e) of this title, including—

(i) an estimate of the amount of Federal, State, local, and tribal expenditures required to attain the preparedness priorities; and

(ii) the extent to which the use of Federal assistance during the preceding fiscal year achieved the preparedness priorities;

(E) an evaluation of the extent to which grants administered by the Department, including grants under title XX of the Homeland Security Act of 2002 [6 U.S.C. 601 et seq.]—

(i) have contributed to the progress of State, local, and tribal governments in achieving target capabilities; and

(ii) have led to the reduction of risk from natural disasters, acts of terrorism, or other man-made disasters nationally and in State, local, and tribal jurisdictions; and

(F) a discussion of whether the list of credentialed personnel of the Agency described in section 751(b)(2) of this title—

(i) complies with the strategic human capital plan developed under section 10102 of title 5; and

(ii) is sufficient to respond to a natural disaster, act of terrorism, or other man-made disaster, including a catastrophic incident.

(b) Catastrophic resource report

(1) In general

The Administrator shall develop and submit to the appropriate committees of Congress annually an estimate of the resources of the Agency and other Federal agencies needed for and devoted specifically to developing the capabilities of Federal, State, local, and tribal governments necessary to respond to a catastrophic incident.

(2) Contents

Each estimate under paragraph (1) shall include the resources both necessary for and devoted to—

(A) planning;

(B) training and exercises;

(C) Regional Office enhancements;

(D) staffing, including for surge capacity during a catastrophic incident;

(E) additional logistics capabilities;

(F) other responsibilities under the catastrophic incident annex and the catastrophic incident supplement of the National Response Plan;

(G) State, local, and tribal government catastrophic incident preparedness; and

(H) covering increases in the fixed costs or expenses of the Agency, including rent or property acquisition costs or expenses, taxes, contributions to the working capital fund of the Department, and security costs for the year after the year in which such estimate is submitted.

(c) State preparedness report

(1) In general

Not later than 15 months after October 4, 2006, and annually thereafter, a State receiving Federal preparedness assistance administered by the Department shall submit a report to the Administrator on the State's level of preparedness.

(2) Contents

Each report shall include—

(A) an assessment of State compliance with the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies;

(B) an assessment of current capability levels and a description of target capability levels; and

(C) a discussion of the extent to which target capabilities identified in the applicable State homeland security plan and other applicable plans remain unmet and an assessment of resources needed to meet the preparedness priorities established under section 746(e) of this title, including—

(i) an estimate of the amount of expenditures required to attain the preparedness priorities; and

(ii) the extent to which the use of Federal assistance during the preceding fiscal year achieved the preparedness priorities.

(Pub. L. 109–295, title VI, §652, Oct. 4, 2006, 120 Stat. 1429; Pub. L. 110–53, title I, §103, title IV, §406, Aug. 3, 2007, 121 Stat. 293, 304.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Homeland Security Act of 2002, referred to in subsec. (a)(2)(E), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135. Title XX of the Act is classified generally to subchapter XV (§601 et seq.) of chapter 1 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2007—Subsec. (a)(2)(C). Pub. L. 110–53, §406(1), substituted "section 751 of this title, including the number and type of credentialed personnel in each category of personnel trained and ready to respond to a natural disaster, act of terrorism, or other man-made disaster" for "section 751(a) of this title".

Subsec. (a)(2)(E). Pub. L. 110–53, §103(a), added subpar. (E).

Subsec. (a)(2)(F). Pub. L. 110–53, §406(2)–(4), added subpar. (F).

Subsec. (c)(2)(C). Pub. L. 110–53, §103(b), which directed amendment of subpar. (D) by substituting "a discussion of the extent to which target capabilities identified in the applicable State homeland security plan and other applicable plans remain unmet and an assessment of resources needed" for "an assessment of resource needs", was executed by making the substitution in subpar. (C) to reflect the probable intent of Congress.

§753. Federal preparedness

(a) Agency responsibility

In support of the national preparedness system, the President shall ensure that each Federal agency with responsibilities under the National Response Plan—

(1) has the operational capability to meet the national preparedness goal, including—

(A) the personnel to make and communicate decisions;

(B) organizational structures that are assigned, trained, and exercised for the missions of the agency;

(C) sufficient physical resources; and

(D) the command, control, and communication channels to make, monitor, and communicate decisions;

(2) complies with the National Incident Management System, including credentialing of personnel and typing of resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster in accordance with section 320 of this title;

(3) develops, trains, and exercises rosters of response personnel to be deployed when the agency is called upon to support a Federal response;

(4) develops deliberate operational plans and the corresponding capabilities, including crisis planning, to respond effectively to natural disasters, acts of terrorism, and other man-made disasters in support of the National Response Plan to ensure a coordinated Federal response; and

(5) regularly updates, verifies the accuracy of, and provides to the Administrator the information in the inventory required under section 751 of this title.

(b) Operational plans

An operations plan developed under subsection (a)(4) shall meet the following requirements:

(1) The operations plan shall be coordinated under a unified system with a common terminology, approach, and framework.

(2) The operations plan shall be developed, in coordination with State, local, and tribal government officials, to address both regional and national risks.

(3) The operations plan shall contain, as appropriate, the following elements:

(A) Concepts of operations.

(B) Critical tasks and responsibilities.

(C) Detailed resource and personnel requirements, together with sourcing requirements.

(D) Specific provisions for the rapid integration of the resources and personnel of the agency into the overall response.

(4) The operations plan shall address, as appropriate, the following matters:

(A) Support of State, local, and tribal governments in conducting mass evacuations, including—

(i) transportation and relocation;

(ii) short- and long-term sheltering and accommodation;

(iii) provisions for populations with special needs, keeping families together, and expeditious location of missing children; and

(iv) policies and provisions for pets.

(B) The preparedness and deployment of public health and medical resources, including resources to address the needs of evacuees and populations with special needs.

(C) The coordination of interagency search and rescue operations, including land, water, and airborne search and rescue operations.

(D) The roles and responsibilities of the Senior Federal Law Enforcement Official with respect to other law enforcement entities.

(E) The protection of critical infrastructure.

(F) The coordination of maritime salvage efforts among relevant agencies.

(G) The coordination of Department of Defense and National Guard support of civilian authorities.

(H) To the extent practicable, the utilization of Department of Defense, National Air and Space Administration, National Oceanic and Atmospheric Administration, and commercial aircraft and satellite remotely sensed imagery.

(I) The coordination and integration of support from the private sector and nongovernmental organizations.

(J) The safe disposal of debris, including hazardous materials, and, when practicable, the recycling of debris.

(K) The identification of the required surge capacity.

(L) Specific provisions for the recovery of affected geographic areas.

(c) Mission assignments

To expedite the provision of assistance under the National Response Plan, the President shall ensure that the Administrator, in coordination with Federal agencies with responsibilities under the National Response Plan, develops prescripted mission assignments, including logistics, communications, mass care, health services, and public safety.

(d) Certification

The President shall certify to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives on an annual basis that each Federal agency with responsibilities under the National Response Plan complies with subsections (a) and (b).

(e) Construction

Nothing in this section shall be construed to limit the authority of the Secretary of Defense with regard to—

(1) the command, control, training, planning, equipment, exercises, or employment of Department of Defense forces; or

(2) the allocation of Department of Defense resources.

(Pub. L. 109–295, title VI, §653, Oct. 4, 2006, 120 Stat. 1430; Pub. L. 110–53, title IV, §407, Aug. 3, 2007, 121 Stat. 304.)

EDITORIAL NOTES

AMENDMENTS

2007—Subsec. (a). Pub. L. 110–53, §407(1)(A), struck out "coordinating, primary, or supporting" before "responsibilities" in introductory provisions.

Subsec. (a)(2). Pub. L. 110–53, §407(1)(B), inserted ", including credentialing of personnel and typing of resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster in accordance with section 320 of this title" before semicolon at end.

Subsec. (a)(5). Pub. L. 110–53, §407(1)(C)–(E), added par. (5).

Subsec. (d). Pub. L. 110–53, §407(2), inserted "to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives" after "certify" and struck out "coordinating, primary, or supporting" before "responsibilities".

§754. Use of existing resources

In establishing the national preparedness goal and national preparedness system, the Administrator shall use existing preparedness documents, planning tools, and guidelines to the extent practicable and consistent with this Act.

(Pub. L. 109–295, title VI, §654, Oct. 4, 2006, 120 Stat. 1432.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in text, means title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1394, known as the Post-Katrina Emergency Management Reform Act of 2006. For complete classification of title VI to the Code, see Short Title note set out under section 701 of this title and Tables.

PART B—ADDITIONAL PREPAREDNESS

§761. Emergency Management Assistance Compact grants

(a) In general

The Administrator may make grants to administer the Emergency Management Assistance Compact consented to by the Joint Resolution entitled "Joint Resolution granting the consent of Congress to the Emergency Management Assistance Compact" (Public Law 104–321; 110 Stat. 3877).

(b) Uses

A grant under this section shall be used—

(1) to carry out recommendations identified in the Emergency Management Assistance Compact after-action reports for the 2004 and 2005 hurricane season;

(2) to administer compact operations on behalf of all member States and territories;

(3) to continue coordination with the Agency and appropriate Federal agencies;

(4) to continue coordination with State, local, and tribal government entities and their respective national organizations; and

(5) to assist State and local governments, emergency response providers, and organizations representing such providers with credentialing emergency response providers and the typing of emergency response resources.

(c) Coordination

The Administrator shall consult with the Administrator of the Emergency Management Assistance Compact to ensure effective coordination of efforts in responding to requests for assistance.

(d) Authorization

There is authorized to be appropriated to carry out this section $4,000,000 for each of fiscal years 2018 through 2022. Such sums shall remain available until expended.

(Pub. L. 109–295, title VI, §661, Oct. 4, 2006, 120 Stat. 1432; Pub. L. 115–254, div. D, §1217(b), Oct. 5, 2018, 132 Stat. 3451.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Joint Resolution entitled "Joint Resolution granting the consent of Congress to the Emergency Management Assistance Compact", referred to in subsec. (a), is Pub. L. 104–321, Oct. 19, 1996, 110 Stat. 3877, which is not classified to the Code.

AMENDMENTS

2018—Subsec. (d). Pub. L. 115–254 substituted "for each of fiscal years 2018 through 2022" for "for fiscal year 2008".

§762. Emergency management performance grants program

(a) Definitions

In this section—

(1) the term "program" means the emergency management performance grants program described in subsection (b); and

(2) the term "State" has the meaning given that term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(b) In general

The Administrator of the Federal Emergency Management Agency shall continue implementation of an emergency management performance grants program, to make grants to States to assist State, local, and tribal governments in preparing for all hazards, as authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(c) Federal share

Except as otherwise specifically provided by title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act [42 U.S.C. 5195 et seq.], the Federal share of the cost of an activity carried out using funds made available under the program shall not exceed 50 percent.

(d) Apportionment

For fiscal year 2008, and each fiscal year thereafter, the Administrator shall apportion the amounts appropriated to carry out the program among the States as follows:

(1) Baseline amount

The Administrator shall first apportion 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands and 0.75 percent of such amounts to each of the remaining States.

(2) Remainder

The Administrator shall apportion the remainder of such amounts in the ratio that—

(A) the population of each State; bears to

(B) the population of all States.

(e) Consistency in allocation

Notwithstanding subsection (d), in any fiscal year before fiscal year 2013 in which the appropriation for grants under this section is equal to or greater than the appropriation for emergency management performance grants in fiscal year 2007, no State shall receive an amount under this section for that fiscal year less than the amount that State received in fiscal year 2007.

(f) Authorization of appropriations

There is authorized to be appropriated to carry out the program, for each of fiscal years 2018 through 2022, $950,000,000.

(Pub. L. 109–295, title VI, §662, Oct. 4, 2006, 120 Stat. 1433; Pub. L. 110–53, title II, §201, Aug. 3, 2007, 121 Stat. 294; Pub. L. 115–254, div. D, §1217(c), Oct. 5, 2018, 132 Stat. 3451.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsecs. (b) and (c), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. Title VI of the Act is classified generally to subchapter IV–B (§5195 et seq.) of chapter 68 of Title 42. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

AMENDMENTS

2018—Subsec. (f). Pub. L. 115–254 substituted "the program, for each of fiscal years 2018 through 2022" for "the program—

"(1) for fiscal year 2008, $400,000,000;
"(2) for fiscal year 2009, $535,000,000;
"(3) for fiscal year 2010, $680,000,000;
"(4) for fiscal year 2011, $815,000,000; and
"(5) for fiscal year 2012".

2007—Pub. L. 110–53 amended section catchline and text generally. Prior to amendment, text read as follows: "There is authorized to be appropriated for the Emergency Management Performance Grants Program for fiscal year 2008, an amount equal to the amount appropriated for the program for fiscal year 2007 and an additional $175,000,000."

§763. Transfer of Noble Training Center

The Noble Training Center is transferred to the Center for Domestic Preparedness. The Center for Domestic Preparedness shall integrate the Noble Training Center into the program structure of the Center for Domestic Preparedness.

(Pub. L. 109–295, title VI, §663, Oct. 4, 2006, 120 Stat. 1433.)

§763a. Training for Federal Government, foreign governments, or private entities

In fiscal year 2013 and thereafter: (a) the Center for Domestic Preparedness may provide training to emergency response providers from the Federal Government, foreign governments, or private entities, if the Center for Domestic Preparedness is reimbursed for the cost of such training, and any reimbursement under this subsection shall be credited to the account from which the expenditure being reimbursed was made and shall be available, without fiscal year limitation, for the purposes for which amounts in the account may be expended; (b) the head of the Center for Domestic Preparedness shall ensure that any training provided under (a) does not interfere with the primary mission of the Center to train State and local emergency response providers; and (c) subject to (b), nothing in (a) prohibits the Center for Domestic Preparedness from providing training to employees of the Federal Emergency Management Agency in existing chemical, biological, radiological, nuclear, explosives, mass casualty, and medical surge courses pursuant to 5 U.S.C. 4103 without reimbursement for the cost of such training.

(Pub. L. 113–6, div. D, title III, Mar. 26, 2013, 127 Stat. 359.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2013, and not as part of the Post-Katrina Emergency Management Reform Act of 2006 which comprises this chapter.

§764. National exercise simulation center

The President shall establish a national exercise simulation center that—

(1) uses a mix of live, virtual, and constructive simulations to—

(A) prepare elected officials, emergency managers, emergency response providers, and emergency support providers at all levels of government to operate cohesively;

(B) provide a learning environment for the homeland security personnel of all Federal agencies;

(C) assist in the development of operational procedures and exercises, particularly those based on catastrophic incidents; and

(D) allow incident commanders to exercise decisionmaking in a simulated environment; and

(2) uses modeling and simulation for training, exercises, and command and control functions at the operational level.

(Pub. L. 109–295, title VI, §664, Oct. 4, 2006, 120 Stat. 1433.)

§765. Real property transactions

(a) Reports to the Armed Services Committees

The Director of the Office of Civil and Defense Mobilization, or his designee, may not enter into any of the following listed transactions by or for the use of that agency until after the expiration of thirty days from the date upon which a report of the facts concerning the proposed transaction is submitted to the Committees on Armed Services of the Senate and House of Representatives:

(1) An acquisition of fee title to any real property, if the estimated price is more than $50,000.

(2) A lease of any real property to the United States, if the estimated annual rental is more than $50,000.

(3) A lease of real property owned by the United States, if the estimated annual rental is more than $50,000.

(4) A transfer of real property owned by the United States to another Federal agency or to a State, if the estimated value is more than $50,000.

(5) A report of excess real property owned by the United States to a disposal agency, if the estimated value is more than $50,000.

If a transaction covered by clause (1) or (2) is part of a project, the report must include a summarization of the general plan for that project, including an estimate of the total cost of the lands to be acquired or leases to be made.

(b) Annual reports to Armed Services Committees

The Director of the Office of Civil and Defense Mobilization shall report annually to the Committees on Armed Services of the Senate and the House of Representatives on transactions described in subsection (a) that involve an estimated value of more than $5,000 but not more than $50,000.

(c) Real property governed by this section

This section applies only to real property in the States of the Union, the District of Columbia, and Puerto Rico. It does not apply to real property for river and harbor projects or flood-control projects, or to leases of Government-owned real property for agricultural or grazing purposes.

(d) Recital of compliance in instrument of conveyance as conclusive

A statement in an instrument of conveyance, including a lease, that the requirements of this section have been met, or that the conveyance is not subject to this section, is conclusive.

(Aug. 10, 1956, ch. 1041, §43, 70A Stat. 636; Pub. L. 86–70, §37, June 25, 1959, 73 Stat. 150; Pub. L. 86–500, title V, §512, June 8, 1960, 74 Stat. 187; Pub. L. 86–624, §38, June 12, 1960, 74 Stat. 421; Pub. L. 96–470, title II, §202(c), Oct. 19, 1980, 94 Stat. 2242.)

EDITORIAL NOTES

CODIFICATION

Section was formerly classified to section 2285 of the former Appendix to Title 50, War and National Defense, prior to editorial reclassification and renumbering as this section.

Prior to classification as section 2285, section was formerly classified to section 171x of Title 5 prior to the general revision and enactment of Title 5, Government Organization and Employees, by Pub. L. 89–554, §1, Sept. 6, 1966, 80 Stat. 378.

Section was enacted as a part of act Aug. 10, 1956, ch. 1041, and not as part of the Post-Katrina Emergency Management Reform Act of 2006 which comprises this chapter.

AMENDMENTS

1980—Subsec. (b). Pub. L. 96–470 substituted "annually" for "quarterly".

1960—Subsec. (a). Pub. L. 86–500 substituted "Director of the Office of Civil and Defense Mobilization" for "Administrator of the Federal Civil Defense Administration", prohibited the Director from entering into any of the transactions listed in subsec. (a) until after the expiration of 30 days from the date upon which a report of the facts concerning the proposed transaction is submitted to the Committees on Armed Services of the Senate and House of Representatives, and increased the amounts in cls. (1) to (5) from $25,000 to $50,000.

Subsec. (b). Pub. L. 86–500 substituted "Director of the Office of Civil and Defense Mobilization" for "Administrator" and "$50,000" for "$25,000".

Subsec. (c). Pub. L. 86–624 substituted "States of the Union, the District of Columbia" for "United States, Hawaii."

Pub. L. 86–500 struck out ", Hawaii," after "United States".

Subsec. (d). Pub. L. 86–500 reenacted subsection without change.

1959—Subsec. (c). Pub. L. 86–70 struck out "Alaska," after "United States,".

STATUTORY NOTES AND RELATED SUBSIDIARIES

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective May 15, 2000, of provisions of law requiring submittal to Congress of any annual, semiannual, or other regular periodic report listed in House Document No. 103–7 (in which a report required under 50 U.S.C. app. 2285(b) (now subsec. (b) of this section) is listed as the 10th item on page 169), see section 3003 of Pub. L. 104–66, as amended, set out as a note under section 1113 of Title 31, Money and Finance.

TRANSFER OF FUNCTIONS

Pub. L. 85–763, Aug. 26, 1958, 72 Stat. 861, amended Reorg. Plan No. 1 of 1958 by redesignating Office of Defense and Civilian Mobilization as Office of Civil and Defense Mobilization.

Pub. L. 87–296, Sept. 22, 1961, 75 Stat. 630, amended Reorg. Plan No. 1 of 1958 by redesignating Office of Civil and Defense Mobilization as Office of Emergency Planning.

Office of Emergency Planning renamed Office of Emergency Preparedness pursuant to section 402 of Pub. L. 90–608, Oct. 21, 1968, 82 Stat. 1194, which provided that references to Office of Emergency Planning after Oct. 21, 1968, should be deemed references to Office of Emergency Preparedness.

For transfer of all functions, personnel, assets, components, authorities, grant programs, and liabilities of the Federal Emergency Management Agency, including the functions of the Under Secretary for Federal Emergency Management relating thereto, to the Federal Emergency Management Agency, see section 315(a)(1) of this title.

For transfer of functions, personnel, assets, and liabilities of the Federal Emergency Management Agency, including the functions of the Director of the Federal Emergency Management Agency relating thereto, to the Secretary of Homeland Security, and for treatment of related references, see former section 313(1) and sections 551(d), 552(d), and 557 of this title, and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of this title.

EXECUTIVE DOCUMENTS

TRANSFER OF FUNCTIONS

Functions of Federal Civil Defense Administration transferred to President by section 1 of Reorg. Plan No. 1 of 1958, eff. July 1, 1958, 23 F.R. 4991, 72 Stat. 1799, as amended, set out as a note under section 5195 of Title 42, The Public Health and Welfare. The Plan created a new agency in Executive Office of President known as Office of Defense and Civilian Mobilization.

Office of Emergency Preparedness, including offices of Director, Deputy Director, Assistant Directors, and Regional Directors, abolished and functions vested by law in Office of Emergency Preparedness or Director of Office of Emergency Preparedness transferred to President by sections 1 and 3(a)(1) of Reorg. Plan No. 1 of 1973, eff. July 1, 1973, 38 F.R. 9579, 87 Stat. 1089, set out as a note under section 5195 of Title 42, The Public Health and Welfare.

Functions vested in Director of Office of Emergency Preparedness as of June 30, 1973, by Executive Order, proclamation, or other directive issued by or on behalf of President or otherwise, with certain exceptions,

transferred to Administrator of General Services, effective July 1, 1973, by Ex. Ord. No. 11725, §3, eff. June 29, 1973, 38 F.R. 17175, formerly set out as a note under section 2271 of the former Appendix to Title 50, War and National Defense.

Functions of Administrator of Federal Civil Defense Administration under this section, previously transferred to President, delegated to Director of Federal Emergency Management Agency by section 4–105 of Ex. Ord. No. 12148, July 20, 1979, 44 F.R. 43242, set out as a note under section 5195 of Title 42, The Public Health and Welfare.

PART C—MISCELLANEOUS AUTHORITIES

§771. National Disaster Recovery Strategy

(a) In general

The Administrator, in coordination with the Secretary of Housing and Urban Development, the Administrator of the Environmental Protection Agency, the Secretary of Agriculture, the Secretary of Commerce, the Secretary of the Treasury, the Secretary of Transportation, the Administrator of the Small Business Administration, the Assistant Secretary for Indian Affairs of the Department of the Interior, and the heads of other appropriate Federal agencies, State, local, and tribal government officials (including through the National Advisory Council), and representatives of appropriate nongovernmental organizations shall develop, coordinate, and maintain a National Disaster Recovery Strategy to serve as a guide to recovery efforts after major disasters and emergencies.

(b) Contents

The National Disaster Recovery Strategy shall—

(1) outline the most efficient and cost-effective Federal programs that will meet the recovery needs of States, local and tribal governments, and individuals and households affected by a major disaster;

(2) clearly define the role, programs, authorities, and responsibilities of each Federal agency that may be of assistance in providing assistance in the recovery from a major disaster;

(3) promote the use of the most appropriate and cost-effective building materials (based on the hazards present in an area) in any area affected by a major disaster, with the goal of encouraging the construction of disaster-resistant buildings; and

(4) describe in detail the programs that may be offered by the agencies described in paragraph (2), including—

(A) discussing funding issues;

(B) detailing how responsibilities under the National Disaster Recovery Strategy will be shared; and

(C) addressing other matters concerning the cooperative effort to provide recovery assistance.

(c) Report

(1) In general

Not later than 270 days after October 4, 2006, the Administrator shall submit to the appropriate committees of Congress a report describing in detail the National Disaster Recovery Strategy and any additional authorities necessary to implement any portion of the National Disaster Recovery Strategy.

(2) Update

The Administrator shall submit to the appropriate committees of Congress a report updating the report submitted under paragraph (1)—

(A) on the same date that any change is made to the National Disaster Recovery Strategy; and

(B) on a periodic basis after the submission of the report under paragraph (1), but not less than once every 5 years after the date of the submission of the report under paragraph (1).

(Pub. L. 109–295, title VI, §682, Oct. 4, 2006, 120 Stat. 1445.)

§772. National Disaster Housing Strategy

(a) In general

The Administrator, in coordination with representatives of the Federal agencies, governments, and organizations listed in subsection (b)(2) of this section, the National Advisory Council, the National Council on Disability, and other entities at the Administrator's discretion, shall develop, coordinate, and maintain a National Disaster Housing Strategy.

(b) Contents

The National Disaster Housing Strategy shall—

(1) outline the most efficient and cost effective Federal programs that will best meet the short-term and long-term housing needs of individuals and households affected by a major disaster;

(2) clearly define the role, programs, authorities, and responsibilities of each entity in providing housing assistance in the event of a major disaster, including—

(A) the Agency;

(B) the Department of Housing and Urban Development;

(C) the Department of Agriculture;

(D) the Department of Veterans Affairs;

(E) the Department of Health and Human Services;

(F) the Bureau of Indian Affairs;

(G) any other Federal agency that may provide housing assistance in the event of a major disaster;

(H) the American Red Cross; and

(I) State, local, and tribal governments;

(3) describe in detail the programs that may be offered by the entities described in paragraph (2), including—

(A) outlining any funding issues;

(B) detailing how responsibilities under the National Disaster Housing Strategy will be shared; and

(C) addressing other matters concerning the cooperative effort to provide housing assistance during a major disaster;

(4) consider methods through which housing assistance can be provided to individuals and households where employment and other resources for living are available;

(5) describe programs directed to meet the needs of special needs and low-income populations and ensure that a sufficient number of housing units are provided for individuals with disabilities;

(6) describe plans for the operation of clusters of housing provided to individuals and households, including access to public services, site management, security, and site density;

(7) describe plans for promoting the repair or rehabilitation of existing rental housing, including through lease agreements or other means, in order to improve the provision of housing to individuals and households under section 408 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5174); and

(8) describe any additional authorities necessary to carry out any portion of the strategy.

(c) Guidance

The Administrator should develop and make publicly available guidance on—

(1) types of housing assistance available under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) to individuals and households affected by an emergency or major disaster;

(2) eligibility for such assistance (including, where appropriate, the continuation of such assistance); and

(3) application procedures for such assistance.

(d) Report

(1) In general

Not later than 270 days after October 4, 2006, the Administrator shall submit to the appropriate committees of Congress a report describing in detail the National Disaster Housing Strategy, including programs directed to meeting the needs of special needs populations.

(2) Updated report

The Administrator shall submit to the appropriate committees of Congress a report updating the report submitted under paragraph (1)—

(A) on the same date that any change is made to the National Disaster Housing Strategy; and

(B) on a periodic basis after the submission of the report under paragraph (1), but not less than once every 5 years after the date of the submission of the report under paragraph (1).

(Pub. L. 109–295, title VI, §683, Oct. 4, 2006, 120 Stat. 1446.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (c)(1), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

§773. Individuals with disabilities guidelines

Not later than 90 days after October 4, 2006, and in coordination with the National Advisory Council, the National Council on Disability, the Interagency Coordinating Council on Preparedness and Individuals With Disabilities established under Executive Order No. 13347, and the Disability Coordinator (established under section 321b of this title), the Administrator shall develop guidelines to accommodate individuals with disabilities, which shall include guidelines for—

(1) the accessibility of, and communications and programs in, shelters, recovery centers, and other facilities; and

(2) devices used in connection with disaster operations, including first aid stations, mass feeding areas, portable payphone stations, portable toilets, and temporary housing.

(Pub. L. 109–295, title VI, §689(a), Oct. 4, 2006, 120 Stat. 1448.)

EDITORIAL NOTES

REFERENCES IN TEXT

Executive Order No. 13347, referred to in text, is set out as a note under section 314 of this title.

§774. Reunification

(a) Definitions

In this section:

(1) Child Locator Center

The term "Child Locator Center" means the National Emergency Child Locator Center established under subsection (b).

(2) Declared event

The term "declared event" means a major disaster or emergency.

(3) Displaced adult

The term "displaced adult" means an individual 21 years of age or older who is displaced from the habitual residence of that individual as a result of a declared event.

(4) Displaced child

The term "displaced child" means an individual under 21 years of age who is displaced from the habitual residence of that individual as a result of a declared event.

(b) National Emergency Child Locator Center

(1) In general

Not later than 180 days after October 4, 2006, the Administrator, in coordination with the Attorney General of the United States, shall establish within the National Center for Missing and Exploited Children the National Emergency Child Locator Center. In establishing the National Emergency Child Locator Center, the Administrator shall establish procedures to make all relevant information available to the National Emergency Child Locator Center in a timely manner to facilitate the expeditious identification and reunification of children with their families.

(2) Purposes

The purposes of the Child Locator Center are to—

(A) enable individuals to provide to the Child Locator Center the name of and other identifying information about a displaced child or a displaced adult who may have information about the location of a displaced child;

(B) enable individuals to receive information about other sources of information about displaced children and displaced adults; and

(C) assist law enforcement in locating displaced children.

(3) Responsibilities and duties

The responsibilities and duties of the Child Locator Center are to—

(A) establish a toll-free telephone number to receive reports of displaced children and information about displaced adults that may assist in locating displaced children;

(B) create a website to provide information about displaced children;

(C) deploy its staff to the location of a declared event to gather information about displaced children;

(D) assist in the reunification of displaced children with their families;

(E) provide information to the public about additional resources for disaster assistance;

(F) work in partnership with Federal, State, and local law enforcement agencies;

(G) provide technical assistance in locating displaced children;

(H) share information on displaced children and displaced adults with governmental agencies and nongovernmental organizations providing disaster assistance;

(I) use its resources to gather information about displaced children;

(J) refer reports of displaced adults to—

(i) an entity designated by the Attorney General to provide technical assistance in locating displaced adults; and

(ii) the National Emergency Family Registry and Locator System as defined under section 775(a) of this title;

(K) enter into cooperative agreements with Federal and State agencies and other organizations such as the American Red Cross as necessary to implement the mission of the Child Locator Center; and

(L) develop an emergency response plan to prepare for the activation of the Child Locator Center.

(c) Omitted

(d) Report

Not later than 270 days after October 4, 2006, the Administrator shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Transportation and Infrastructure and the Committee on the Judiciary of the House of Representatives a report describing in detail the status of the Child Locator Center, including funding issues and any difficulties or issues in establishing the Center or completing the cooperative agreements described in subsection (b)(3)(K).

(Pub. L. 109–295, title VI, §689b, Oct. 4, 2006, 120 Stat. 1449.)

EDITORIAL NOTES

CODIFICATION

Section is comprised of section 689b of Pub. L. 109–295. Subsec. (c) of section 689b of Pub. L. 109–295 amended section 11292 of Title 34, Crime Control and Law Enforcement.

§775. National Emergency Family Registry and Locator System

(a) Definitions

In this section—

(1) the term "displaced individual" means an individual displaced by an emergency or major disaster; and

(2) the term "National Emergency Family Registry and Locator System" means the National Emergency Family Registry and Locator System established under subsection (b).

(b) Establishment

Not later than 180 days after October 4, 2006, the Administrator shall establish a National Emergency Family Registry and Locator System to help reunify families separated after an emergency or major disaster.

(c) Operation of System

The National Emergency Family Registry and Locator System shall—

(1) allow a displaced adult (including medical patients) to voluntarily register (and allow an adult that is the parent or guardian of a displaced child to register such child), by submitting personal information to be entered into a database (such as the name, current location of residence, and any other relevant information that could be used by others seeking to locate that individual);

(2) ensure that information submitted under paragraph (1) is accessible to those individuals named by a displaced individual and to those law enforcement officials;

(3) be accessible through the Internet and through a toll-free number, to receive reports of displaced individuals; and

(4) include a means of referring displaced children to the National Emergency Child Locator Center established under section 774 of this title.

(d) Publication of information

Not later than 210 days after October 4, 2006, the Administrator shall establish a mechanism to inform the public about the National Emergency Family Registry and Locator System and its potential usefulness for assisting to reunite displaced individuals with their families.

(e) Coordination

Not later than 90 days after October 4, 2006, the Administrator shall enter a memorandum of understanding with the Department of Justice, the National Center for Missing and Exploited

Children, the Department of Health and Human Services, and the American Red Cross and other relevant private organizations that will enhance the sharing of information to facilitate reuniting displaced individuals (including medical patients) with their families.

(f) Report

Not later than 270 days after October 4, 2006, the Administrator shall submit to the appropriate committees of Congress a report describing in detail the status of the National Emergency Family Registry and Locator System, including any difficulties or issues in establishing the System, including funding issues.

(Pub. L. 109–295, title VI, §689c, Oct. 4, 2006, 120 Stat. 1451.)

§776. Individuals and households pilot program

(a) Pilot program

(1) In general

The President, acting through the Administrator, in coordination with State, local, and tribal governments, shall establish and conduct a pilot program. The pilot program shall be designed to make better use of existing rental housing, located in areas covered by a major disaster declaration, in order to provide timely and cost-effective temporary housing assistance to individuals and households eligible for assistance under section 5174 of title 42 where alternative housing options are less available or less cost-effective.

(2) Administration

(A) In general

For the purposes of the pilot program under this section, the Administrator may—

(i) enter into lease agreements with owners of multi-family rental property located in areas covered by a major disaster declaration to house individuals and households eligible for assistance under section 5174 of title 42;

(ii) make improvements to properties under such lease agreements;

(iii) use the pilot program where the program is cost effective in that the cost to the Government for the lease agreements is in proportion to the savings to the Government by not providing alternative housing; and

(iv) limit repairs to those required to ensure that the housing units shall meet Federal housing quality standards.

(B) Improvements to leased properties

Under the terms of any lease agreement for a property described under subparagraph (A)(ii), the value of the contribution of the Agency to such improvements—

(i) shall be deducted from the value of the lease agreement; and

(ii) may not exceed the value of the lease agreement.

(3) Consultation

In administering the pilot program under this section, the Administrator may consult with State, local, and tribal governments.

(4) Report

(A) In general

Not later than March 31, 2009, the Administrator shall submit to the appropriate committees of Congress a report regarding the effectiveness of the pilot program.

(B) Contents

The Administrator shall include in the report—

(i) an assessment of the effectiveness of the pilot program under this section, including an

assessment of cost-savings to the Federal Government and any benefits to individuals and households eligible for assistance under section 5174 of title 42 under the pilot program;

(ii) findings and conclusions of the Administrator with respect to the pilot program;

(iii) an assessment of additional authorities needed to aid the Agency in its mission of providing disaster housing assistance to individuals and households eligible for assistance under section 5174 of title 42, either under the pilot program under this section or other potential housing programs; and

(iv) any recommendations of the Administrator for additional authority to continue or make permanent the pilot program.

(b) Pilot program project approval

The Administrator shall not approve a project under the pilot program after December 31, 2008.

(Pub. L. 109–295, title VI, §689i, Oct. 4, 2006, 120 Stat. 1454.)

§777. Public assistance pilot program

(a) Pilot program

(1) In general

The President, acting through the Administrator, and in coordination with State and local governments, shall establish and conduct a pilot program to—

(A) reduce the costs to the Federal Government of providing assistance to States and local governments under sections 5170b(a)(3)(A), 5172, and 5173 of title 42;

(B) increase flexibility in the administration of sections 5170b(a)(3)(A), 5172, and 5173 of title 42; and

(C) expedite the provision of assistance to States and local governments provided under sections 5170b(a)(3)(A), 5172, and 5173 of title 42.

(2) Participation

Only States and local governments that elect to participate in the pilot program may participate in the pilot program for a particular project.

(3) Innovative administration

(A) In general

For purposes of the pilot program, the Administrator shall establish new procedures to administer assistance provided under the sections referred to in paragraph (1).

(B) New procedures

The new procedures established under subparagraph (A) may include 1 or more of the following:

(i) Notwithstanding section 5172(c)(1)(A) of title 42, providing an option for a State or local government to elect to receive an in-lieu contribution in an amount equal to 90 percent of the Federal share of the Federal estimate of the cost of repair, restoration, reconstruction, or replacement of a public facility owned or controlled by the State or local government and of management expenses.

(ii) Making grants on the basis of estimates agreed to by the local government (or where no local government is involved, by the State government) and the Administrator to provide financial incentives and disincentives for the local government (or where no local government is involved, for the State government) for the timely or cost effective completion of projects under sections 5170b(a)(3)(A), 5172, and 5173 of title 42.

(iii) Increasing the Federal share for removal of debris and wreckage for States and local governments that have a debris management plan approved by the Administrator and have pre-qualified 1 or more debris and wreckage removal contractors before the date of declaration of the major disaster.

(iv) Using a sliding scale for the Federal share for removal of debris and wreckage based on the time it takes to complete debris and wreckage removal.

(v) Using a financial incentive to recycle debris.

(vi) Reimbursing base wages for employees and extra hires of a State or local government involved in or administering debris and wreckage removal.

(4) Waiver

The Administrator may waive such regulations or rules applicable to the provisions of assistance under the sections referred to in paragraph (1) as the Administrator determines are necessary to carry out the pilot program under this section.

(b) Report

(1) In general

Not later than March 31, 2009, the Administrator shall submit to the appropriate committees of Congress a report regarding the effectiveness of the pilot program under this section.

(2) Contents

The report submitted under paragraph (1) shall include—

(A) an assessment by the Administrator of any administrative or financial benefits of the pilot program;

(B) an assessment by the Administrator of the effect, including any savings in time and cost, of the pilot program;

(C) any identified legal or other obstacles to increasing the amount of debris recycled after a major disaster;

(D) any other findings and conclusions of the Administrator with respect to the pilot program; and

(E) any recommendations of the Administrator for additional authority to continue or make permanent the pilot program.

(c) Deadline for initiation of implementation

The Administrator shall initiate implementation of the pilot program under this section not later than 90 days after October 4, 2006.

(d) Pilot program project duration

The Administrator may not approve a project under the pilot program under this section after December 31, 2008.

(Pub. L. 109–295, title VI, §689j, Oct. 4, 2006, 120 Stat. 1455.)

PART D—PREVENTION OF FRAUD, WASTE, AND ABUSE

§791. Advance contracting

(a) Initial report

(1) In general

Not later than 180 days after October 4, 2006, the Administrator shall submit a report under paragraph (2) identifying—

(A) recurring disaster response requirements, including specific goods and services, for which the Agency is capable of contracting for in advance of a natural disaster or act of terrorism or other man-made disaster in a cost effective manner;

(B) recurring disaster response requirements, including specific goods and services, for which the Agency can not contract in advance of a natural disaster or act of terrorism or other

man-made disaster in a cost effective manner; and

(C) a contracting strategy that maximizes the use of advance contracts to the extent practical and cost-effective.

(2) Submission

The report under paragraph (1) shall be submitted to the appropriate committees of Congress.

(b) Entering into contracts

(1) In general

Not later than 1 year after October 4, 2006, the Administrator shall enter into 1 or more contracts for each type of goods or services identified under subsection (a)(1)(A), and in accordance with the contracting strategy identified in subsection (a)(1)(C). Any contract for goods or services identified in subsection (a)(1)(A) previously awarded may be maintained in fulfilling this requirement.

(2) Considered factors

Before entering into any contract under this subsection, the Administrator shall consider section 5150 of title 42.

(3) Prenegotiated Federal contracts for goods and services

The Administrator, in coordination with State and local governments and other Federal agencies, shall establish a process to ensure that Federal prenegotiated contracts for goods and services are coordinated with State and local governments, as appropriate.

(4) Prenegotiated State and local contracts for goods and services

The Administrator shall encourage State and local governments to establish prenegotiated contracts with vendors for goods and services in advance of natural disasters and acts of terrorism or other man-made disasters.

(c) Maintenance of contracts

After the date described under subsection (b), the Administrator shall have the responsibility to maintain contracts for appropriate levels of goods and services in accordance with subsection (a)(1)(C).

(d) Report on contracts not using competitive procedures

At the end of each fiscal quarter, beginning with the first fiscal quarter occurring at least 90 days after October 4, 2006, the Administrator shall submit a report on each disaster assistance contract entered into by the Agency by other than competitive procedures to the appropriate committees of Congress.

(e) Updated report

Not later than 180 days after December 31, 2020, the Administrator shall submit to the appropriate committees of Congress an updated report that contains—

(1) the information required in the initial report under subparagraphs (A) and (B) of subsection (a)(1); and

(2) an updated strategy described in subsection (a)(1)(C) that clearly defines—

(A) the objectives of advance contracts;

(B) how advance contracts contribute to disaster response operations of the Agency;

(C) how to maximize the award of advance contracts to small business concerns, as defined in section 632 of title 15; and

(D) whether and how advance contracts should be prioritized in relation to new post-disaster contract awards.

(f) Additional Duties of the Administrator

(1) Head of contracting

The Administrator shall ensure that the head of contracting activity of the Agency—

(A) not later than 270 days after December 31, 2020, updates the Disaster Contracting Desk Guide of the Agency to provide specific guidance—

(i) on whether and under what circumstances contracting officers should consider using existing advance contracts entered into in accordance with this section prior to making new post-disaster contract awards, and include this guidance in existing semi-annual training given to contracting officers; and

(ii) for contracting officers to perform outreach to State and local governments on the potential benefits of establishing their own pre-negotiated advance contracts;

(B) adheres to hard copy contract file management requirements in effect to ensure that the files relating to advance contracts entered into in accordance with this section are complete and up to date, whether the files will be transferred into the Electronic Contract Filing System of the Agency or remain in hard copy format;

(C) notifies contracting officers of the 3-day time frame requirement for entering completed award documentation into the contract writing system of the Agency when executing notice to proceed documentation;

(D) not later than 180 days after December 31, 2020, revises the reporting methodology of the Agency to ensure that all disaster contracts are included in each quarterly report submitted to the appropriate congressional committees under this section on disaster contract actions;

(E) identifies a single centralized resource listing advance contracts entered into under this section and ensures that source is current and up to date and includes all available advance contracts; and

(F) communicates complete and up-to-date information on available advance contracts to State and local governments to inform their advance contracting efforts.

(2) Master acquisition planning schedule

Not later than 180 days after December 31, 2020, the Administrator shall update and implement guidance for program office and acquisition personnel of the Agency to—

(A) identify acquisition planning time frames and considerations across the entire acquisition planning process of the Agency; and

(B) clearly communicate the purpose and use of a master acquisition planning schedule.

(Pub. L. 109–295, title VI, §691, Oct. 4, 2006, 120 Stat. 1457; Pub. L. 116–272, §3(a), Dec. 31, 2020, 134 Stat. 3349.)

EDITORIAL NOTES

AMENDMENTS

2020—Subsecs. (e), (f). Pub. L. 116–272 added subsecs. (e) and (f).

STATUTORY NOTES AND RELATED SUBSIDIARIES

FINDINGS

Pub. L. 116–272, §2, Dec. 31, 2020, 134 Stat. 3349, provided that:

"Congress finds that—

"(1) the Post-Katrina Emergency Management and Reform Act of 2006 [Post-Katrina Emergency Management Reform Act of 2006] (Public Law 109–925 [Pub. L. 109–295, title VI]; 120 Stat. 1394) required the Federal Emergency Management Agency to establish advance contracts, which are established prior to disasters and are typically needed to quickly provide life-sustaining goods and services in the immediate aftermath of a disaster;

"(2) the catastrophic hurricanes and wildfires in the United States in 2017 highlighted the importance of these advance contracts in disaster response;

"(3) in a report issued by the Government Accountability Office entitled '2017 Disaster Contracting: Action Needed to Better Ensure More Effective Use and Management of Advance Contracts', the Government Accountability Office identified a number of challenges with advance contracts and

recommended actions to improve management by the Federal Emergency Management Agency of these contracts for future disasters; and

"(4) section 691 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 791) should be amended to incorporate the recommendations made by the report described in paragraph (3) to ensure more effective use and management of advance contracts."

REPORT

Pub. L. 116–272, §3(b), Dec. 31, 2020, 134 Stat. 3351, provided that: "The Administrator of the Federal Emergency Management Agency shall regularly update the appropriate committees of Congress (as defined in section 602 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 701)) on the progress of the Federal Emergency Management Agency in implementing the recommendations of the Government Accountability Office in the report entitled '2017 Disaster Contracting: Action Needed to Better Ensure More Effective Use and Management of Advance Contracts', as required under section 691 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 791), as amended by subsection (a)."

§792. Repealed. Pub. L. 117–253, §1, Dec. 20, 2022, 136 Stat. 2360

Section, Pub. L. 109–295, title VI, §692, Oct. 4, 2006, 120 Stat. 1458, related to limitations on tiering of subcontractors.

§793. Oversight and accountability of Federal disaster expenditures

(a) Authority of Administrator to designate funds for oversight activities

The Administrator may designate up to 1 percent of the total amount provided to a Federal agency for a mission assignment as oversight funds to be used by the recipient agency for performing oversight of activities carried out under the Agency reimbursable mission assignment process. Such funds shall remain available until expended.

(b) Use of funds

(1) Types of oversight activities

Oversight funds may be used for the following types of oversight activities related to Agency mission assignments:

(A) Monitoring, tracking, and auditing expenditures of funds.

(B) Ensuring that sufficient management and internal control mechanisms are available so that Agency funds are spent appropriately and in accordance with all applicable laws and regulations.

(C) Reviewing selected contracts and other activities.

(D) Investigating allegations of fraud involving Agency funds.

(E) Conducting and participating in fraud prevention activities with other Federal, State, and local government personnel and contractors.

(2) Plans and reports

Oversight funds may be used to issue the plans required under subsection (e) and the reports required under subsection (f).

(c) Restriction on use of funds

Oversight funds may not be used to finance existing agency oversight responsibilities related to direct agency appropriations used for disaster response, relief, and recovery activities.

(d) Methods of oversight activities

(1) In general

Oversight activities may be carried out by an agency under this section either directly or by contract. Such activities may include evaluations and financial and performance audits.

(2) Coordination of oversight activities

To the extent practicable, evaluations and audits under this section shall be performed by the inspector general of the agency.

(e) Development of oversight plans

(1) In general

If an agency receives oversight funds for a fiscal year, the head of the agency shall prepare a plan describing the oversight activities for disaster response, relief, and recovery anticipated to be undertaken during the subsequent fiscal year.

(2) Selection of oversight activities

In preparing the plan, the head of the agency shall select oversight activities based upon a risk assessment of those areas that present the greatest risk of fraud, waste, and abuse.

(3) Schedule

The plan shall include a schedule for conducting oversight activities, including anticipated dates of completion.

(f) Federal disaster assistance accountability reports

A Federal agency receiving oversight funds under this section shall submit annually to the Administrator and the appropriate committees of Congress a consolidated report regarding the use of such funds, including information summarizing oversight activities and the results achieved.

(g) Definition

In this section, the term "oversight funds" means funds referred to in subsection (a) that are designated for use in performing oversight activities.

(Pub. L. 109–295, title VI, §693, Oct. 4, 2006, 120 Stat. 1458.)

§794. Limitation on length of certain noncompetitive contracts

(a) Regulations

The Secretary shall promulgate regulations applicable to contracts described in subsection (c) to restrict the contract period of any such contract entered into using procedures other than competitive procedures pursuant to the exception provided in paragraph (2) of section 3304(a) of title 41 to the minimum contract period necessary—

(1) to meet the urgent and compelling requirements of the work to be performed under the contract; and

(2) to enter into another contract for the required goods or services through the use of competitive procedures.

(b) Specific contract period

The regulations promulgated under subsection (a) shall require the contract period to not to exceed [1] 150 days, unless the Secretary determines that exceptional circumstances apply.

(c) Covered contracts

This section applies to any contract in an amount greater than the simplified acquisition threshold (as defined by section 134 of title 41) entered into by the Department to facilitate response to or recovery from a natural disaster, act of terrorism, or other man-made disaster.

(Pub. L. 109–295, title VI, §695, Oct. 4, 2006, 120 Stat. 1460.)

EDITORIAL NOTES

CODIFICATION

In subsec. (a), "paragraph (2) of section 3304(a) of title 41" substituted for "paragraph (2) of section 303(c) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(c))" on authority of Pub. L.

111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

In subsec. (c), "section 134 of title 41" substituted for "section 4 of the Office of Federal Procurement Policy Act (41 U.S.C. 403)" on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

[1] *So in original. Probably should be "period not to exceed".*

§795. Fraud, waste, and abuse controls

(a) In general

The Administrator shall ensure that—

(1) all programs within the Agency administering Federal disaster relief assistance develop and maintain proper internal management controls to prevent and detect fraud, waste, and abuse;

(2) application databases used by the Agency to collect information on eligible recipients must record disbursements;

(3) such tracking is designed to highlight and identify ineligible applications; and

(4) the databases used to collect information from applications for such assistance must be integrated with disbursements and payment records.

(b) Audits and reviews required

The Administrator shall ensure that any database or similar application processing system for Federal disaster relief assistance programs administered by the Agency undergoes a review by the Inspector General of the Agency to determine the existence and implementation of such internal controls required under this section and the amendments made by this section.

(Pub. L. 109–295, title VI, §696, Oct. 4, 2006, 120 Stat. 1460.)

EDITORIAL NOTES

REFERENCES IN TEXT

For the amendments made by this section, referred to in subsec. (b), see Codification note below.

CODIFICATION

Section is comprised of section 696 of Pub. L. 109–295. Subsec. (c) of section 696 of Pub. L. 109–295 amended section 5174 of Title 42, The Public Health and Welfare.

§796. Registry of disaster response contractors

(a) Definitions

In this section—

(1) the term "registry" means the registry created under subsection (b); and

(2) the terms "small business concern", "small business concern owned and controlled by socially and economically disadvantaged individuals", "small business concern owned and controlled by women", and "small business concern owned and controlled by service-disabled veterans" have the meanings given those terms under the Small Business Act (15 U.S.C. 631 et seq.).

(b) Registry

(1) In general

The Administrator shall establish and maintain a registry of contractors who are willing to perform debris removal, distribution of supplies, reconstruction, and other disaster or emergency relief activities.

(2) Contents

The registry shall include, for each business concern—

(A) the name of the business concern;

(B) the location of the business concern;

(C) the area served by the business concern;

(D) the type of good or service provided by the business concern;

(E) the bonding level of the business concern; and

(F) whether the business concern is—

(i) a small business concern;

(ii) a small business concern owned and controlled by socially and economically disadvantaged individuals;

(iii) a small business concern owned and controlled by women; or

(iv) a small business concern owned and controlled by service-disabled veterans.

(3) Source of information

(A) Submission

Information maintained in the registry shall be submitted on a voluntary basis and be kept current by the submitting business concerns.

(B) Attestation

Each business concern submitting information to the registry shall submit—

(i) an attestation that the information is true; and

(ii) documentation supporting such attestation.

(C) Verification

The Administrator shall verify that the documentation submitted by each business concern supports the information submitted by that business concern.

(4) Availability of registry

The registry shall be made generally available on the Internet site of the Agency.

(5) Consultation of registry

As part of the acquisition planning for contracting for debris removal, distribution of supplies in a disaster, reconstruction, and other disaster or emergency relief activities, a Federal agency shall consult the registry.

(Pub. L. 109–295, title VI, §697, Oct. 4, 2006, 120 Stat. 1461.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Small Business Act, referred to in subsec. (a)(2), is Pub. L. 85–536, §2(1 et seq.), July 18, 1958, 72 Stat. 384, which is classified generally to chapter 14A (§631 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 631 of Title 15 and Tables.

§797. Fraud prevention training program

The Administrator shall develop and implement a program to provide training on the prevention of waste, fraud, and abuse of Federal disaster relief assistance relating to the response to or recovery from natural disasters and acts of terrorism or other man-made disasters and ways to identify such potential waste, fraud, and abuse.

(Pub. L. 109–295, title VI, §698, Oct. 4, 2006, 120 Stat. 1462.)

PART E—AUTHORIZATION OF APPROPRIATIONS

§811. Authorization of appropriations

There are authorized to be appropriated to carry out this title [1] and the amendments made by this title for the administration and operations of the Agency—

(1) for fiscal year 2008, an amount equal to the amount appropriated for fiscal year 2007 for administration and operations of the Agency, multiplied by 1.1;

(2) for fiscal year 2009, an amount equal to the amount described in paragraph (1), multiplied by 1.1; and

(3) for fiscal year 2010, an amount equal to the amount described in paragraph (2), multiplied by 1.1.

(Pub. L. 109–295, title VI, §699, Oct. 4, 2006, 120 Stat. 1462.)

EDITORIAL NOTES

REFERENCES IN TEXT

This title, referred to in text, is title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1355, known as the Post-Katrina Emergency Management Reform Act of 2006. For complete classification of title VI to the Code, see Short Title note set out under section 701 of this title and Tables.

[1] *See References in Text note below.*

PART F—GLOBAL CATASTROPHIC RISK MANAGEMENT

EDITORIAL NOTES

CODIFICATION

Part was enacted as part of the Global Catastrophic Risk Management Act of 2022 and also as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not part of the Post-Katrina Emergency Management Reform Act of 2006 which comprises this chapter.

§821. Definitions

In this part:

(1) Administrator

The term "Administrator" means the Administrator of the Federal Emergency Management Agency.

(2) Basic need

The term "basic need"—

(A) means any good, service, or activity necessary to protect the health, safety, and general welfare of the civilian population of the United States; and

(B) includes—

(i) food;

(ii) water;

(iii) shelter;

(iv) basic communication services;

(v) basic sanitation and health services; and

(vi) public safety.

(3) Catastrophic incident

The term "catastrophic incident"—

(A) means any natural or man-made disaster that results in extraordinary levels of casualties or damage, mass evacuations, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions in an area; and

(B) may include an incident—

(i) with a sustained national impact over a prolonged period of time;

(ii) that may rapidly exceed resources available to State and local government and private sector authorities in the impacted area; or

(iii) that may significantly interrupt governmental operations and emergency services to such an extent that national security could be threatened.

(4) Critical infrastructure

The term "critical infrastructure" has the meaning given such term in section 5195c(e) of title 42.

(5) Existential risk

The term "existential risk" means the potential for an outcome that would result in human extinction.

(6) Global catastrophic risk

The term "global catastrophic risk" means the risk of events or incidents consequential enough to significantly harm or set back human civilization at the global scale.

(7) Global catastrophic and existential threats

The term "global catastrophic and existential threats" means threats that with varying likelihood may produce consequences severe enough to result in systemic failure or destruction of critical infrastructure or significant harm to human civilization. Examples of global catastrophic and existential threats include severe global pandemics, nuclear war, asteroid and comet impacts, supervolcanoes, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies.

(8) Indian Tribal government

The term "Indian Tribal government" has the meaning given the term "Indian tribal government" in section 5122 of title 42.

(9) Local government; State

The terms "local government" and "State" have the meanings given such terms in section 5122 of title 42.

(10) National exercise program

The term "national exercise program" means activities carried out to test and evaluate the national preparedness goal and related plans and strategies as described in section 748(b) of this title.

(11) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(Pub. L. 117–263, div. G, title LXXIII, §7302, Dec. 23, 2022, 136 Stat. 3684.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 5195c(e) of title 42, referred to in par. (4), was in the original "section 1016(e) of the Critical Infrastructure Protection Act of 2001" and was translated as reading "section 1016(e) of the Critical Infrastructures Protection Act of 2001", to reflect the probable intent of Congress.

§822. Assessment of global catastrophic risk

(a) In general

The Secretary and the Administrator shall coordinate an assessment of global catastrophic risk.

(b) Coordination

When coordinating the assessment under subsection (a), the Secretary and the Administrator shall coordinate with senior designees of—

(1) the Assistant to the President for National Security Affairs;

(2) the Director of the Office of Science and Technology Policy;

(3) the Secretary of State and the Under Secretary of State for Arms Control and International Security;

(4) the Attorney General and the Director of the Federal Bureau of Investigation;

(5) the Secretary of Energy, the Under Secretary of Energy for Nuclear Security, and the Director of Science;

(6) the Secretary of Health and Human Services, the Assistant Secretary for Preparedness and Response, and the Assistant Secretary of Global Affairs;

(7) the Secretary of Commerce, the Under Secretary of Commerce for Oceans and Atmosphere, and the Under Secretary of Commerce for Standards and Technology;

(8) the Secretary of the Interior and the Director of the United States Geological Survey;

(9) the Administrator of the Environmental Protection Agency and the Assistant Administrator for Water;

(10) the Administrator of the National Aeronautics and Space Administration;

(11) the Director of the National Science Foundation;

(12) the Secretary of the Treasury;

(13) the Secretary of Defense, the Assistant Secretary of the Army for Civil Works, and the Chief of Engineers and Commanding General of the Army Corps of Engineers;

(14) the Chairman of the Joint Chiefs of Staff;

(15) the Administrator of the United States Agency for International Development;

(16) the Secretary of Transportation; and

(17) other stakeholders the Secretary and the Administrator determine appropriate.

(Pub. L. 117–263, div. G, title LXXIII, §7303, Dec. 23, 2022, 136 Stat. 3685.)

§823. Report required

(a) In general

Not later than 1 year after December 23, 2022, and every 10 years thereafter, the Secretary, in coordination with the Administrator, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate and the Committee on Transportation and Infrastructure and the Committee on Armed Services of the House of Representatives a report containing a detailed assessment, based on the input and coordination required under section 822 of this title, of global catastrophic and existential risk.

(b) Matters covered

Each report required under subsection (a) shall include—

(1) expert estimates of cumulative global catastrophic and existential risk in the next 30 years, including separate estimates for the likelihood of occurrence and potential consequences;

(2) expert-informed analyses of the risk of the most concerning specific global catastrophic and existential threats, including separate estimates, where reasonably feasible and credible, of each threat for its likelihood of occurrence and its potential consequences, as well as associated uncertainties;

(3) a comprehensive list of potential catastrophic or existential threats, including even those that may have very low likelihood;

(4) technical assessments and lay explanations of the analyzed global catastrophic and existential risks, including their qualitative character and key factors affecting their likelihood of occurrence and potential consequences;

(5) an explanation of any factors that limit the ability of the Secretary to assess the risk both cumulatively and for particular threats, and how those limitations may be overcome through future research or with additional resources, programs, or authorities;

(6) a forecast of if and why global catastrophic and existential risk is likely to increase or decrease significantly in the next 10 years, both qualitatively and quantitatively, as well as a description of associated uncertainties;

(7) proposals for how the Federal Government may more adequately assess global catastrophic and existential risk on an ongoing basis in future years;

(8) recommendations for legislative actions, as appropriate, to support the evaluation and assessment of global catastrophic and existential risk; and

(9) other matters deemed appropriate by the Secretary, in coordination with the Administrator, and based on the input and coordination required under section 822 of this title.

(c) Consultation requirement

In producing the report required under subsection (a), the Secretary shall—

(1) regularly consult with experts on severe global pandemics, nuclear war, asteroid and comet impacts, supervolcanoes, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies; and

(2) share information gained through the consultation required under paragraph (1) with relevant Federal partners listed in section 822(b) of this title.

(Pub. L. 117–263, div. G, title LXXIII, §7304, Dec. 23, 2022, 136 Stat. 3686.)

§824. Enhanced catastrophic incident annex

(a) In general

The Secretary, in coordination with the Administrator and the Federal partners listed in section 822(b) of this title, shall supplement each Federal Interagency Operational Plan to include an annex containing a strategy to ensure the health, safety, and general welfare of the civilian population affected by catastrophic incidents by—

(1) providing for the basic needs of the civilian population of the United States that is impacted by catastrophic incidents in the United States;

(2) coordinating response efforts with State, local, and Indian Tribal governments, the private sector, and nonprofit relief organizations;

(3) promoting personal and local readiness and non-reliance on government relief during periods of heightened tension or after catastrophic incidents; and

(4) developing international partnerships with allied nations for the provision of relief services and goods.

(b) Elements of the strategy

The strategy required under subsection (a) shall include a description of—

(1) actions the Federal Government should take to ensure the basic needs of the civilian population of the United States in a catastrophic incident are met;

(2) how the Federal Government should coordinate with non-Federal entities to multiply resources and enhance relief capabilities, including—

(A) State and local governments;

(B) Indian Tribal governments;

(C) State disaster relief agencies;

(D) State and local disaster relief managers;

(E) State National Guards;
(F) law enforcement and first response entities; and
(G) nonprofit relief services;

(3) actions the Federal Government should take to enhance individual resiliency to the effects of a catastrophic incident, which actions shall include—
(A) readiness alerts to the public during periods of elevated threat;
(B) efforts to enhance domestic supply and availability of critical goods and basic necessities; and
(C) information campaigns to ensure the public is aware of response plans and services that will be activated when necessary;

(4) efforts the Federal Government should undertake and agreements the Federal Government should seek with international allies to enhance the readiness of the United States to provide for the general welfare;
(5) how the strategy will be implemented should multiple levels of critical infrastructure be destroyed or taken offline entirely for an extended period of time; and
(6) the authorities the Federal Government should implicate in responding to a catastrophic incident.

(c) Assumptions

In designing the strategy under subsection (a), the Secretary, in coordination with the Administrator and the Federal partners listed in section 822(b) of this title, shall account for certain factors to make the strategy operationally viable, including the assumption that—
(1) multiple levels of critical infrastructure have been taken offline or destroyed by catastrophic incidents or the effects of catastrophic incidents;
(2) impacted sectors may include—
(A) the transportation sector;
(B) the communication sector;
(C) the energy sector;
(D) the healthcare and public health sector; and
(E) the water and wastewater sector;

(3) State, local, Indian Tribal, and territorial governments have been equally affected or made largely inoperable by catastrophic incidents or the effects of catastrophic incidents;
(4) the emergency has exceeded the response capabilities of State, local, and Indian Tribal governments under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) and other relevant disaster response laws; and
(5) the United States military is sufficiently engaged in armed or cyber conflict with State or non-State adversaries, or is otherwise unable to augment domestic response capabilities in a significant manner due to a catastrophic incident.

(Pub. L. 117–263, div. G, title LXXIII, §7305, Dec. 23, 2022, 136 Stat. 3687.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (c)(4), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

VALIDATION OF STRATEGY; RECOMMENDATIONS; REPORT

Pub. L. 117–263, div. G, title LXXIII, §§7306–7308, Dec. 23, 2022, 136 Stat. 3688, provided that:

"SEC. 7306. VALIDATION OF THE STRATEGY THROUGH AN EXERCISE.

"Not later than 1 year after the addition of the annex required under section 7305 [6 U.S.C. 824], the Administrator shall lead an exercise as part of the national exercise program to test and enhance the operationalization of the strategy required under section 7305.

"SEC. 7307. RECOMMENDATIONS.

"(a) IN GENERAL.—The Secretary, in coordination with the Administrator and the Federal partners listed in section 7303(b) of this title [6 U.S.C. 822(b)], shall provide recommendations to Congress for—

"(1) actions that should be taken to prepare the United States to implement the strategy required under section 7305, increase readiness, and address preparedness gaps for responding to the impacts of catastrophic incidents on citizens of the United States; and

"(2) additional authorities that should be considered for Federal agencies to more effectively implement the strategy required under section 7305.

"(b) INCLUSION IN REPORTS.—The Secretary may include the recommendations required under subsection (a) in a report submitted under section 7308.

"SEC. 7308. REPORTING REQUIREMENTS.

"Not later than 1 year after the date on which the Administrator leads the exercise under section 7306, the Secretary, in coordination with the Administrator, shall submit to Congress a report that includes—

"(1) a description of the efforts of the Secretary and the Administrator to develop and update the strategy required under section 7305; and

"(2) an after-action report following the conduct of the exercise described in section 7306."

§825. Rules of construction

(a) Administrator

Nothing in this part shall be construed to supersede the civilian emergency management authority of the Administrator under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or the Post Katrina Emergency Management Reform Act [1] (6 U.S.C. 701 et seq.).

(b) Secretary

Nothing in this part shall be construed as providing new authority to the Secretary, except to coordinate and facilitate the development of the assessments and reports required pursuant to this part.

(Pub. L. 117–263, div. G, title LXXIII, §7309, Dec. 23, 2022, 136 Stat. 3689.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (a), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 5121 of Title 42 and Tables.

The Post Katrina Emergency Management Reform Act, referred to in subsec. (a), probably means the Post-Katrina Emergency Management Reform Act of 2006, which is title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1394, which enacted this chapter and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title note set out under section 701 of this title and Tables.

[1] *See References in Text note below.*

CHAPTER 3—SECURITY AND ACCOUNTABILITY FOR EVERY PORT

Sec.

901. Definitions.

SUBCHAPTER I—SECURITY OF UNITED STATES SEAPORTS

PART A—PORT SECURITY GRANTS; TRAINING AND EXERCISE PROGRAMS

911. Repealed.
912. Port Security Exercise Program.
913. Facility exercise requirements.

PART B—PORT OPERATIONS

921. Domestic radiation detection and imaging.
921a. Integration of detection equipment and technologies.
922. Repealed.
923. Random searches of containers.
924. Threat assessment screening of port truck drivers.
925. Border Patrol unit for United States Virgin Islands.
926. Center of Excellence for Maritime Domain Awareness.

SUBCHAPTER II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

PART A—GENERAL PROVISIONS

941. Strategic plan to enhance the security of the international supply chain.
942. Post-incident resumption of trade.
943. Automated Targeting System.
944. Container security standards and procedures.
945. Container Security Initiative.

PART B—CUSTOMS–TRADE PARTNERSHIP AGAINST TERRORISM

961. Establishment.
962. Eligible entities.
963. Minimum requirements.
964. Tier 1 participants in C–TPAT.
965. Tier 2 participants in C–TPAT.
966. Tier 3 participants in C–TPAT.
967. Consequences for lack of compliance.
968. Third party validations.
969. Revalidation.
970. Noncontainerized cargo.
971. C–TPAT program management.
972. Additional personnel.
973. Authorization of appropriations.

PART C—MISCELLANEOUS PROVISIONS

981. Pilot integrated scanning system.
981a. Pilot integrated scanning system.
982. Screening and scanning of cargo containers.
983. Inspection technology and training.
984. Repealed.
985. Information sharing relating to supply chain security cooperation.

SUBCHAPTER III—ADMINISTRATION

1001. Designation of liaison office of Department of State.
1002. Homeland Security Science and Technology Advisory Committee.
1003. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.

§901. Definitions

In this Act:

(1) Appropriate congressional committees

Except as otherwise provided, the term "appropriate congressional committees" means—

(A) the Committee on Appropriations of the Senate;
(B) the Committee on Commerce, Science, and Transportation of the Senate;
(C) the Committee on Finance of the Senate;
(D) the Committee on Homeland Security and Governmental Affairs of the Senate;
(E) the Committee on Appropriations of the House of Representatives;
(F) the Committee on Homeland Security of the House of Representatives;
(G) the Committee on Transportation and Infrastructure of the House of Representatives;
(H) the Committee on Ways and Means of the House of Representatives; and
(I) other congressional committees, as appropriate.

(2) Commercial Operations Advisory Committee

The term "Commercial Operations Advisory Committee" means the Advisory Committee established pursuant to section 9503(c) of the Omnibus Budget Reconciliation Act of 1987 (19 U.S.C. 2071 note) [1] or any successor committee.

(3) Commercial seaport personnel

The term "commercial seaport personnel" includes any person engaged in an activity relating to the loading or unloading of cargo or passengers, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go in the United States.

(4) Commissioner

The term "Commissioner" means the Commissioner responsible for the United States Customs and Border Protection of the Department of Homeland Security.

(5) Container

The term "container" has the meaning given the term in the International Convention for Safe Containers, with annexes, done at Geneva, December 2, 1972 (29 UST 3707).

(6) Container security device

The term "container security device" means a device, or system, designed, at a minimum, to identify positively a container, to detect and record the unauthorized intrusion of a container, and to secure a container against tampering throughout the supply chain. Such a device, or system, shall have a low false alarm rate as determined by the Secretary.

(7) Department

The term "Department" means the Department of Homeland Security.

(8) Examination

The term "examination" means an inspection of cargo to detect the presence of misdeclared, restricted, or prohibited items that utilizes nonintrusive imaging and detection technology.

(9) Inspection

The term "inspection" means the comprehensive process used by the United States Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. The process may include screening, conducting an examination, or conducting a search.

(10) International supply chain

The term "international supply chain" means the end-to-end process for shipping goods to or from the United States beginning at the point of origin (including manufacturer, supplier, or

vendor) through a point of distribution to the destination.

(11) Radiation detection equipment

The term "radiation detection equipment" means any technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

(12) Scan

The term "scan" means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container.

(13) Screening

The term "screening" means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo.

(14) Search

The term "search" means an intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of misdeclared, restricted, or prohibited items.

(15) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(16) Transportation disruption

The term "transportation disruption" means any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, an act of terrorism, or any transportation security incident (as defined in section 70101(6) [1] of title 46).

(17) Transportation security incident

The term "transportation security incident" has the meaning given the term in section 70101(6) [1] of title 46.

(Pub. L. 109–347, §2, Oct. 13, 2006, 120 Stat. 1886.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in text, is Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1884, known as the Security and Accountability For Every Port Act of 2006 or the SAFE Port Act. For complete classification of this Act to the Code, see Tables.

Section 9503(c) of the Omnibus Budget Reconciliation Act of 1987, referred to in par. (2), is section 9503(c) of title IX of Pub. L. 100–203, which was set out as a note under section 2071 of Title 19, Customs Duties, prior to repeal by Pub. L. 114–125, title I, §109(g)(1), Feb. 24, 2016, 130 Stat. 137. For establishment of successor committee, see section 4316(a) of Title 19.

Section 70101(6) of title 46, referred to in pars. (16) and (17), was redesignated section 70101(7) of title 46 by Pub. L. 115–254, div. J, §1805(b)(1), Oct. 5, 2018, 132 Stat. 3534.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

Pub. L. 109–347, §1(a), Oct. 13, 2006, 120 Stat. 1884, provided that: "This Act [see Tables for classification] may be cited as the 'Security and Accountability For Every Port Act of 2006' or the 'SAFE Port Act'."

[1] *See References in Text note below.*

SUBCHAPTER I—SECURITY OF UNITED STATES SEAPORTS

PART A—PORT SECURITY GRANTS; TRAINING AND EXERCISE PROGRAMS

§911. Repealed. Pub. L. 111–281, title VIII, §821(b), Oct. 15, 2010, 124 Stat. 3003

Section, Pub. L. 109–347, title I, §113, Oct. 13, 2006, 120 Stat. 1895, established the Port Security Training Program and its requirements.

§912. Port Security Exercise Program

(a) In general

The Secretary, acting through the Under Secretary for Preparedness and in coordination with the Commandant of the Coast Guard, shall establish a Port Security Exercise Program (referred to in this section as the "Exercise Program") for the purpose of testing and evaluating the capabilities of Federal, State, local, and foreign governments, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities required to submit a plan under section 70103(c) of title 46.

(b) Requirements

The Secretary shall ensure that the Exercise Program—

(1) conducts, on a periodic basis, port security exercises at such facilities that are—

(A) scaled and tailored to the needs of each facility;

(B) live, in the case of the most at-risk facilities;

(C) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, the National Maritime Transportation Security Plan, and other such national initiatives;

(E) evaluated against clear and consistent performance measures;

(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, and local officials, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, and the private sector; and

(G) followed by remedial action in response to lessons learned; and

(2) assists State and local governments and facilities in designing, implementing, and evaluating exercises that—

(A) conform to the requirements of paragraph (1); and

(B) are consistent with any applicable Area Maritime Transportation Security Plan and State or Urban Area Homeland Security Plan.

(c) Improvement plan

The Secretary shall establish a port security exercise improvement plan process to—

(1) identify and analyze each port security exercise for lessons learned and best practices;

(2) disseminate lessons learned and best practices to participants in the Exercise Program;

(3) monitor the implementation of lessons learned and best practices by participants in the Exercise Program; and

(4) conduct remedial action tracking and long-term trend analysis.

(Pub. L. 109–347, title I, §114, Oct. 13, 2006, 120 Stat. 1896.)

§913. Facility exercise requirements

The Secretary of the Department in which the Coast Guard is operating shall require each high risk facility to conduct live or full-scale exercises described in section 105.220(c) of title 33, Code of Federal Regulations, not less frequently than once every 2 years, in accordance with the facility security plan required under section 70103(c) of title 46.

(Pub. L. 109–347, title I, §115, Oct. 13, 2006, 120 Stat. 1897.)

PART B—PORT OPERATIONS

§921. Domestic radiation detection and imaging

(a) Scanning containers

Subject to section 1318 of title 19, not later than December 31, 2007, all containers entering the United States through the 22 ports through which the greatest volume of containers enter the United States by vessel shall be scanned for radiation. To the extent practicable, the Secretary shall deploy next generation radiation detection technology.

(b) Strategy

The Secretary shall develop a strategy for the deployment of radiation detection capabilities that includes—

(1) a risk-based prioritization of ports of entry at which radiation detection equipment will be deployed;

(2) a proposed timeline of when radiation detection equipment will be deployed at each port of entry identified under paragraph (1);

(3) the type of equipment to be used at each port of entry identified under paragraph (1), including the joint deployment and utilization of radiation detection equipment and nonintrusive imaging equipment;

(4) standard operating procedures for examining containers with such equipment, including sensor alarming, networking, and communications and response protocols;

(5) operator training plans;

(6) an evaluation of the environmental health and safety impacts of nonintrusive imaging technology and a radiation risk reduction plan, in consultation with the Nuclear Regulatory Commission, the Occupational Safety and Health Administration, and the National Institute for Occupational Safety and Health, that seeks to minimize radiation exposure of workers and the public to levels as low as reasonably achievable;

(7) the policy of the Department for using nonintrusive imaging equipment in tandem with radiation detection equipment; and

(8) a classified annex that—

(A) details plans for covert testing; and

(B) outlines the risk-based prioritization of ports of entry identified under paragraph (1).

(c) Standards

The Secretary, acting through the Director for Domestic Nuclear Detection [1] and in collaboration with the National Institute of Standards and Technology, shall publish technical capability standards

and recommended standard operating procedures for the use of nonintrusive imaging and radiation detection equipment in the United States. Such standards and procedures—

(1) should take into account relevant standards and procedures utilized by other Federal departments or agencies as well as those developed by international bodies; and

(2) shall not be designed so as to endorse specific companies or create sovereignty conflicts with participating countries.

(d) Implementation

Not later than 3 years after October 13, 2006, the Secretary shall fully implement the strategy developed under subsection (b).

(e) Expansion to other United States ports of entry

(1) In general

As soon as practicable after—

(A) implementation of the program for the examination of containers for radiation at ports of entry described in subsection (a); and

(B) submission of the strategy developed under subsection (b),

but not later than December 31, 2008, the Secretary shall expand the strategy developed under subsection (b), in a manner consistent with the requirements of subsection (b), to provide for the deployment of radiation detection capabilities at all other United States ports of entry not covered by the strategy developed under subsection (b).

(2) Risk assessment

In expanding the strategy under paragraph (1), the Secretary shall identify and assess the risks to those other ports of entry in order to determine what equipment and practices will best mitigate the risks.

(f) Intermodal Rail Radiation Detection Test Center

(1) Establishment

In accordance with subsection (b), and in order to comply with this section, the Secretary shall establish an Intermodal Rail Radiation Detection Test Center (referred to in this subsection as the "Test Center").

(2) Projects

The Secretary shall conduct multiple, concurrent projects at the Test Center to rapidly identify and test concepts specific to the challenges posed by on-dock rail.

(3) Location

The Test Center shall be located within a public port facility at which a majority of the containerized cargo is directly laden from (or unladen to) on-dock, intermodal rail.

(Pub. L. 109–347, title I, §121, Oct. 13, 2006, 120 Stat. 1898; Pub. L. 115–254, div. J, §1816(b), Oct. 5, 2018, 132 Stat. 3541.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsecs. (c) to (e). Pub. L. 115–254, §1816(b)(1), (2), redesignated subsecs. (f) to (h) as (c) to (e), respectively, and struck out former subsecs. (c) to (e). Prior to amendment, subsecs. (c) to (e) read as follows:

"(c) REPORT.—Not later than 90 days after October 13, 2006, the Secretary shall submit the strategy developed under subsection (b) to the appropriate congressional committees.

"(d) UPDATE.—Not later than 180 days after the date of the submission of the report under subsection (c), the Secretary shall provide a more complete evaluation under subsection (b)(6).

"(e) OTHER WEAPONS OF MASS DESTRUCTION THREATS.—Not later than 180 days after October 13, 2006, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of,

and a strategy for, the development of equipment to detect and prevent shielded nuclear and radiological threat material and chemical, biological, and other weapons of mass destruction from entering the United States."

Subsec. (e)(1)(B). Pub. L. 115–254, §1816(b)(3), struck out "(and updating, if any, of that strategy under subsection (c))" after "under subsection (b)".

Subsecs. (f) to (i). Pub. L. 115–254, §1816(b)(2), redesignated subsecs. (f) to (i) as (c) to (f), respectively.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director for Domestic Nuclear Detection deemed to be a reference to the Assistant Secretary for the Countering Weapons of Mass Destruction Office, see section 2(b)(1)(B) of Pub. L. 115–387, set out as a note under section 591 of this title.

[1] *See Change of Name note below.*

§921a. Integration of detection equipment and technologies

(a) Responsibility of Secretary

The Secretary of Homeland Security shall have responsibility for ensuring that domestic chemical, biological, radiological, and nuclear detection equipment and technologies are integrated, as appropriate, with other border security systems and detection technologies.

(b) Report

Not later than 6 months after August 3, 2007, the Secretary shall submit a report to Congress that contains a plan to develop a departmental technology assessment process to determine and certify the technology readiness levels of chemical, biological, radiological, and nuclear detection technologies before the full deployment of such technologies within the United States.

(Pub. L. 110–53, title XI, §1104, Aug. 3, 2007, 121 Stat. 380.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Implementing Recommendations of the 9/11 Commission Act of 2007, and not as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, which comprises this chapter.

§922. Repealed. Pub. L. 115–254, div. J, §1816(c), Oct. 5, 2018, 132 Stat. 3541

Section, Pub. L. 109–347, title I, §122, Oct. 13, 2006, 120 Stat. 1899, related to inspection of car ferries entering from abroad.

§923. Random searches of containers

Not later than 1 year after October 13, 2006, the Secretary, acting through the Commissioner, shall develop and implement a plan, utilizing best practices for empirical scientific research design and random sampling, to conduct random searches of containers in addition to any targeted or preshipment inspection of such containers required by law or regulation or conducted under any other program conducted by the Secretary. Nothing in this section shall be construed to mean that implementation of the random sampling plan precludes additional searches of containers not inspected pursuant to the plan.

(Pub. L. 109–347, title I, §123, Oct. 13, 2006, 120 Stat. 1899.)

§924. Threat assessment screening of port truck drivers

Not later than 90 days after October 13, 2006, the Secretary shall implement a threat assessment screening, including name-based checks against terrorist watch lists and immigration status check, for all port truck drivers with access to secure areas of a port who have a commercial driver's license but do not have a current and valid hazardous materials endorsement issued in accordance with section 1572 [1] of title 49, Code of Federal Regulations, that is the same as the threat assessment screening required for facility employees and longshoremen by the Commandant of the Coast Guard under Coast Guard Notice USCG–2006–24189 (Federal Register, Vol. 71, No. 82, Friday, April 28, 2006).

(Pub. L. 109–347, title I, §125, Oct. 13, 2006, 120 Stat. 1900.)

[1] *So in original. Probably should be "part 1572".*

§925. Border Patrol unit for United States Virgin Islands

(a) In general

The Secretary may establish at least 1 Border Patrol unit for the United States Virgin Islands.

(b) Report

Not later than 180 days after October 13, 2006, the Secretary shall submit a report to the appropriate congressional committees that includes the schedule, if any, for carrying out subsection (a).

(Pub. L. 109–347, title I, §126, Oct. 13, 2006, 120 Stat. 1900.)

§926. Center of Excellence for Maritime Domain Awareness

(a) Establishment

The Secretary shall establish a university-based Center for Excellence for Maritime Domain Awareness following the merit-review processes and procedures that have been established by the Secretary for selecting university program centers of excellence.

(b) Duties

The Center established under subsection (a) shall—

(1) prioritize its activities based on the "National Plan To Improve Maritime Domain Awareness" published by the Department in October 2005;

(2) recognize the extensive previous and ongoing work and existing competence in the field of maritime domain awareness at numerous academic and research institutions, such as the Naval Postgraduate School;

(3) leverage existing knowledge and continue development of a broad base of expertise within academia and industry in maritime domain awareness; and

(4) provide educational, technical, and analytical assistance to Federal agencies with responsibilities for maritime domain awareness, including the Coast Guard, to focus on the need for interoperability, information sharing, and common information technology standards and architecture.

(Pub. L. 109–347, title I, §128, Oct. 13, 2006, 120 Stat. 1900.)

SUBCHAPTER II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

PART A—GENERAL PROVISIONS

§941. Strategic plan to enhance the security of the international supply chain

(a) Strategic plan

The Secretary, in consultation with appropriate Federal, State, local, and tribal government agencies and private sector stakeholders responsible for security matters that affect or relate to the movement of containers through the international supply chain, shall develop, implement, and update, triennially, a strategic plan to enhance the security of the international supply chain.

(b) Requirements

The strategic plan required under subsection (a) shall—

(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private-sector stakeholders that relate to the security of the movement of containers through the international supply chain;

(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;

(4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;

(5) build on available resources and consider costs and benefits;

(6) provide incentives for additional voluntary measures to enhance cargo security, as recommended by the Commissioner;

(7) consider the impact of supply chain security requirements on small- and medium-sized companies;

(8) include a process for sharing intelligence and information with private-sector stakeholders to assist in their security efforts;

(9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

(10) provide protocols for the expeditious resumption of the flow of trade in accordance with section 942 of this title;

(11) consider the linkages between supply chain security and security programs within other systems of movement, including travel security and terrorism finance programs; and

(12) expand upon and relate to existing strategies and plans, including the National Response Plan, the National Maritime Transportation Security Plan, the National Strategy for Maritime Security, and the 8 supporting plans of the Strategy, as required by Homeland Security Presidential Directive 13.

(c) Consultation

In developing protocols under subsection (b)(10), the Secretary shall consult with Federal, State, local, and private sector stakeholders, including the National Maritime Security Advisory Committee and the Commercial Operations Advisory Committee.

(d) Communication

To the extent practicable, the strategic plan developed under subsection (a) shall provide for coordination with, and lines of communication among, appropriate Federal, State, local, and private-sector stakeholders on law enforcement actions, intermodal rerouting plans, and other strategic infrastructure issues resulting from a transportation security incident or transportation disruption.

(e) Utilization of Advisory Committees

As part of the consultations described in subsection (a), the Secretary shall, to the extent practicable, utilize the Homeland Security Advisory Committee, the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee to review, as necessary, the draft strategic plan and any subsequent updates to the strategic plan.

(f) International standards and practices

In furtherance of the strategic plan required under subsection (a), the Secretary is encouraged to consider proposed or established standards and practices of foreign governments and international organizations, including the International Maritime Organization, the World Customs Organization, the International Labor Organization, and the International Organization for Standardization, as appropriate, to establish standards and best practices for the security of containers moving through the international supply chain.

(g) Reports

(1) Initial report

Not later than 270 days after October 13, 2006, the Secretary shall submit to the appropriate congressional committees a report that contains the strategic plan required by subsection (a).

(2) Updates

Not later than 270 days after October 5, 2018, and triennially thereafter, the Secretary shall submit to the appropriate congressional committees a report that contains any updates to the strategic plan under subsection (a) since the prior report.

(Pub. L. 109–347, title II, §201, Oct. 13, 2006, 120 Stat. 1901; Pub. L. 115–254, div. J, §1804, Oct. 5, 2018, 132 Stat. 3533.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–254, §1804(1), substituted "triennially" for "as appropriate".

Subsec. (g). Pub. L. 115–254, §1804(2)(A), substituted "Reports" for "Report" in heading.

Subsec. (g)(2). Pub. L. 115–254, §1804(2)(B), amended par. (2) generally. Prior to amendment, text read as follows: "Not later than 3 years after the date on which the strategic plan is submitted under paragraph (1), the Secretary shall submit a report to the appropriate congressional committees that contains an update of the strategic plan."

§942. Post-incident resumption of trade

(a) In general

The Secretary shall develop and update, as necessary, protocols for the resumption of trade in accordance with section 941(b)(10) of this title in the event of a transportation disruption or a transportation security incident. The protocols shall include—

(1) the identification of the appropriate initial incident commander, if the Commandant of the Coast Guard is not the appropriate person, and lead departments, agencies, or offices to execute such protocols;

(2) a plan to redeploy resources and personnel, as necessary, to reestablish the flow of trade;

(3) a plan to provide training for the periodic instruction of personnel of the United States Customs and Border Protection, the Coast Guard, and the Transportation Security Administration in trade resumption functions and responsibilities; and

(4) appropriate factors for establishing prioritization of vessels and cargo determined by the President to be critical for response and recovery, including factors relating to public health, national security, and economic need.

(b) Vessels

In determining the prioritization of vessels accessing facilities (as defined under section 70101 of title 46), the Commandant of the Coast Guard may, to the extent practicable and consistent with the protocols and plans required under this section to ensure the safe and secure transit of vessels to ports in the United States after a transportation security incident, give priority to a vessel—

(1) that has an approved security plan under section 70103(c) of title 46 or a valid international ship security certificate, as provided under part 104 of title 33, Code of Federal Regulations;

(2) that is manned by individuals who are described in section 70105(b)(2)(B) of title 46; and

(3) that is operated by validated participants in the Customs-Trade Partnership Against Terrorism program.

(c) Cargo

In determining the prioritization of the resumption of the flow of cargo and consistent with the protocols established under this section, the Commissioner may give preference to cargo—

(1) entering a port of entry directly from a foreign seaport designated under the Container Security Initiative;

(2) from the supply chain of a validated C–TPAT participant and other private sector entities, as appropriate; or

(3) that has undergone—

(A) a nuclear or radiological detection scan;

(B) an x-ray, density, or other imaging scan; and

(C) a system to positively identify the container at the last port of departure prior to arrival in the United States, which data has been evaluated and analyzed by personnel of the United States Customs and Border Protection.

(d) Coordination

The Secretary shall ensure that there is appropriate coordination among the Commandant of the Coast Guard, the Commissioner, and other Federal officials following a maritime disruption or maritime transportation security incident in order to provide for the resumption of trade.

(e) Communication

Consistent with section 941 of this title, the Commandant of the Coast Guard, Commissioner, and other appropriate Federal officials, shall promptly communicate any revised procedures or instructions intended for the private sector following a maritime disruption or maritime transportation security incident.

(Pub. L. 109–347, title II, §202, Oct. 13, 2006, 120 Stat. 1903.)

§943. Automated Targeting System

(a) In general

The Secretary, acting through the Commissioner, shall—

(1) identify and seek the submission of data related to the movement of a shipment of cargo through the international supply chain; and

(2) analyze the data described in paragraph (1) to identify high-risk cargo for inspection.

(b) Requirement

The Secretary, acting through the Commissioner, shall require the electronic transmission to the Department of additional data elements for improved high-risk targeting, including appropriate security elements of entry data, as determined by the Secretary, to be provided as advanced information with respect to cargo destined for importation into the United States prior to loading of such cargo on vessels at foreign seaports.

(c) Consideration

The Secretary, acting through the Commissioner, shall—

(1) consider the cost, benefit, and feasibility of—

(A) requiring additional nonmanifest documentation;

(B) reducing the time period allowed by law for revisions to a container cargo manifest;

(C) reducing the time period allowed by law for submission of certain elements of entry data, for vessel or cargo; and

(D) such other actions the Secretary considers beneficial for improving the information relied upon for the Automated Targeting System and any successor targeting system in furthering the security and integrity of the international supply chain; and

(2) consult with stakeholders, including the Commercial Operations Advisory Committee, and identify to them the need for such information, and the appropriate timing of its submission.

(d) Regulations

The Secretary shall promulgate regulations to carry out this section. In promulgating such regulations, the Secretary shall adhere to the parameters applicable to the development of regulations under section 343(a) of the Trade Act of 2002 (19 U.S.C. 2071 note),[1] including provisions relating to consultation, technology, analysis, use of information, confidentiality, and timing requirements.

(e) System improvements

The Secretary, acting through the Commissioner, shall—

(1) conduct, through an independent panel, a review of the effectiveness and capabilities of the Automated Targeting System;

(2) consider future iterations of the Automated Targeting System, which would incorporate smart features, such as more complex algorithms and real-time intelligence, instead of relying solely on rule sets that are periodically updated;

(3) ensure that the Automated Targeting System has the capability to electronically compare manifest and other available data for cargo entered into or bound for the United States to detect any significant anomalies between such data and facilitate the resolution of such anomalies;

(4) ensure that the Automated Targeting System has the capability to electronically identify, compile, and compare select data elements for cargo entered into or bound for the United States following a maritime transportation security incident, in order to efficiently identify cargo for increased inspection or expeditious release; and

(5) develop a schedule to address the recommendations of the Comptroller General of the United States, the Inspector General of the Department of the Treasury, and the Inspector General of the Department with respect to the operation of the Automated Targeting System.

(f) Secure transmission of certain information

All information required by the Department from supply chain partners shall be transmitted in a secure fashion, as determined by the Secretary, so as to protect the information from unauthorized access.

(g) Authorization of appropriations

There are authorized to be appropriated to the United States Customs and Border Protection to carry out the Automated Targeting System for identifying high-risk oceanborne container cargo for inspection—

(1) $33,200,000 for fiscal year 2008;

(2) $35,700,000 for fiscal year 2009; and

(3) $37,485,000 for fiscal year 2010.

(Pub. L. 109–347, title II, §203, Oct. 13, 2006, 120 Stat. 1904.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 343(a) of the Trade Act of 2002, referred to in subsec. (d), is section 343(a) of Pub. L. 107–210, which was set out as a note under section 2071 of Title 19, Customs Duties, prior to editorial transfer to

section 1415(a) of Title 19.

[1] *See References in Text note below.*

§944. Container security standards and procedures

(a) Establishment

(1) In general

Not later than 90 days after October 13, 2006, the Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States.

(2) Interim rule

Not later than 180 days after October 13, 2006, the Secretary shall issue an interim final rule pursuant to the proceeding described in paragraph (1).

(3) Missed deadline

If the Secretary is unable to meet the deadline established pursuant to paragraph (2), the Secretary shall submit a letter to the appropriate congressional committees explaining why the Secretary is unable to meet that deadline and describing what must be done before such minimum standards and procedures can be established.

(4) Deadline for enforcement

(A) Enforcement of rule

Not later than 2 years after the date on which the standards and procedures are established pursuant to paragraph (1), all containers bound for ports of entry in the United States shall meet such standards and procedures.

(B) Interim requirement

If the interim final rule described in paragraph (2) is not issued by April 1, 2008, then—

(i) effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers; and

(ii) the requirements of this subparagraph shall cease to be effective upon the effective date of the interim final rule issued pursuant to this subsection.

(b) Review and enhancement

The Secretary shall regularly review and enhance the standards and procedures established pursuant to subsection (a), as appropriate, based on tests of technologies as they become commercially available to detect container intrusion and the highest consequence threats, particularly weapons of mass destruction.

(c) International cargo security standards

The Secretary, in consultation with the Secretary of State, the Secretary of Energy, and other Federal Government officials, as appropriate, and with the Commercial Operations Advisory Committee, the Homeland Security Advisory Committee, and the National Maritime Security Advisory Committee, is encouraged to promote and establish international standards for the security of containers moving through the international supply chain with foreign governments and international organizations, including the International Maritime Organization, the International Organization for Standardization, the International Labor Organization, and the World Customs Organization.

(d) International trade and other obligations

In carrying out this section, the Secretary shall consult with appropriate Federal departments and

agencies and private sector stakeholders and ensure that actions under this section do not violate international trade obligations or other international obligations of the United States.

(Pub. L. 109–347, title II, §204, Oct. 13, 2006, 120 Stat. 1905; Pub. L. 110–53, title XVII, §1701(b), Aug. 3, 2007, 121 Stat. 491.)

EDITORIAL NOTES

AMENDMENTS

2007—Subsec. (a)(4). Pub. L. 110–53, which directed amendment of par. (4) by substituting "(1) Deadline for enforcement" and subpar. (A) designation and heading for "(1) Deadline for enforcement", was executed by inserting the subpar. (A) designation and heading before "Not later than" and making no change in the par. designation or heading, to reflect the probable intent of Congress.

Subsec. (a)(4)(B). Pub. L. 110–53, §1701(b)(2), added subpar. (B).

§945. Container Security Initiative

(a) Establishment

The Secretary, acting through the Commissioner, shall establish and implement a program (referred to in this section as the "Container Security Initiative" or "CSI") to identify and examine or search maritime containers that pose a security risk before loading such containers in a foreign port for shipment to the United States, either directly or through a foreign port.

(b) Assessment

The Secretary, acting through the Commissioner, may designate foreign seaports to participate in the Container Security Initiative after the Secretary has assessed the costs, benefits, and other factors associated with such designation, including—

(1) the level of risk for the potential compromise of containers by terrorists, or other threats as determined by the Secretary;

(2) the volume of cargo being imported to the United States directly from, or being transshipped through, the foreign seaport;

(3) the results of the Coast Guard assessments conducted pursuant to section 70108 of title 46;

(4) the commitment of the government of the country in which the foreign seaport is located to cooperating with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and

(5) the potential for validation of security practices at the foreign seaport by the Department.

(c) Notification

The Secretary shall notify the appropriate congressional committees of the designation of a foreign port under the Container Security Initiative or the revocation of such a designation before notifying the public of such designation or revocation.

(d) Negotiations

The Secretary, in cooperation with the Secretary of State and in consultation with the United States Trade Representative, may enter into negotiations with the government of each foreign nation in which a seaport is designated under the Container Security Initiative to ensure full compliance with the requirements under the Container Security Initiative.

(e) Overseas inspections

(1) Requirements and procedures

The Secretary shall—

(A) establish minimum technical capability criteria and standard operating procedures for the use of nonintrusive inspection and nuclear and radiological detection systems in conjunction with CSI;

(B) require each port designated under CSI to operate nonintrusive inspection and nuclear and radiological detection systems in accordance with the technical capability criteria and standard operating procedures established under subparagraph (A);

(C) continually monitor the technologies, processes, and techniques used to inspect cargo at ports designated under CSI to ensure adherence to such criteria and the use of such procedures; and

(D) consult with the Secretary of Energy in establishing the minimum technical capability criteria and standard operating procedures established under subparagraph (A) pertaining to radiation detection technologies to promote consistency in detection systems at foreign ports designated under CSI.

(2) Constraints

The criteria and procedures established under paragraph (1)(A)—

(A) shall be consistent, as practicable, with relevant standards and procedures utilized by other Federal departments or agencies, or developed by international bodies if the United States consents to such standards and procedures;

(B) shall not apply to activities conducted under the Megaports Initiative of the Department of Energy; and

(C) shall not be designed to endorse the product or technology of any specific company or to conflict with the sovereignty of a country in which a foreign seaport designated under the Container Security Initiative is located.

(f) Savings provision

The authority of the Secretary under this section shall not affect any authority or duplicate any efforts or responsibilities of the Federal Government with respect to the deployment of radiation detection equipment outside of the United States.

(g) Coordination

The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment required to support the Container Security Initiative through the Department of Energy's Second Line of Defense Program and Megaports Initiative; or

(2) work with the private sector or host governments, when possible, to obtain radiation detection equipment that meets the Department's and the Department of Energy's technical specifications for such equipment.

(h) Staffing

The Secretary shall develop a human capital management plan to determine adequate staffing levels in the United States and in foreign seaports including, as appropriate, the remote location of personnel in countries in which foreign seaports are designated under the Container Security Initiative.

(i) Annual discussions

The Secretary, in coordination with the appropriate Federal officials, shall hold annual discussions with foreign governments of countries in which foreign seaports designated under the Container Security Initiative are located regarding best practices, technical assistance, training needs, and technological developments that will assist in ensuring the efficient and secure movement of international cargo.

(j) Lesser risk port

The Secretary, acting through the Commissioner, may treat cargo loaded in a foreign seaport designated under the Container Security Initiative as presenting a lesser risk than similar cargo loaded in a foreign seaport that is not designated under the Container Security Initiative, for the purpose of clearing such cargo into the United States.

(k) Prohibition

(1) In general

The Secretary shall issue a "do not load" order, using existing authorities, to prevent the onload of any cargo loaded at a port designated under CSI that has been identified as high risk, including by the Automated Targeting System, unless the cargo is determined to no longer be high risk through—

(A) a scan of the cargo with nonintrusive imaging equipment and radiation detection equipment;

(B) a search of the cargo; or

(C) additional information received by the Department.

(2) Rule of construction

Nothing in this subsection shall be construed to interfere with the ability of the Secretary to deny entry of any cargo into the United States.

(l) Report

Not later than 270 days after October 5, 2018, the Secretary, acting through the Commissioner, shall, in consultation with other appropriate government officials and the Commercial Operations Advisory Committee, submit a report to the appropriate congressional committees on the effectiveness of, and the need for any improvements to, the Container Security Initiative. The report shall include—

(1) a description of the technical assistance delivered to, as well as needed at, each designated seaport;

(2) a description of the human capital management plan at each designated seaport;

(3) a summary of the requests made by the United States to foreign governments to conduct physical or nonintrusive inspections of cargo at designated seaports, and whether each such request was granted or denied by the foreign government;

(4) an assessment of the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports and the effect on the flow of commerce at such seaports, as well as any recommendations for improving the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports;

(5) a description and assessment of the outcome of any security incident involving a foreign seaport designated under the Container Security Initiative;

(6) the rationale for the continuance of each port designated under CSI;

(7) a description of the potential for remote targeting to decrease the number of personnel who are deployed at foreign ports under CSI; and

(8) a summary and assessment of the aggregate number and extent of trade compliance lapses at each seaport designated under the Container Security Initiative.

(m) Authorization of appropriations

There are authorized to be appropriated to the United States Customs and Border Protection to carry out the provisions of this section—

(1) $144,000,000 for fiscal year 2008;

(2) $146,000,000 for fiscal year 2009; and

(3) $153,300,000 for fiscal year 2010.

(Pub. L. 109–347, title II, §205, Oct. 13, 2006, 120 Stat. 1906; Pub. L. 115–254, div. J, §1812, Oct. 5, 2018, 132 Stat. 3539.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (l). Pub. L. 115–254 struck out par. (1) designation and heading, substituted "Not later than 270 days after October 5, 2018," for "Not later than September 30, 2007," in introductory provisions, redesignated subpars. (A) to (H) of former par. (1) as pars. (1) to (8), respectively, and struck out former par. (2). Prior to amendment, text of par. (2) read as follows: "Not later than September 30, 2010, the Secretary,

acting through the Commissioner, shall, in consultation with other appropriate government officials and the Commercial Operations Advisory Committee, submit an updated report to the appropriate congressional committees on the effectiveness of, and the need for any improvements to, the Container Security Initiative. The updated report shall address each of the elements required to be included in the report provided for under paragraph (1)."

STATUTORY NOTES AND RELATED SUBSIDIARIES

INTERNATIONAL PORT AND FACILITY INSPECTION COORDINATION

Pub. L. 111–281, title VIII, §825, Oct. 15, 2010, 124 Stat. 3004, as amended by Pub. L. 114–120, title III, §320, Feb. 8, 2016, 130 Stat. 66, provided that:

"(a) COORDINATION.—The Secretary of Homeland Security shall, to the extent practicable, conduct the assessments required by the following provisions of law concurrently, or develop a process by which the assessments are coordinated between the Coast Guard and Customs and Border Protection:

"(1) Section 205 of the SAFE Port Act (6 U.S.C. 945).

"(2) Section 213 of that Act (6 U.S.C. 964 [963]).

"(3) Section 70108 of title 46, United States Code.

"(b) LIMITATION.—Nothing in subsection (a) shall be construed to affect or diminish the Secretary's authority or discretion—

"(1) to conduct an assessment of a foreign port at any time;

"(2) to compel the Secretary to conduct an assessment of a foreign port so as to ensure that 2 or more assessments are conducted concurrently; or

"(3) to cancel an assessment of a foreign port if the Secretary is unable to conduct 2 or more assessments concurrently.

"(c) MULTIPLE ASSESSMENT REPORT.—The Secretary shall provide written notice to the Committee on Commerce, Science, and Transportation of the Senate and the Committees on Transportation and Infrastructure and Homeland Security of the House of Representatives whenever the Secretary conducts 2 or more assessments of the same port within a 3-year period."

PART B—CUSTOMS–TRADE PARTNERSHIP AGAINST TERRORISM

§961. Establishment

(a) Establishment

The Secretary, acting through the Commissioner, is authorized to establish a voluntary government-private sector program (to be known as the "Customs–Trade Partnership Against Terrorism" or "C–TPAT") to strengthen and improve the overall security of the international supply chain and United States border security, and to facilitate the movement of secure cargo through the international supply chain, by providing benefits to participants meeting or exceeding the program requirements. Participants in C–TPAT shall include Tier 1 participants, Tier 2 participants, and Tier 3 participants.

(b) Minimum security requirements

The Secretary, acting through the Commissioner, shall review the minimum security requirements of C–TPAT at least once every year and update such requirements as necessary.

(Pub. L. 109–347, title II, §211, Oct. 13, 2006, 120 Stat. 1909.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CTPAT PILOT PROGRAM ON PARTICIPATION OF THIRD-PARTY LOGISTICS PROVIDERS

Pub. L. 118–98, Oct. 1, 2024, 138 Stat. 1575, provided that:

"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Customs Trade Partnership Against Terrorism Pilot Program Act of 2023' or the 'CTPAT Pilot Program Act of 2023'.

"SEC. 2. DEFINITIONS.

"In this Act:

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate; and

"(B) the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives.

"(2) CTPAT.—The term 'CTPAT' means the Customs Trade Partnership Against Terrorism established under subtitle B of title II of the Security and Accountability for Every Port Act (6 U.S.C. 961 et seq.).

"SEC. 3. PILOT PROGRAM ON PARTICIPATION OF THIRD-PARTY LOGISTICS PROVIDERS IN CTPAT.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary of Homeland Security shall carry out a pilot program to assess whether allowing entities described in subsection (b) to participate in CTPAT would enhance port security, combat terrorism, prevent supply chain security breaches, or otherwise meet the goals of CTPAT.

"(2) FEDERAL REGISTER NOTICE.—Not later than one year after the date of the enactment of this Act [Oct. 1, 2024], the Secretary shall publish in the Federal Register a notice specifying the requirements for the pilot program required by paragraph (1).

"(b) ENTITIES DESCRIBED.—An entity described in this subsection is—

"(1) a non-asset-based third-party logistics provider that—

"(A) arranges international transportation of freight and is licensed by the Department of Transportation; and

"(B) meets such other requirements as the Secretary specifies in the Federal Register notice required by subsection (a)(2); or

"(2) an asset-based third-party logistics provider that—

"(A) facilitates cross border activity and is licensed or bonded by the Federal Maritime Commission, the Transportation Security Administration, U.S. Customs and Border Protection, or the Department of Transportation;

"(B) manages and executes logistics services using its own warehousing assets and resources on behalf of its customers; and

"(C) meets such other requirements as the Secretary specifies in the Federal Register notice required by subsection (a)(2).

"(c) REQUIREMENTS.—In carrying out the pilot program required by subsection (a)(1), the Secretary shall—

"(1) ensure that—

"(A) not more than 10 entities described in paragraph (1) of subsection (b) participate in the pilot program; and

"(B) not more than 10 entities described in paragraph (2) of that subsection participate in the program;

"(2) provide for the participation of those entities on a voluntary basis;

"(3) continue the program for a period of not less than one year after the date on which the Secretary publishes the Federal Register notice required by subsection (a)(2); and

"(4) terminate the pilot program not more than 5 years after that date.

"(d) REPORT REQUIRED.—Not later than 180 days after the termination of the pilot program under subsection (c)(4), the Secretary shall submit to the appropriate congressional committees a report on the findings of, and any recommendations arising from, the pilot program concerning the participation in CTPAT of entities described in subsection (b), including an assessment of participation by those entities.

"SEC. 4. REPORT ON EFFECTIVENESS OF CTPAT.

"(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act [Oct. 1, 2024], the Comptroller General of the United States shall submit to the appropriate congressional committees a report assessing the effectiveness of CTPAT.

"(b) ELEMENTS.—The report required by subsection (a) shall include the following:

"(1) An analysis of—

"(A) security incidents in the cargo supply chain during the 5-year period preceding submission of the report that involved criminal activity, including drug trafficking, human smuggling, commercial fraud, or terrorist activity; and

"(B) whether those incidents involved participants in CTPAT or entities not participating in CTPAT.

"(2) An analysis of causes for the suspension or removal of entities from participating in CTPAT as a result of security incidents during that 5-year period.

"(3) An analysis of the number of active CTPAT participants involved in one or more security incidents while maintaining their status as participants.

"(4) Recommendations to the Commissioner of U.S. Customs and Border Protection for improvements to CTPAT to improve prevention of security incidents in the cargo supply chain involving participants in CTPAT.

"SEC. 5. NO ADDITIONAL FUNDS AUTHORIZED.

"No additional funds are authorized to be appropriated for the purpose of carrying out this Act."

§962. Eligible entities

Importers, customs brokers, forwarders, air, sea, land carriers, contract logistics providers, and other entities in the international supply chain and intermodal transportation system are eligible to apply to voluntarily enter into partnerships with the Department under C–TPAT.

(Pub. L. 109–347, title II, §212, Oct. 13, 2006, 120 Stat. 1909.)

§963. Minimum requirements

An applicant seeking to participate in C–TPAT shall—

(1) demonstrate a history of moving cargo in the international supply chain;

(2) conduct an assessment of its supply chain based upon security criteria established by the Secretary, acting through the Commissioner, including—

(A) business partner requirements;

(B) container security;

(C) physical security and access controls;

(D) personnel security;

(E) procedural security;

(F) security training and threat awareness; and

(G) information technology security;

(3) implement and maintain security measures and supply chain security practices meeting security criteria established by the Commissioner; and

(4) meet all other requirements established by the Commissioner, in consultation with the Commercial Operations Advisory Committee.

(Pub. L. 109–347, title II, §213, Oct. 13, 2006, 120 Stat. 1909.)

§964. Tier 1 participants in C–TPAT

(a) Benefits

The Secretary, acting through the Commissioner, shall offer limited benefits to a Tier 1 participant who has been certified in accordance with the guidelines referred to in subsection (b). Such benefits may include a reduction in the score assigned pursuant to the Automated Targeting System of not greater than 20 percent of the high-risk threshold established by the Secretary.

(b) Guidelines

Not later than 180 days after October 13, 2006, the Secretary, acting through the Commissioner, shall update the guidelines for certifying a C–TPAT participant's security measures and supply chain security practices under this section. Such guidelines shall include a background investigation and extensive documentation review.

(c) Timeframe

To the extent practicable, the Secretary, acting through the Commissioner, shall complete the Tier 1 certification process within 90 days of receipt of an application for participation in C–TPAT.

(Pub. L. 109–347, title II, §214, Oct. 13, 2006, 120 Stat. 1910.)

§965. Tier 2 participants in C–TPAT

(a) Validation

The Secretary, acting through the Commissioner, shall validate the security measures and supply chain security practices of a Tier 1 participant in accordance with the guidelines referred to in subsection (c). Such validation shall include on-site assessments at appropriate foreign locations utilized by the Tier 1 participant in its supply chain and shall, to the extent practicable, be completed not later than 1 year after certification as a Tier 1 participant.

(b) Benefits

The Secretary, acting through the Commissioner, shall extend benefits to each C–TPAT participant that has been validated as a Tier 2 participant under this section, which may include—

(1) reduced scores in the Automated Targeting System;

(2) reduced examinations of cargo; and

(3) priority searches of cargo.

(c) Guidelines

Not later than 180 days after October 13, 2006, the Secretary, acting through the Commissioner, shall develop a schedule and update the guidelines for validating a participant's security measures and supply chain security practices under this section.

(Pub. L. 109–347, title II, §215, Oct. 13, 2006, 120 Stat. 1910.)

§966. Tier 3 participants in C–TPAT

(a) In general

The Secretary, acting through the Commissioner, shall establish a third tier of C–TPAT participation that offers additional benefits to participants who demonstrate a sustained commitment to maintaining security measures and supply chain security practices that exceed the guidelines established for validation as a Tier 2 participant in C–TPAT under section 965 of this title.

(b) Criteria

The Secretary, acting through the Commissioner, shall designate criteria for validating a C–TPAT participant as a Tier 3 participant under this section. Such criteria may include—

(1) compliance with any additional guidelines established by the Secretary that exceed the guidelines established pursuant to section 965 of this title for validating a C–TPAT participant as a Tier 2 participant, particularly with respect to controls over access to cargo throughout the supply chain;

(2) submission of additional information regarding cargo prior to loading, as determined by the Secretary;

(3) utilization of container security devices, technologies, policies, or practices that meet standards and criteria established by the Secretary; and

(4) compliance with any other cargo requirements established by the Secretary.

(c) Benefits

The Secretary, acting through the Commissioner, in consultation with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee, shall extend benefits to each C–TPAT participant that has been validated as a Tier 3 participant under this section, which may include—

(1) the expedited release of a Tier 3 participant's cargo in destination ports within the United States during all threat levels designated by the Secretary;

(2) further reduction in examinations of cargo;

(3) priority for examinations of cargo; and

(4) further reduction in the risk score assigned pursuant to the Automated Targeting System; and

(5) inclusion in joint incident management exercises, as appropriate.

(d) Deadline

Not later than 2 years after October 13, 2006, the Secretary, acting through the Commissioner, shall designate appropriate criteria pursuant to subsection (b) and provide benefits to validated Tier 3 participants pursuant to subsection (c).

(Pub. L. 109–347, title II, §216, Oct. 13, 2006, 120 Stat. 1910.)

§967. Consequences for lack of compliance

(a) In general

If at any time a C–TPAT participant's security measures and supply chain security practices fail to meet any of the requirements under this part, the Commissioner may deny the participant benefits otherwise available under this part, in whole or in part. The Commissioner shall develop procedures that provide appropriate protections to C–TPAT participants before benefits are revoked. Such procedures may not limit the ability of the Commissioner to take actions to protect the national security of the United States.

(b) False or misleading information

If a C–TPAT participant knowingly provides false or misleading information to the Commissioner during the validation process provided for under this part, the Commissioner shall suspend or expel the participant from C–TPAT for an appropriate period of time. The Commissioner, after the completion of the process under subsection (c), may publish in the Federal Register a list of participants who have been suspended or expelled from C–TPAT pursuant to this subsection, and may make such list available to C–TPAT participants.

(c) Right of appeal

(1) In general

A C–TPAT participant may appeal a decision of the Commissioner pursuant to subsection (a). Such appeal shall be filed with the Secretary not later than 90 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

(2) Appeals of other decisions

A C–TPAT participant may appeal a decision of the Commissioner pursuant to subsection (b). Such appeal shall be filed with the Secretary not later than 30 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

(Pub. L. 109–347, title II, §217, Oct. 13, 2006, 120 Stat. 1911.)

§968. Third party validations

(a) Plan

The Secretary, acting through the Commissioner, shall develop a plan to implement a 1-year voluntary pilot program to test and assess the feasibility, costs, and benefits of using third party entities to conduct validations of C–TPAT participants.

(b) Consultations

Not later than 120 days after October 13, 2006, after consulting with private sector stakeholders, including the Commercial Operations Advisory Committee, the Secretary shall submit a report to the appropriate congressional committees on the plan described in subsection (a).

(c) Pilot program

(1) In general

Not later than 1 year after the consultations described in subsection (b), the Secretary shall carry out the 1-year pilot program to conduct validations of C–TPAT participants using third party entities described in subsection (a).

(2) Authority of the Secretary

The decision to validate a C–TPAT participant is solely within the discretion of the Secretary, or the Secretary's designee.

(d) Certification of third party entities

The Secretary shall certify a third party entity to conduct validations under subsection (c) if the entity—

(1) demonstrates to the satisfaction of the Secretary that the entity has the ability to perform validations in accordance with standard operating procedures and requirements designated by the Secretary; and

(2) agrees—

(A) to perform validations in accordance with such standard operating procedures and requirements (and updates to such procedures and requirements); and

(B) to maintain liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary; and

(3) signs an agreement to protect all proprietary information of C–TPAT participants with respect to which the entity will conduct validations.

(e) Information for establishing limits of liability insurance

A third party entity seeking a certificate under subsection (d) shall submit to the Secretary necessary information for establishing the limits of liability insurance required to be maintained by the entity under this Act.

(f) Additional requirements

The Secretary shall ensure that—

(1) any third party entity certified under this section does not have—

(A) any beneficial interest in or any direct or indirect control over the C–TPAT participant for which the validation services are performed; or

(B) any other conflict of interest with respect to the C–TPAT participant; and

(2) the C–TPAT participant has entered into a contract with the third party entity under which the C–TPAT participant agrees to pay all costs associated with the validation.

(g) Monitoring

(1) In general

The Secretary shall regularly monitor and inspect the operations of a third party entity conducting validations under subsection (c) to ensure that the entity is meeting the minimum standard operating procedures and requirements for the validation of C–TPAT participants established by the Secretary and all other applicable requirements for validation services.

(2) Revocation

If the Secretary determines that a third party entity is not meeting the minimum standard operating procedures and requirements designated by the Secretary under subsection (d)(1), the Secretary shall—

(A) revoke the entity's certificate of conformance issued under subsection (d)(1); and

(B) review any validations conducted by the entity.

(h) Limitation on authority

The Secretary may only grant a C–TPAT validation by a third party entity pursuant to subsection (c) if the C–TPAT participant voluntarily submits to validation by such third party entity.

(i) Report

Not later than 30 days after the completion of the pilot program conducted pursuant to subsection (c), the Secretary shall submit a report to the appropriate congressional committees that contains—

(1) the results of the pilot program, including the extent to which the pilot program ensured sufficient protection for proprietary commercial information;

(2) the cost and efficiency associated with validations under the pilot program;

(3) the impact of the pilot program on the rate of validations conducted under C–TPAT;

(4) any impact on national security of the pilot program; and

(5) any recommendations by the Secretary based upon the results of the pilot program.

(Pub. L. 109–347, title II, §218, Oct. 13, 2006, 120 Stat. 1912.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (e), is Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1884, known as the Security and Accountability For Every Port Act of 2006 or the SAFE Port Act. For complete classification of this Act to the Code, see Tables.

§969. Revalidation

The Secretary, acting through the Commissioner, shall develop and implement—

(1) a revalidation process for Tier 2 and Tier 3 participants;

(2) a framework based upon objective criteria for identifying participants for periodic revalidation not less frequently than once during each 4-year period following the initial validation; and

(3) an annual plan for revalidation that includes—

(A) performance measures;

(B) an assessment of the personnel needed to perform the revalidations; and

(C) the number of participants that will be revalidated during the following year.

(Pub. L. 109–347, title II, §219, Oct. 13, 2006, 120 Stat. 1913.)

§970. Noncontainerized cargo

The Secretary, acting through the Commissioner, shall consider the potential for participation in C–TPAT by importers of noncontainerized cargoes that otherwise meet the requirements under this part.

(Pub. L. 109–347, title II, §220, Oct. 13, 2006, 120 Stat. 1914.)

§971. C–TPAT program management

(a) In general

The Secretary, acting through the Commissioner, shall establish sufficient internal quality controls and record management to support the management systems of C–TPAT. In managing the program, the Secretary shall ensure that the program includes:

(1) Strategic plan

A 5-year plan to identify outcome-based goals and performance measures of the program.

(2) Annual plan

An annual plan for each fiscal year designed to match available resources to the projected workload.

(3) Standardized work program

A standardized work program to be used by agency personnel to carry out the certifications, validations, and revalidations of participants. The Secretary shall keep records and monitor staff hours associated with the completion of each such review.

(b) Documentation of reviews

The Secretary, acting through the Commissioner, shall maintain a record management system to document determinations on the reviews of each C–TPAT participant, including certifications, validations, and revalidations.

(c) Confidential information safeguards

In consultation with the Commercial Operations Advisory Committee, the Secretary, acting through the Commissioner, shall develop and implement procedures to ensure the protection of confidential data collected, stored, or shared with government agencies or as part of the application, certification, validation, and revalidation processes.

(d) Resource management staffing plan

The Secretary, acting through the Commissioner, shall—

(1) develop a staffing plan to recruit and train staff (including a formalized training program) to meet the objectives identified in the strategic plan of the C–TPAT program; and

(2) provide cross-training in postincident trade resumption for personnel who administer the C–TPAT program.

(e) Report to Congress

In connection with the President's annual budget submission for the Department, the Secretary shall report to the appropriate congressional committees on the progress made by the Commissioner to certify, validate, and revalidate C–TPAT participants. Such report shall be due on the same date that the President's budget is submitted to the Congress.

(Pub. L. 109–347, title II, §221, Oct. 13, 2006, 120 Stat. 1914.)

§972. Additional personnel

For fiscal years 2008 and 2009, the Commissioner shall increase by not less than 50 the number of full-time personnel engaged in the validation and revalidation of C–TPAT participants (over the number of such personnel on the last day of the previous fiscal year), and shall provide appropriate training and support to such additional personnel.

(Pub. L. 109–347, title II, §222, Oct. 13, 2006, 120 Stat. 1914.)

§973. Authorization of appropriations

(a) C–TPAT

There are authorized to be appropriated to the United States Customs and Border Protection to

carry out the provisions of sections 961 through 971 of this title to remain available until expended—

(1) $65,000,000 for fiscal year 2008;

(2) $72,000,000 for fiscal year 2009; and

(3) $75,600,000 for fiscal year 2010.

(b) Additional personnel

In addition to any amounts otherwise appropriated to the United States Customs and Border Protection, there are authorized to be appropriated for the purpose of meeting the staffing requirement provided for in section 972 of this title, to remain available until expended—

(1) $8,500,000 for fiscal year 2008;

(2) $17,600,000 for fiscal year 2009;

(3) $19,000,000 for fiscal year 2010;

(4) $20,000,000 for fiscal year 2011; and

(5) $21,000,000 for fiscal year 2012.

(Pub. L. 109–347, title II, §223, Oct. 13, 2006, 120 Stat. 1915.)

PART C—MISCELLANEOUS PROVISIONS

§981. Pilot integrated scanning system

(a) Designations

Not later than 90 days after October 13, 2006, the Secretary shall designate 3 foreign seaports through which containers pass or are transshipped to the United States for the establishment of pilot integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment. In making the designations under this subsection, the Secretary shall consider 3 distinct ports with unique features and differing levels of trade volume.

(b) Coordination

The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment through the Department of Energy's Second Line of Defense and Megaports programs; or

(2) work with the private sector or, when possible, host governments to obtain radiation detection equipment that meets both the Department's and the Department of Energy's technical specifications for such equipment.

(c) Pilot system implementation

Not later than 1 year after October 13, 2006, the Secretary shall achieve a full-scale implementation of the pilot integrated scanning system at the ports designated under subsection (a), which—

(1) shall scan all containers destined for the United States that are loaded in such ports;

(2) shall electronically transmit the images and information to appropriate United States Government personnel in the country in which the port is located or in the United States for evaluation and analysis;

(3) shall resolve every radiation alarm according to established Department procedures;

(4) shall utilize the information collected to enhance the Automated Targeting System or other relevant programs;

(5) shall store the information for later retrieval and analysis; and

(6) may provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(d) Report

Not later than 180 days after achieving full-scale implementation under subsection (c), the Secretary, in consultation with the Secretary of State and, as appropriate, the Secretary of Energy, shall submit a report to the appropriate congressional committees, that includes—

(1) an evaluation of the lessons derived from the pilot system implemented under this subsection;

(2) an analysis of the efficacy of the Automated Targeting System or other relevant programs in utilizing the images captured to examine high-risk containers;

(3) an evaluation of the effectiveness of the integrated scanning system in detecting shielded and unshielded nuclear and radiological material;

(4) an evaluation of software and other technologies that are capable of automatically identifying potential anomalies in scanned containers; and

(5) an analysis of the need and feasibility of expanding the integrated scanning system to other container security initiative ports, including—

(A) an analysis of the infrastructure requirements;

(B) a projection of the effect on current average processing speed of containerized cargo;

(C) an evaluation of the scalability of the system to meet both current and future forecasted trade flows;

(D) the ability of the system to automatically maintain and catalog appropriate data for reference and analysis in the event of a transportation disruption;

(E) an analysis of requirements, including costs, to install and maintain an integrated scanning system;

(F) the ability of administering personnel to efficiently manage and utilize the data produced by a nonintrusive scanning system;

(G) the ability to safeguard commercial data generated by, or submitted to, a nonintrusive scanning system; and

(H) an assessment of the reliability of currently available technology to implement an integrated scanning system.

(Pub. L. 109–347, title II, §231, Oct. 13, 2006, 120 Stat. 1915.)

§981a. Pilot integrated scanning system

(a) Designations

(1) In general

Not later than 90 days after October 4, 2006, the Secretary of Homeland Security (referred to in this section as the "Secretary") shall designate three foreign seaports through which containers pass or are transshipped to the United States to pilot an integrated scanning system that couples nonintrusive imaging equipment and radiation detection equipment, which may be provided by the Megaports Initiative of the Department of Energy. In making designations under this subsection, the Secretary shall consider three distinct ports with unique features and differing levels of trade volume.

(2) Collaboration and cooperation

The Secretary shall collaborate with the Secretary of Energy and cooperate with the private sector and host foreign government to implement the pilot program under this subsection.

(b) Implementation

Not later than one year after October 4, 2006, the Secretary shall achieve a full-scale implementation of the pilot integrated screening system, which shall—

(1) scan all containers destined for the United States that transit through the terminal;

(2) electronically transmit the images and information to the container security initiative personnel in the host country and/or Customs and Border Protection personnel in the United States for evaluation and analysis;

(3) resolve every radiation alarm according to established Department procedures;

(4) utilize the information collected to enhance the Automated Targeting System or other relevant programs; and

(5) store the information for later retrieval and analysis.

(c) Evaluation

The Secretary shall evaluate the pilot program in subsection (b) to determine whether such a system—

(1) has a sufficiently low false alarm rate for use in the supply chain;

(2) is capable of being deployed and operated at ports overseas, including consideration of cost, personnel, and infrastructure required to operate the system;

(3) is capable of integrating, where necessary, with existing systems;

(4) does not significantly impact trade capacity and flow of cargo at foreign or United States ports; and

(5) provides an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(d) Report

Not later than 120 days after achieving full-scale implementation under subsection (b), the Secretary, in consultation with the Secretary of Energy and the Secretary of State, shall submit a report, to the appropriate congressional committees, that includes—

(1) an evaluation of the lessons derived from the pilot program implemented under this section;

(2) an analysis of the efficacy of the Automated Targeted System or other relevant programs in utilizing the images captured to examine high-risk containers;

(3) an evaluation of software that is capable of automatically identifying potential anomalies in scanned containers; and

(4) a plan and schedule to expand the integrated scanning system developed under this section to other container security initiative ports.

(e) Implementation

If the Secretary determines the available technology meets the criteria outlined in subsection (c), the Secretary, in cooperation with the Secretary of State, shall seek to secure the cooperation of foreign governments to initiate and maximize the use of such technology at foreign ports to scan all cargo bound for the United States as quickly as possible.

(Pub. L. 109–295, title V, §558, Oct. 4, 2006, 120 Stat. 1392.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2007, and not as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, which comprises this chapter.

§982. Screening and scanning of cargo containers

(a) One hundred percent screening of cargo containers and 100 percent scanning of high-risk containers

(1) Screening of cargo containers

The Secretary shall ensure that 100 percent of the cargo containers originating outside the United States and unloaded at a United States seaport undergo a screening to identify high-risk containers.

(2) Scanning of high-risk containers

The Secretary shall ensure that 100 percent of the containers that have been identified as high-risk under paragraph (1), or through other means, are scanned or searched before such containers leave a United States seaport facility.

(b) Full-scale implementation

(1) In general

A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.

(2) Application

Paragraph (1) shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of—

(A) July 1, 2012; or

(B) such other date as may be established by the Secretary under paragraph (3).

(3) Establishment of earlier deadline

The Secretary shall establish a date under (2)(B) [1] pursuant to the lessons learned through the pilot integrated scanning systems established under section 981 of this title.

(4) Extensions

The Secretary may extend the date specified in paragraph (2)(A) or (2)(B) for 2 years, and may renew the extension in additional 2-year increments, for containers loaded in a port or ports, if the Secretary certifies to Congress that at least two of the following conditions exist:

(A) Systems to scan containers in accordance with paragraph (1) are not available for purchase and installation.

(B) Systems to scan containers in accordance with paragraph (1) do not have a sufficiently low false alarm rate for use in the supply chain.

(C) Systems to scan containers in accordance with paragraph (1) cannot be purchased, deployed, or operated at ports overseas, including, if applicable, because a port does not have the physical characteristics to install such a system.

(D) Systems to scan containers in accordance with paragraph (1) cannot be integrated, as necessary, with existing systems.

(E) Use of systems that are available to scan containers in accordance with paragraph (1) will significantly impact trade capacity and the flow of cargo.

(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(5) Exemption for military cargo

Notwithstanding any other provision in the section, supplies bought by the Secretary of Defense and transported in compliance section 2631 of title 10 and military cargo of foreign countries are exempt from the requirements of this section.

(6) Report on extensions

An extension under paragraph (4) for a port or ports shall take effect upon the expiration of the 60-day period beginning on the date the Secretary provides a report to Congress that—

(A) states what container traffic will be affected by the extension;

(B) provides supporting evidence to support the Secretary's certification of the basis for the extension; and

(C) explains what measures the Secretary is taking to ensure that scanning can be implemented as early as possible at the port or ports that are the subject of the report.

(7) Report on renewal of extension

If an extension under paragraph (4) takes effect, the Secretary shall, after one year, submit a

report to Congress on whether the Secretary expects to seek to renew the extension.

(8) Scanning technology standards

In implementing paragraph (1), the Secretary shall—

(A) establish technological and operational standards for systems to scan containers;

(B) ensure that the standards are consistent with the global nuclear detection architecture developed under the Homeland Security Act of 2002 [6 U.S.C. 101 et seq.]; and

(C) coordinate with other Federal agencies that administer scanning or detection programs at foreign ports.

(9) International trade and other obligations

In carrying out this subsection, the Secretary shall consult with appropriate Federal departments and agencies and private sector stakeholders, and ensure that actions under this section do not violate international trade obligations, and are consistent with the World Customs Organization framework, or other international obligations of the United States.

(c) Report

Not later than 6 months after the submission of a report under section 981(d) of this title, and every 6 months thereafter, the Secretary shall submit a report to the appropriate congressional committees describing the status of full-scale deployment under subsection (b) and the cost of deploying the system at each foreign port at which the integrated scanning systems are deployed.

(Pub. L. 109–347, title II, §232, Oct. 13, 2006, 120 Stat. 1916; Pub. L. 110–53, title XVII, §1701(a), Aug. 3, 2007, 121 Stat. 489.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Homeland Security Act of 2002, referred to in subsec. (b)(8)(B), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, which is classified principally to chapter 1 (§101 et seq.) of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2007—Subsec. (b). Pub. L. 110–53 reenacted heading without change and amended text of subsec. (b) generally. Prior to amendment, text related to full deployment of an integrated scanning system after the Secretary had determined that such system had met section 981(c) requirements, had a sufficiently low false alarm rate, was capable of being deployed overseas, was capable of integrating with existing systems, would not significantly impact trade flow, and had provided for automated notification of high-risk cargo.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CARGO CONTAINER SCANNING TECHNOLOGY REVIEW

Pub. L. 115–254, div. K, title I, §1979, Oct. 5, 2018, 132 Stat. 3618, provided that:

"(a) DESIGNATIONS.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act [Oct. 5, 2018], and not less frequently than once every 5 years thereafter until the date of full-scale implementation of 100 percent screening of cargo containers and 100 percent scanning of high-risk containers required under section 232 of the SAFE Port Act (6 U.S.C. 982), the Secretary [of Homeland Security] shall solicit proposals for scanning technologies, consistent with the standards under subsection (b)(8) of that section, to improve scanning of cargo at domestic ports.

"(2) EVALUATION.—In soliciting proposals under paragraph (1), the Secretary shall establish measures to assess the performance of the proposed scanning technologies, including—

"(A) the rate of false positives;

"(B) the delays in processing times; and

"(C) the impact on the supply chain.

"(b) PILOT PROGRAM.—

"(1) ESTABLISHMENT.—The Secretary may establish a pilot program to determine the efficacy of a

scanning technology referred to in subsection (a).

"(2) APPLICATION PROCESS.—In carrying out the pilot program under this subsection, the Secretary shall—

"(A) solicit applications from domestic ports;

"(B) select up to 4 domestic ports to participate in the pilot program; and

"(C) select ports with unique features and differing levels of trade volume.

"(3) REPORT.—Not later than 1 year after initiating a pilot program under paragraph (1), the Secretary shall submit to the appropriate committees of Congress [Committees on Commerce, Science and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] a report on the pilot program, including—

"(A) an evaluation of the scanning technologies proposed to improve security at domestic ports and to meet the full-scale implementation requirement;

"(B) the costs to implement a pilot program;

"(C) the benefits of the proposed scanning technologies;

"(D) the impact of the pilot program on the supply chain; and

"(E) recommendations for implementation of advanced cargo scanning technologies at domestic ports.

"(4) SHARING PILOT PROGRAM TESTING RESULTS.—The results of the pilot testing of advanced cargo scanning technologies shall be shared, as appropriate, with government agencies and private stakeholders whose responsibilities encompass the secure transport of cargo."

[1] *So in original. Probably should be "paragraph (2)(B)".*

§983. Inspection technology and training

(a) In general

The Secretary, in coordination with the Secretary of State, the Secretary of Energy, and appropriate representatives of other Federal agencies, may provide technical assistance, equipment, and training to facilitate the implementation of supply chain security measures at ports designated under the Container Security Initiative.

(b) Acquisition and training

Unless otherwise prohibited by law, the Secretary may—

(1) lease, loan, provide, or otherwise assist in the deployment of nonintrusive inspection and radiation detection equipment at foreign land and sea ports under such terms and conditions as the Secretary prescribes, including nonreimbursable loans or the transfer of ownership of equipment; and

(2) provide training and technical assistance for domestic or foreign personnel responsible for operating or maintaining such equipment.

(Pub. L. 109–347, title II, §233(a), Oct. 13, 2006, 120 Stat. 1917; Pub. L. 115–254, div. J, §1816(e)(1), Oct. 5, 2018, 132 Stat. 3541.)

EDITORIAL NOTES

AMENDMENTS

2018—Pub. L. 115–254, which directed the general amendment of "section 233 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 983)", was executed by generally amending section 233(a) of the Security and Accountability for Every Port Act of 2006, which comprises this section, to reflect the probable intent of Congress. Prior to amendment, section read as follows:

"(1) IN GENERAL.—The Secretary, in coordination with the Secretary of State, the Secretary of Energy, and appropriate representatives of other Federal agencies, may provide technical assistance, equipment, and training to facilitate the implementation of supply chain security measures at ports designated under the Container Security Initiative.

"(2) ACQUISITION AND TRAINING.—Unless otherwise prohibited by law, the Secretary may—

"(A) lease, loan, provide, or otherwise assist in the deployment of nonintrusive inspection and radiation detection equipment at foreign land and sea ports under such terms and conditions as the Secretary prescribes, including nonreimbursable loans or the transfer of ownership of equipment; and

"(B) provide training and technical assistance for domestic or foreign personnel responsible for operating or maintaining such equipment."

§984. Repealed. Pub. L. 115–254, div. J, §1816(f), Oct. 5, 2018, 132 Stat. 3541

Section, Pub. L. 109–347, title II, §235, Oct. 13, 2006, 120 Stat. 1919, related to pilot program to improve the security of empty containers.

§985. Information sharing relating to supply chain security cooperation

(a) Purposes

The purposes of this section are—

(1) to establish continuing liaison and to provide for supply chain security cooperation between Department and the private sector; and

(2) to provide for regular and timely interchange of information between the private sector and the Department concerning developments and security risks in the supply chain environment.

(b) System

The Secretary shall develop a system to collect from and share appropriate risk information related to the supply chain with the private sector entities determined appropriate by the Secretary.

(c) Consultation

In developing the system under subsection (b), the Secretary shall consult with the Commercial Operations Advisory Committee and a broad range of public and private sector entities likely to utilize the system, including importers, exporters, carriers, customs brokers, and freight forwarders, among other parties.

(d) Independently obtained information

Nothing in this section shall be construed to limit or otherwise affect the ability of a Federal, State, or local government entity, under applicable law, to obtain supply chain security information, including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(e) Authority to issue warnings

The Secretary may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential risks to the supply chain as appropriate. In issuing a warning, the Secretary shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted supply chain security information that forms the basis for the warning; and

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(Pub. L. 109–347, title II, §236, Oct. 13, 2006, 120 Stat. 1919.)

SUBCHAPTER III—ADMINISTRATION

§1001. Designation of liaison office of Department of State

The Secretary of State shall designate a liaison office within the Department of State to assist the Secretary, as appropriate, in negotiating cargo security-related international agreements.

(Pub. L. 109–347, title III, §301(b), Oct. 13, 2006, 120 Stat. 1920.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

RULE OF CONSTRUCTION

Nothing in this section to be construed to affect the authorities, functions, or capabilities of the Coast Guard to perform its missions or the requirement under section 468 of this title that those authorities, functions, and capabilities be maintained intact, see section 301(c) of Pub. L. 109–347, set out as a note under section 239 of this title.

§1002. Homeland Security Science and Technology Advisory Committee

The Under Secretary for Science and Technology shall utilize the Homeland Security Science and Technology Advisory Committee, as appropriate, to provide outside expertise in advancing cargo security technology.

(Pub. L. 109–347, title III, §302(c), Oct. 13, 2006, 120 Stat. 1921.)

§1003. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security

(a) In general

The Secretary shall—

(1) direct research, development, testing, and evaluation efforts in furtherance of maritime and cargo security;

(2) coordinate with public and private sector entities to develop and test technologies, and process innovations in furtherance of these objectives; and

(3) evaluate such technologies.

(b) Coordination

The Secretary, in coordination with the Under Secretary for Science and Technology, the Assistant Secretary for Policy, the Commandant of the Coast Guard, the Director for Domestic Nuclear Detection,[1] the Chief Financial Officer, and the heads of other appropriate offices or entities of the Department, shall ensure that—

(1) research, development, testing, and evaluation efforts funded by the Department in furtherance of maritime and cargo security are coordinated within the Department and with other appropriate Federal agencies to avoid duplication of efforts; and

(2) the results of such efforts are shared throughout the Department and with other Federal, State, and local agencies, as appropriate.

(Pub. L. 109–347, title III, §303, Oct. 13, 2006, 120 Stat. 1921.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Director for Domestic Nuclear Detection deemed to be a reference to the Assistant Secretary for the Countering Weapons of Mass Destruction Office, see section 2(b)(1)(B) of Pub. L. 115–387, set out as a note under section 591 of this title.

[1] *See Change of Name note below.*

CHAPTER 4—TRANSPORTATION SECURITY

SUBCHAPTER I—TRANSPORTATION SECURITY PLANNING AND INFORMATION SHARING

Sec.
1101. Definitions.
1102. National Domestic Preparedness Consortium.
1103. National Transportation Security Center of Excellence.
1104. Immunity for reports of suspected terrorist activity or suspicious behavior and response.

SUBCHAPTER II—TRANSPORTATION SECURITY ENHANCEMENTS

1111. Definitions.
1112. Authorization of Visible Intermodal Prevention and Response teams.
1113. Surface transportation security inspectors.
1114. Surface transportation security technology information sharing.
1115. TSA personnel limitations.
1116. National explosives detection canine team training program.
1117. Roles of the Department of Homeland Security and the Department of Transportation.
1118. Biometrics expansion.
1119. Voluntary use of credentialing.

SUBCHAPTER III—PUBLIC TRANSPORTATION SECURITY

1131. Definitions.
1132. Findings.
1133. National Strategy for Public Transportation Security.
1134. Security assessments and plans.
1135. Public transportation security assistance.
1136. Security exercises.
1137. Public transportation security training program.
1137a. Local law enforcement security training.
1138. Public transportation research and development.
1139. Information sharing.
1140. Threat assessments.
1141. Reporting requirements.
1142. Public transportation employee protections.
1143. Security background checks of covered individuals for public transportation.
1144. Limitation on fines and civil penalties.

SUBCHAPTER IV—SURFACE TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

1151. Definitions.
1152. Oversight and grant procedures.
1153. Authorization of appropriations.
1154. Public awareness.
1155. Security awareness program.
1156. Nuclear material and explosive detection technology.

PART B—RAILROAD SECURITY

1161. Railroad transportation security risk assessment and National Strategy.
1162. Railroad carrier assessments and plans.
1163. Railroad security assistance.
1164. Systemwide Amtrak security upgrades.
1165. Fire and life safety improvements.
1166. Railroad carrier exercises.
1167. Railroad security training program.

1168. Railroad security research and development.
1169. Railroad tank car security testing.
1170. Security background checks of covered individuals.
1171. International railroad security program.
1172. Railroad security enhancements; Model State legislation.

PART C—OVER-THE-ROAD BUS AND TRUCKING SECURITY

1181. Over-the-road bus security assessments and plans.
1182. Over-the-road bus security assistance.
1183. Over-the-road bus exercises.
1184. Over-the-road bus security training program.
1185. Over-the-road bus security research and development.
1186. Memorandum of Understanding annex.

PART D—HAZARDOUS MATERIAL AND PIPELINE SECURITY

1201. Railroad routing of security-sensitive materials.
1202. Railroad security-sensitive material tracking.
1203. Hazardous materials highway routing.
1204. Motor carrier security-sensitive material tracking.
1205. Hazardous materials security inspections and study.
1206. Use of transportation security card in hazmat licensing.
1207. Pipeline security inspections and enforcement.
1208. Pipeline security and incident recovery plan.

SUBCHAPTER I—TRANSPORTATION SECURITY PLANNING AND INFORMATION SHARING

§1101. Definitions

For purposes of this subchapter, the following terms apply:

(1) Department

The term "Department" means the Department of Homeland Security.

(2) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(Pub. L. 110–53, title XII, §1201, Aug. 3, 2007, 121 Stat. 381.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title XII of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 381, which enacted this subchapter, amended section 114 of Title 49, Transportation, and enacted provisions set out as a note under section 114 of Title 49. For complete classification of title XII to the Code, see Tables.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

Pub. L. 110–53, title XIV, §1401, Aug. 3, 2007, 121 Stat. 400, provided that: "This title [enacting subchapter III of this chapter] may be cited as the 'National Transit Systems Security Act of 2007'."

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13416. STRENGTHENING SURFACE TRANSPORTATION SECURITY

Ex. Ord. No. 13416, Dec. 5, 2006, 71 F.R. 71033, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to strengthen the security of the Nation's surface transportation systems and thereby enhance the protection of the people, property, and territory of the United States of America against terrorist attacks, it is hereby ordered as follows:

SECTION 1. *Policy*. The security of our Nation's surface transportation systems is a national priority, vital to our economy, and essential to the security of our Nation. Federal, State, local, and tribal governments, the private sector, and the public share responsibility for the security of surface transportation. It is the policy of the United States to protect the people, property, and territory of the United States by facilitating the implementation of a comprehensive, coordinated, and efficient security program to protect surface transportation systems within and adjacent to the United States against terrorist attacks.

SEC. 2. *Definitions*. For purposes of this order:

(a) "agencies" means those executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;

(b) "Secretary" means the Secretary of Homeland Security;

(c) "security guideline" means any security-related guidance that the Secretary recommends, for implementation on a voluntary basis, to enhance the security of surface transportation;

(d) "security requirement" means any "regulatory action" as defined in section 3 of Executive Order 12866 of September 30, 1993, as amended (Regulatory Planning and Review), including security directives when appropriate, to implement measures to enhance the security of surface transportation;

(e) "surface transportation modes" means mass transit, commuter and long-distance passenger rail, freight rail, commercial vehicles (including intercity buses), and pipelines, and related infrastructure (including roads and highways), that are within the territory of the United States, but does not include electric grids; and

(f) "surface transportation" means any conveyance of people, goods, or commodities using one or more surface transportation modes.

SEC. 3. *Functions of the Secretary of Homeland Security*. The Secretary is the principal Federal official responsible for infrastructure protection activities for surface transportation. To implement the policy set forth in section 1 of this order, the Secretary shall, consistent with the National Infrastructure Protection Plan (NIPP), in coordination with the Secretary of Transportation, and in consultation with the heads of other relevant agencies:

(a) assess the security of each surface transportation mode and evaluate the effectiveness and efficiency of current Federal Government surface transportation security initiatives;

(b) building upon current security initiatives, not later than December 31, 2006, develop a comprehensive transportation systems sector specific plan, as defined in the NIPP;

(c) not later than 90 days after the comprehensive transportation systems sector specific plan is completed, develop an annex to such plan that addresses each surface transportation mode, which shall also include, at a minimum—

(i) an identification of existing security guidelines and security requirements and any security gaps, a description of how the transportation systems sector specific plan will be implemented for such mode, and the respective roles, responsibilities, and authorities of Federal, State, local, and tribal governments and the private sector;

(ii) schedules and protocols for annual reviews of the effectiveness of surface transportation security-related information sharing mechanisms in bringing about the timely exchange of surface transportation security information among Federal, State, local, and tribal governments and the private sector, as appropriate; and

(iii) a process for assessing (A) compliance with any security guidelines and security requirements issued by the Secretary for surface transportation, and (B) the need for revision of such guidelines and requirements to ensure their continuing effectiveness;

(d) in consultation with State, local, and tribal government officials and the private sector, not later than 180 days after the date of this order, identify surface transportation modes, or components thereof, that are subject to high risk of terrorist attack, draft appropriate security guidelines or security requirements to mitigate such risks, and ensure that, prior to their issuance, draft security requirements are transmitted to the Office of Management and Budget for review in accordance with Executive Order 12866 and draft security guidelines receive appropriate interagency review;

(e) develop, implement, and lead a process, in collaboration with other agencies, State, local, and tribal governments, and the private sector, as appropriate, to coordinate research, development, testing, and evaluation of technologies (including alternative uses for commercial off-the-shelf technologies and products) relating to the protection of surface transportation, including—

(i) determining product and technology needs to inform the requirements for and prioritization of research,

development, testing, and evaluation, based on the security guidelines and security requirements developed pursuant to subsection (c) of this section and evolving terrorist threats to the security of surface transportation;

(ii) collecting information on existing and planned research, development, testing, and evaluation efforts; and

(iii) not later than 180 days after the date of this order, consistent with section 313 of the Homeland Security Act of 2002, as amended (6 U.S.C. 193), establishing and making available to Federal, State, local, and tribal government entities, and private sector owners and operators of surface transportation systems, lists of available technologies and products relating to the protection of surface transportation; and

(f) use security grants authorized by law to assist in implementing security requirements and security guidelines issued pursuant to law and consistent with subsection (c) of this section.

SEC. 4. *Duties of Heads of Other Agencies*. Heads of agencies, as appropriate, shall provide such assistance and information as the Secretary may request to implement this order.

SEC. 5. *General Provisions*. This order:

(a) shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

GEORGE W. BUSH.

§1102. National Domestic Preparedness Consortium

(a) In general

The Secretary is authorized to establish, operate, and maintain a National Domestic Preparedness Consortium within the Department.

(b) Members

Members of the National Domestic Preparedness Consortium shall consist of—

(1) the Center for Domestic Preparedness;

(2) the National Energetic Materials Research and Testing Center, New Mexico Institute of Mining and Technology;

(3) the National Center for Biomedical Research and Training, Louisiana State University;

(4) the National Emergency Response and Rescue Training Center, Texas A&M University;

(5) the National Exercise, Test, and Training Center, Nevada Test Site;

(6) the Transportation Technology Center, Incorporated, in Pueblo, Colorado; and

(7) the National Disaster Preparedness Training Center, University of Hawaii.

(c) Duties

The National Domestic Preparedness Consortium shall identify, develop, test, and deliver training to State, local, and tribal emergency response providers, provide on-site and mobile training at the performance and management and planning levels, and facilitate the delivery of training by the training partners of the Department.

(d) Authorization of appropriations

There are authorized to be appropriated to the Secretary—

(1) for the Center for Domestic Preparedness—

(A) $57,000,000 for fiscal year 2008;

(B) $60,000,000 for fiscal year 2009;

(C) $63,000,000 for fiscal year 2010; and

(D) $66,000,000 for fiscal year 2011; and

(2) for the National Energetic Materials Research and Testing Center, the National Center for Biomedical Research and Training, the National Emergency Response and Rescue Training

Center, the National Exercise, Test, and Training Center, the Transportation Technology Center, Incorporated, and the National Disaster Preparedness Training Center each—

(A) $22,000,000 for fiscal year 2008;

(B) $23,000,000 for fiscal year 2009;

(C) $24,000,000 for fiscal year 2010; and

(D) $25,500,000 for fiscal year 2011.

(e) Savings provision

From the amounts appropriated pursuant to this section, the Secretary shall ensure that future amounts provided to each of the following entities are not less than the amounts provided to each such entity for participation in the Consortium in fiscal year 2007—

(1) the Center for Domestic Preparedness;

(2) the National Energetic Materials Research and Testing Center, New Mexico Institute of Mining and Technology;

(3) the National Center for Biomedical Research and Training, Louisiana State University;

(4) the National Emergency Response and Rescue Training Center, Texas A&M University; and

(5) the National Exercise, Test, and Training Center, Nevada Test Site.

(Pub. L. 110–53, title XII, §1204, Aug. 3, 2007, 121 Stat. 386.)

§1103. National Transportation Security Center of Excellence

(a) Establishment

The Secretary shall establish a National Transportation Security Center of Excellence to conduct research and education activities, and to develop or provide professional security training, including the training of transportation employees and transportation professionals.

(b) Designation

The Secretary shall select one of the institutions identified in subsection (c) as the lead institution responsible for coordinating the National Transportation Security Center of Excellence.

(c) Member institutions

(1) Consortium

The institution of higher education selected under subsection (b) shall execute agreements with the other institutions of higher education identified in this subsection and other institutions designated by the Secretary to develop a consortium to assist in accomplishing the goals of the Center.

(2) Members

The National Transportation Security Center of Excellence shall consist of—

(A) Texas Southern University in Houston, Texas;

(B) the National Transit Institute at Rutgers, The State University of New Jersey;

(C) Tougaloo College;

(D) the Connecticut Transportation Institute at the University of Connecticut;

(E) the Homeland Security Management Institute, Long Island University;

(F) the Mack-Blackwell National Rural Transportation Study Center at the University of Arkansas; and

(G) any additional institutions or facilities designated by the Secretary.

(3) Certain inclusions

To the extent practicable, the Secretary shall ensure that an appropriate number of any additional consortium colleges or universities designated by the Secretary under this subsection are Historically Black Colleges and Universities, Hispanic Serving Institutions, and Indian Tribally Controlled Colleges and Universities.

(d) Authorization of appropriations

There are authorized to be appropriated to carry out this section—

(1) $18,000,000 for fiscal year 2008;
(2) $18,000,000 for fiscal year 2009;
(3) $18,000,000 for fiscal year 2010; and
(4) $18,000,000 for fiscal year 2011.

(Pub. L. 110–53, title XII, §1205, Aug. 3, 2007, 121 Stat. 387.)

§1104. Immunity for reports of suspected terrorist activity or suspicious behavior and response

(a) Immunity for reports of suspected terrorist activity or suspicious behavior

(1) In general

Any person who, in good faith and based on objectively reasonable suspicion, makes, or causes to be made, a voluntary report of covered activity to an authorized official shall be immune from civil liability under Federal, State, and local law for such report.

(2) False reports

Paragraph (1) shall not apply to any report that the person knew to be false or was made with reckless disregard for the truth at the time that person made that report.

(b) Immunity for response

(1) In general

Any authorized official who observes, or receives a report of, covered activity and takes reasonable action in good faith to respond to such activity shall have qualified immunity from civil liability for such action, consistent with applicable law in the relevant jurisdiction. An authorized official as defined by subsection (d)(1)(A) not entitled to assert the defense of qualified immunity shall nevertheless be immune from civil liability under Federal, State, and local law if such authorized official takes reasonable action, in good faith, to respond to the reported activity.

(2) Savings clause

Nothing in this subsection shall affect the ability of any authorized official to assert any defense, privilege, or immunity that would otherwise be available, and this subsection shall not be construed as affecting any such defense, privilege, or immunity.

(c) Attorney fees and costs

Any person or authorized official found to be immune from civil liability under this section shall be entitled to recover from the plaintiff all reasonable costs and attorney fees.

(d) Definitions

In this section:

(1) Authorized official

The term "authorized official" means—

(A) any employee or agent of a passenger transportation system or other person with responsibilities relating to the security of such systems;

(B) any officer, employee, or agent of the Department of Homeland Security, the Department of Transportation, or the Department of Justice with responsibilities relating to the security of passenger transportation systems; or

(C) any Federal, State, or local law enforcement officer.

(2) Covered activity

The term "covered activity" means any suspicious transaction, activity, or occurrence that

involves, or is directed against, a passenger transportation system or vehicle or its passengers indicating that an individual may be engaging, or preparing to engage, in a violation of law relating to—

(A) a threat to a passenger transportation system or passenger safety or security; or

(B) an act of terrorism (as that term is defined in section 3077 of title 18).

(3) Passenger transportation

The term "passenger transportation" means—

(A) public transportation, as defined in section 5302 of title 49;

(B) over-the-road bus transportation, as defined in subchapter IV, and school bus transportation;

(C) intercity passenger rail [1] transportation [2] as defined in section 24102 of title 49;

(D) the transportation of passengers onboard a passenger vessel [2] as defined in section 2101 of title 46;

(E) other regularly scheduled waterborne transportation service of passengers by vessel of at least 20 gross tons; and

(F) air transportation, as defined in section 40102 of title 49, of passengers.

(4) Passenger transportation system

The term "passenger transportation system" means an entity or entities organized to provide passenger transportation using vehicles, including the infrastructure used to provide such transportation.

(5) Vehicle

The term "vehicle" has the meaning given to that term in section 1992(16) [3] of title 18.

(e) Effective date

This section shall take effect on October 1, 2006, and shall apply to all activities and claims occurring on or after such date.

(Pub. L. 110–53, title XII, §1206, Aug. 3, 2007, 121 Stat. 388.)

EDITORIAL NOTES

REFERENCES IN TEXT

Subchapter IV, referred to in subsec. (d)(3)(B), was in the original "title XV of this Act", meaning title XV of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 422, which is classified principally to subchapter IV (§1151 et seq.) of this chapter. For complete classification of title XV to the Code, see References in Text note set out under section 1151 of this title and Tables.

[1] So in original. Probably should be "intercity rail passenger".

[2] So in original. Probably should be followed by a comma.

[3] So in original. Probably should be section "1992(d)(16)".

SUBCHAPTER II—TRANSPORTATION SECURITY ENHANCEMENTS

§1111. Definitions

For purposes of this subchapter, the following terms apply:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means the Committee on Commerce, Science, and Transportation, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) Department

The term "Department" means the Department of Homeland Security.

(3) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(4) State

The term "State" means any one of the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(5) Terrorism

The term "terrorism" has the meaning that term has in section 101 of this title.

(6) United States

The term "United States" means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(Pub. L. 110–53, title XIII, §1301, Aug. 3, 2007, 121 Stat. 389.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title XIII of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 389, which enacted this subchapter and amended section 70105 of Title 46, Shipping, and sections 114 and 46301 of Title 49, Transportation. For complete classification of title XIII to the Code, see Tables.

§1112. Authorization of Visible Intermodal Prevention and Response teams

(a) In general

The Secretary, acting through the Administrator of the Transportation Security Administration, may develop Visible Intermodal Prevention and Response (referred to in this section as "VIPR") teams to augment the security of any mode of transportation at any location within the United States. In forming a VIPR team, the Secretary—

(1) may use any asset of the Department, including Federal air marshals, surface transportation security inspectors, canine detection teams, and advanced screening technology;

(2) may determine when a VIPR team shall be deployed, as well as the duration of the deployment;

(3) shall, prior to and during the deployment, consult with local security and law enforcement officials in the jurisdiction where the VIPR team is or will be deployed, to develop and agree upon the appropriate operational protocols and provide relevant information about the mission of the VIPR team, as appropriate;

(4) shall, prior to and during the deployment, consult with all transportation entities directly affected by the deployment of a VIPR team as to specific locations and times within the facilities of such entities at which VIPR teams are to be deployed to maximize the effectiveness of such deployment, as appropriate, including railroad carriers, air carriers, airport owners, over-the-road

bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, port operators and facility owners, vessel owners and operators and pipeline operators; and

(5) shall require, as appropriate based on risk, in the case of a VIPR team deployed to an airport, that the VIPR team conduct operations—

(A) in the sterile area and any other areas to which only individuals issued security credentials have unescorted access; and

(B) in nonsterile areas.

(b) Performance measures

Not later than 1 year after October 5, 2018, the Administrator shall develop and implement a system of qualitative performance measures and objectives by which to assess the roles, activities, and effectiveness of VIPR team operations on an ongoing basis, including a mechanism through which the transportation entities referred to in subsection (a)(4) may submit feedback on VIPR team operations involving their systems or facilities.

(c) Plan

Not later than 1 year after October 5, 2018, the Administrator shall develop and implement a plan for ensuring the interoperability of communications among VIPR team participants and between VIPR teams and any transportation entities with systems or facilities that are involved in VIPR team operations. Such plan shall include an analysis of the costs and resources required to carry out such plan.

(Pub. L. 110–53, title XIII, §1303, Aug. 3, 2007, 121 Stat. 392; Pub. L. 114–190, title III, §3601, July 15, 2016, 130 Stat. 664; Pub. L. 115–254, div. K, title I, §§1930(b), 1968(b), Oct. 5, 2018, 132 Stat. 3569, 3608.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a)(4). Pub. L. 115–254, §1968(b)(1), substituted "team as to specific locations and times within the facilities of such entities at which VIPR teams are to be deployed to maximize the effectiveness of such deployment," for "team,".

Subsec. (b). Pub. L. 115–254, §1968(b)(2), added subsec. (b) and struck out former subsec. (b). Prior to amendment, text read as follows: "There are authorized to be appropriated to the Secretary to carry out this section such sums as necessary, including funds to develop not more than 60 VIPR teams, for fiscal years 2016 through 2018."

Pub. L. 115–254, §1930(b), which directed amendment of "section 1303(b) of the National Transit Systems Security Act of 2007 (6 U.S.C. 1112(b))" by substituting "such sums as necessary, including funds to develop at least 30, but not more than 60, VIPR teams, for fiscal years 2019 through 2021" for "to the extent appropriated, including funds to develop not more than 60 VIPR teams, for fiscal years 2016 through 2018", could not be executed to this section, which is section 1303(b) of the Implementing Recommendations of the 9/11 Commission Act of 2007, because the words to be substituted for did not appear.

Subsec. (c). Pub. L. 115–254, §1968(b)(2), added subsec. (c).

2016—Subsec. (a)(5). Pub. L. 114–190, §3601(1), added par. (5).

Subsec. (b). Pub. L. 114–190, §3601(2), substituted "such sums as necessary, including funds to develop not more than 60 VIPR teams, for fiscal years 2016 through 2018" for "such sums as necessary for fiscal years 2007 through 2011".

STATUTORY NOTES AND RELATED SUBSIDIARIES

VIPR TEAM STATISTICS

Pub. L. 115–254, div. K, title I, §1930(a), Oct. 5, 2018, 132 Stat. 3568, provided that:

"(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Oct. 5, 2018], and annually thereafter, the Administrator [of the Transportation Security Administration] shall notify the appropriate committees of Congress [Committees on Commerce, Science and Transportation and Homeland

Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] of the number of VIPR teams available for deployment at transportation facilities, including—

"(A) the number of VIPR team operations that include explosive detection canine teams; and

"(B) the distribution of VIPR team operations deployed across different modes of transportation.

"(2) ANNEX.—The notification under paragraph (1) may contain a classified annex.

"(3) DEFINITION OF VIPR TEAM.—In this subsection, the term 'VIPR' means a Visible Intermodal Prevention and Response team authorized under section 1303 of the National Transit Systems Security Act of 2007 [probably means section 1303 of the Implementing Recommendations of the 9/11 Commission Act of 2007] (6 U.S.C. 1112)."

[For definition of "explosive detection canine teams" as used in section 1930(a) of Pub. L. 115–254, set out above, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.]

§1113. Surface transportation security inspectors

(a) In general

The Secretary, acting through the Administrator of the Transportation Security Administration, is authorized to train, employ, and utilize surface transportation security inspectors.

(b) Mission

The Secretary shall use surface transportation security inspectors to assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security against terrorist attack and other security threats and to assist the Secretary in enforcing applicable surface transportation security regulations and directives.

(c) Authorities

Surface transportation security inspectors employed pursuant to this section shall be authorized such powers and delegated such responsibilities as the Secretary determines appropriate, subject to subsection (e).

(d) Requirements

The Secretary shall require that surface transportation security inspectors have relevant transportation experience and other security and inspection qualifications, as determined appropriate.

(e) Limitations

(1) Inspectors

Surface transportation inspectors shall be prohibited from issuing fines to public transportation agencies, as defined in subchapter III, for violations of the Department's regulations or orders except through the process described in paragraph (2).

(2) Civil penalties

The Secretary shall be prohibited from assessing civil penalties against public transportation agencies, as defined in subchapter III, for violations of the Department's regulations or orders, except in accordance with the following:

(A) In the case of a public transportation agency that is found to be in violation of a regulation or order issued by the Secretary, the Secretary shall seek correction of the violation through a written notice to the public transportation agency and shall give the public transportation agency reasonable opportunity to correct the violation or propose an alternative means of compliance acceptable to the Secretary.

(B) If the public transportation agency does not correct the violation or propose an alternative means of compliance acceptable to the Secretary within a reasonable time period that is specified in the written notice, the Secretary may take any action authorized in section 114 of title 49.

(3) Limitation on Secretary

The Secretary shall not initiate civil enforcement actions for violations of administrative and procedural requirements pertaining to the application for, and expenditure of, funds awarded under transportation security grant programs under this Act.

(f) Number of inspectors

The Secretary shall employ up to a total of—

(1) 100 surface transportation security inspectors in fiscal year 2007;
(2) 150 surface transportation security inspectors in fiscal year 2008;
(3) 175 surface transportation security inspectors in fiscal year 2009; and
(4) 200 surface transportation security inspectors in fiscal years 2010 and 2011.

(g) Coordination

The Secretary shall ensure that the mission of the surface transportation security inspectors is consistent with any relevant risk assessments required by this Act or completed by the Department, the modal plans required under section 114(t) [1] of title 49, the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities, dated September 28, 2004, and any and all subsequent annexes to this Memorandum of Understanding, and other relevant documents setting forth the Department's transportation security strategy, as appropriate.

(h) Consultation

The Secretary shall periodically consult with the surface transportation entities which are or may be inspected by the surface transportation security inspectors, including, as appropriate, railroad carriers, over-the-road bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, and pipeline operators on—

(1) the inspectors' duties, responsibilities, authorities, and mission; and
(2) strategies to improve transportation security and to ensure compliance with transportation security requirements.

(i) Report

Not later than September 30, 2008, the Department of Homeland Security Inspector General shall transmit a report to the appropriate congressional committees on the performance and effectiveness of surface transportation security inspectors, whether there is a need for additional inspectors, and other recommendations.

(j) Authorization of appropriations

There are authorized to be appropriated to the Secretary to carry out this section—

(1) $11,400,000 for fiscal year 2007;
(2) $17,100,000 for fiscal year 2008;
(3) $19,950,000 for fiscal year 2009;
(4) $22,800,000 for fiscal year 2010; and
(5) $22,800,000 for fiscal year 2011.

(Pub. L. 110–53, title XIII, §1304, Aug. 3, 2007, 121 Stat. 393.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsecs. (e)(3) and (g), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266, known as the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted this chapter and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

Section 114(t) of title 49, referred to in subsec. (g), was redesignated section 114(s) of title 49 by Pub. L. 110–161, div. E, title V, §568(a), Dec. 26, 2007, 121 Stat. 2092.

[1] *See References in Text note below.*

§1114. Surface transportation security technology information sharing

(a) In general

(1) Information sharing

The Secretary, in consultation with the Secretary of Transportation, shall establish a program to provide appropriate information that the Department has gathered or developed on the performance, use, and testing of technologies that may be used to enhance railroad, public transportation, and surface transportation security to surface transportation entities, including railroad carriers, over-the-road bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, pipeline operators, and State, local, and tribal governments that provide security assistance to such entities.

(2) Designation of qualified antiterrorism technologies

The Secretary shall include in such information provided in paragraph (1) whether the technology is designated as a qualified antiterrorism technology under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (Public Law 107–296) [6 U.S.C. 441 et seq.], as appropriate.

(b) Purpose

The purpose of the program is to assist eligible grant recipients under this Act and others, as appropriate, to purchase and use the best technology and equipment available to meet the security needs of the Nation's surface transportation system.

(c) Coordination

The Secretary shall ensure that the program established under this section makes use of and is consistent with other Department technology testing, information sharing, evaluation, and standards-setting programs, as appropriate.

(Pub. L. 110–53, title XIII, §1305, Aug. 3, 2007, 121 Stat. 394.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, referred to in subsec. (a)(2), is subtitle G (§§861–865) of title VIII of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2238, also known as the SAFETY Act, which is classified generally to part G (§441 et seq.) of subchapter VIII of chapter 1 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

This Act, referred to in subsec. (b), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266, known as the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted this chapter and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

§1115. TSA personnel limitations

Any statutory limitation on the number of employees in the Transportation Security Administration does not apply to employees carrying out this chapter.

(Pub. L. 110–53, title XIII, §1306, Aug. 3, 2007, 121 Stat. 395.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original a reference to titles XII, XIII, XIV, and XV of Pub. L.

110–53, which enacted this chapter, amended section 1992 of Title 18, Crimes and Criminal Procedure, section 70105 of Title 46, Shipping, and sections 114, 5103a, 14504, 20106, 20109, 24301, 28101, 31105, and 46301 of Title 49, Transportation, enacted provisions set out as notes under section 1101 of this title and sections 114, 13908, and 14504 of Title 49, and amended provisions set out as a note under section 14504 of Title 49. For complete classification of titles XII to XV to the Code, see Tables.

§1116. National explosives detection canine team training program

(a) Definitions

For purposes of this section, the term "explosives detection canine team" means a canine and a canine handler that are trained to detect explosives, radiological materials, chemical, nuclear or biological weapons, or other threats as defined by the Secretary.

(b) In general

(1) Increased capacity

Not later than 180 days after August 3, 2007, the Secretary of Homeland Security shall—

(A) begin to increase the number of explosives detection canine teams certified by the Transportation Security Administration for the purposes of transportation-related security by up to 200 canine teams annually by the end of 2010; and

(B) encourage State, local, and tribal governments and private owners of high-risk transportation facilities to strengthen security through the use of highly trained explosives detection canine teams.

(2) Explosives detection canine teams

The Secretary of Homeland Security shall increase the number of explosives detection canine teams by—

(A) using the Transportation Security Administration's National Explosives Detection Canine Team Training Center, including expanding and upgrading existing facilities, procuring and breeding additional canines, and increasing staffing and oversight commensurate with the increased training and deployment capabilities;

(B) partnering with other Federal, State, or local agencies, nonprofit organizations, universities, or the private sector to increase the training capacity for canine detection teams;

(C) procuring explosives detection canines trained by nonprofit organizations, universities, or the private sector provided they are trained in a manner consistent with the standards and requirements developed pursuant to subsection (c) or other criteria developed by the Secretary; or

(D) a combination of subparagraphs (A), (B), and (C), as appropriate.

(c) Standards for explosives detection canine teams

(1) In general

Based on the feasibility in meeting the ongoing demand for quality explosives detection canine teams, the Secretary shall establish criteria, including canine training curricula, performance standards, and other requirements approved by the Transportation Security Administration necessary to ensure that explosives detection canine teams trained by nonprofit organizations, universities, and private sector entities are adequately trained and maintained.

(2) Expansion

In developing and implementing such curriculum, performance standards, and other requirements, the Secretary shall—

(A) coordinate with key stakeholders, including international, Federal, State, and local officials, and private sector and academic entities to develop best practice guidelines for such a standardized program, as appropriate;

(B) require that explosives detection canine teams trained by nonprofit organizations, universities, or private sector entities that are used or made available by the Secretary be trained

consistent with specific training criteria developed by the Secretary; and

(C) review the status of the private sector programs on at least an annual basis to ensure compliance with training curricula, performance standards, and other requirements.

(d) Deployment

The Secretary shall—

(1) use the additional explosives detection canine teams as part of the Department's efforts to strengthen security across the Nation's transportation network, and may use the canine teams on a more limited basis to support other homeland security missions, as determined appropriate by the Secretary;

(2) make available explosives detection canine teams to all modes of transportation, for high-risk areas or to address specific threats, on an as-needed basis and as otherwise determined appropriate by the Secretary;

(3) encourage, but not require, any transportation facility or system to deploy TSA-certified explosives detection canine teams developed under this section; and

(4) consider specific needs and training requirements for explosives detection canine teams to be deployed across the Nation's transportation network, including in venues of multiple modes of transportation, as appropriate.

(e) Canine procurement

The Secretary, acting through the Administrator of the Transportation Security Administration, shall work to ensure that explosives detection canine teams are procured as efficiently as possible and at the best price, while maintaining the needed level of quality, including, if appropriate, through increased domestic breeding.

(f) Study

Not later than 1 year after August 3, 2007, the Comptroller General shall report to the appropriate congressional committees on the utilization of explosives detection canine teams to strengthen security and the capacity of the national explosive detection canine team program.

(g) Authorization

There are authorized to be appropriated to the Secretary such sums as may be necessary to carry out this section for fiscal years 2007 through 2011.

(h) Third party canine teams for air cargo security

(1) In general

In order to enhance the screening of air cargo and ensure that third party explosives detection canine assets are leveraged for such purpose, the Administrator shall, not later than 180 days after October 5, 2018—

(A) develop and issue standards for the use of such third party explosives detection canine assets for the primary screening of air cargo;

(B) develop a process to identify qualified non-Federal entities that will certify canine assets that meet the standards established by the Administrator under subparagraph (A);

(C) ensure that entities qualified to certify canine assets shall be independent from entities that will train and provide canines to end users of such canine assets;

(D) establish a system of Transportation Security Administration audits of the process developed under subparagraph (B); and

(E) provide that canines certified for the primary screening of air cargo can be used by air carriers, foreign air carriers, freight forwarders, and shippers.

(2) Implementation

Beginning on the date that the development of the process under paragraph (1)(B) is complete, the Administrator shall—

(A) facilitate the deployment of such assets that meet the certification standards of the Administration, as determined by the Administrator;

(B) make such standards available to vendors seeking to train and deploy third party explosives detection canine assets; and

(C) ensure that all costs for the training and certification of canines, and for the use of supplied canines, are borne by private industry and not the Federal Government.

(3) Definitions

In this subsection:

(A) Air carrier

The term "air carrier" has the meaning given the term in section 40102 of title 49.

(B) Foreign air carrier

The term "foreign air carrier" has the meaning given the term in section 40102 of title 49.

(C) Third party explosives detection canine asset

The term "third party explosives detection canine asset" means any explosives detection canine or handler not owned or employed, respectively, by the Transportation Security Administration.

(Pub. L. 110–53, title XIII, §1307, Aug. 3, 2007, 121 Stat. 395; Pub. L. 115–254, div. K, title I, §1941, Oct. 5, 2018, 132 Stat. 3582.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (h). Pub. L. 115–254 added subsec. (h).

STATUTORY NOTES AND RELATED SUBSIDIARIES

PUBLIC AREA SECURITY

Pub. L. 115–254, div. K, title I, §§1926–1929, Oct. 5, 2018, 132 Stat. 3564–3568, provided that:

"SEC. 1926. DEFINITIONS.

"In this subtitle [subtitle C (§§1926–1936) of title I of div. K of Pub. L. 115–254, amending section 1112 of this title and enacting provisions set out as notes under section 1112 of this title and sections 114 and 44903 of Title 49, Transportation]:

"(1) BEHAVIORAL STANDARDS.—The term 'behavioral standards' means standards for the evaluation of explosives detection working canines for certain factors, including canine temperament, work drive, suitability for training, environmental factors used in evaluations, and canine familiarity with natural or man-made surfaces or working conditions relevant to the canine's expected work area.

"(2) MEDICAL STANDARDS.—The term 'medical standards' means standards for the evaluation of explosives detection working canines for certain factors, including canine health, management of heredity health conditions, breeding practices, genetics, pedigree, and long-term health tracking.

"(3) TECHNICAL STANDARDS.—The term 'technical standards' means standards for the evaluation of explosives detection working canines for certain factors, including canine search techniques, handler-canine communication, detection testing conditions and logistics, and learned explosive odor libraries.

"SEC. 1927. EXPLOSIVES DETECTION CANINE CAPACITY BUILDING.

"(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration] shall establish a working group to determine ways to support decentralized, non-Federal domestic canine breeding capacity to produce high quality explosives detection canines and modernize canine training standards.

"(b) WORKING GROUP COMPOSITION.—The working group established under subsection (a) shall be comprised of representatives from the following:

"(1) The TSA [Transportation Security Administration].

"(2) The Science and Technology Directorate of the Department [of Homeland Security].

"(3) National domestic canine associations with expertise in breeding and pedigree.

"(4) Universities with expertise related to explosives detection canines and canine breeding.

"(5) Domestic canine breeders and vendors.

"(c) CHAIRPERSONS.—The Administrator shall approve of 2 individuals from among the representatives of the working group specified in subsection (b) to serve as the Chairpersons of the working group as follows:

"(1) One Chairperson shall be from an entity specified in paragraph (1) or (2) of that subsection.

"(2) One Chairperson shall be from an entity specified in paragraph (3), (4), or (5) of that subsection.

"(d) PROPOSED STANDARDS AND RECOMMENDATIONS.—Not later than 180 days after the date the working group is established under subsection (a), the working group shall submit to the Administrator—

"(1) proposed behavioral standards, medical standards, and technical standards for domestic canine breeding and canine training described in that subsection; and

"(2) recommendations on how the TSA can engage stakeholders to further the development of such domestic non-Federal canine breeding capacity and training.

"(e) STRATEGY.—Not later than 180 days after the date the recommendations are submitted under subsection (d), the Administrator shall develop and submit to the appropriate committees of Congress [Committees on Commerce, Science and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] a strategy for working with non-Federal stakeholders to facilitate expanded [sic] the domestic canine breeding capacity described in subsection (a), based on such recommendations.

"(f) CONSULTATION.—In developing the strategy under subsection (e), the Administrator shall consult with the Under Secretary for Science and Technology of the Department [of Homeland Security], the Commissioner for U.S. Customs and Border Protection, the Director of the United States Secret Service, and the heads of such other Federal departments or agencies as the Administrator considers appropriate to incorporate, to the extent practicable, mission needs across the Department for an expanded non-Federal domestic explosives detection canine breeding capacity that can be leveraged to help meet the Department's operational needs.

"(g) TERMINATION.—The working group established under subsection (a) shall terminate on the date that the strategy is submitted under subsection (e), unless the Administrator extends the termination date for the purposes of section 1928.

"(h) NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act ([former] 5 U.S.C. App.) [see 5 U.S.C. 1001 et seq.] shall not apply to the working group established under this Act [see Short Title of 2018 Amendment note set out under section 40101 of Title 49].

"SEC. 1928. THIRD PARTY DOMESTIC CANINES.

"(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act [Oct. 5, 2018], to enhance the efficiency and efficacy of transportation security by increasing the supply of canine teams for use by the TSA [Transportation Security Administration] and transportation stakeholders, the Administrator [of the Transportation Security Administration] shall develop and issue behavioral standards, medical standards, and technical standards, based on the recommendations of the working group under section 1927, that a third party explosives detection canine must satisfy to be certified for the screening of individuals and property, including detection of explosive vapors among individuals and articles of property, in public areas of an airport under section 44901 of title 49, United States Code.

"(b) AUGMENTING PUBLIC AREA SECURITY.—

"(1) IN GENERAL.—The Administrator shall develop guidance on the coordination of development and deployment of explosives detection canine teams for use by transportation stakeholders to enhance public area security at transportation hubs, including airports.

"(2) CONSULTATION.—In developing the guidance under paragraph (1), the Administrator shall consult with—

"(A) the working group established under section 1927;

"(B) the officials responsible for carrying out section 1941 [amending this section]; and

"(C) such transportation stakeholders, canine providers, law enforcement, privacy groups, and transportation security providers as the Administrator considers relevant.

"(c) AGREEMENT.—Subject to subsections (d), (e), and (f), not later than 270 days after the issuance of standards under subsection (a), the Administrator shall, to the extent possible, enter into an agreement with at least 1 third party to test and certify the capabilities of canines in accordance with the standards under subsection (a).

"(d) EXPEDITED DEPLOYMENT.—In entering into an agreement under subsection (c), the Administrator shall use—

"(1) the other transaction authority under section 114(m) of title 49, United States Code; or

"(2) such other authority of the Administrator as the Administrator considers appropriate to expedite

the deployment of additional canine teams.

"(e) PROCESS.—Before entering into an agreement under subsection (c), the Administrator shall—

"(1) evaluate and verify the third party's ability to effectively evaluate the capabilities of canines;

"(2) designate key elements required for appropriate evaluation venues where third parties may conduct testing; and

"(3) periodically assess the program at evaluation centers to ensure the proficiency of the canines beyond the initial testing and certification by the third party.

"(f) CONSULTATION.—To determine best practices for the use of third parties to test and certify the capabilities of canines, the Administrator shall consult with the following persons before entering into an agreement under subsection (c):

"(1) The Secretary of State.

"(2) The Secretary of Defense.

"(3) Non-profit organizations that train, certify, and provide the services of canines for various purposes.

"(4) Institutions of higher education with research programs related to use of canines for the screening of individuals and property, including detection of explosive vapors among individuals and articles of property.

"(g) THIRD PARTY EXPLOSIVES DETECTION CANINE PROVIDER LIST.—

"(1) IN GENERAL.—Not later than 90 days after the date the Administrator enters into an agreement under subsection (c), the Administrator shall develop and maintain a list of the names of each third party from which the TSA procures explosive detection canines, including for each such third party the relevant contractual period of performance.

"(2) DISTRIBUTION.—The Administrator shall make the list under paragraph (1) available to appropriate transportation stakeholders in such form and manner as the Administrator prescribes.

"(h) OVERSIGHT.—The Administrator shall establish a process to ensure appropriate oversight of the certification program and compliance with the standards under subsection (a), including periodic audits of participating third parties.

"(i) AUTHORIZATION.—

"(1) TSA.—The Administrator shall develop and implement a process for the TSA to procure third party explosives detection canines certified under this section.

"(2) AVIATION STAKEHOLDERS.—

"(A) IN GENERAL.—The Administrator shall authorize an aviation stakeholder, under the oversight of and in coordination with the Federal Security Director at an applicable airport, to contract with, procure or purchase, and deploy one or more third party explosives detection canines certified under this section to augment public area security at that airport.

"(B) APPLICABLE LARGE HUB AIRPORTS.—

"(i) IN GENERAL.—Except as provided under subparagraph [clause] (ii), notwithstanding any law to the contrary, and subject to the other provisions of this paragraph, an applicable large hub airport may provide a certified canine described in subparagraph (A) on an in-kind basis to the TSA to be deployed as a passenger screening canine at that airport unless the applicable large hub airport consents to the use of that certified canine elsewhere.

"(ii) EXCEPTION.—The Administrator may, on a case-by-case basis, deploy a certified canine described in subparagraph (A) to a transportation facility other than the applicable large hub airport described in clause (i) for not more than 90 days per year if the Administrator—

"(I) determines that such deployment is necessary to meet operational or security needs; and

"(II) notifies the applicable large hub airport described in clause (i).

"(iii) NONDEPLOYABLE CANINES.—Any certified canine provided to the TSA under clause (i) that does not complete training for deployment under that clause shall be the responsibility of the large hub airport unless the TSA agrees to a different outcome.

"(C) HANDLERS.—Not later than 30 days before a canine begins training to become a certified canine under subparagraph (B), the airport shall notify the TSA of such training and the Administrator shall assign a TSA canine handler to participate in the training with that canine, as appropriate.

"(D) LIMITATION.—The Administrator may not reduce the staffing allocation model for an applicable large hub airport based on that airport's provision of a certified canine under this paragraph.

"(j) DEFINITIONS.—In this section:

"(1) APPLICABLE LARGE HUB AIRPORT.—The term 'applicable large hub airport' means a large hub airport (as defined in section 40102 of title 49, United States Code) that has less than 100 percent of the allocated passenger screening canine teams staffed by the TSA.

"(2) AVIATION STAKEHOLDER.—The term 'aviation stakeholder' includes an airport, airport operator, and air carrier.

"SEC. 1929. TRACKING AND MONITORING OF CANINE TRAINING AND TESTING.

"Not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration] shall use, to the extent practicable, a digital monitoring system for all training, testing, and validation or certification of public and private canine assets utilized or funded by the TSA [Transportation Security Administration] to facilitate improved review, data analysis, and record keeping of canine testing performance and program administration."

EXPANSION OF NATIONAL EXPLOSIVES DETECTION CANINE TEAM PROGRAM

Pub. L. 115–254, div. K, title I, §1971, Oct. 5, 2018, 132 Stat. 3613, provided that:

"(a) IN GENERAL.—The Secretary [of Homeland Security], where appropriate, shall encourage State, local, and tribal governments and private owners of high-risk transportation facilities to strengthen security through the use of explosives detection canine teams.

"(b) INCREASED CAPACITY.—

"(1) IN GENERAL.—Before the date the Inspector General of the Department [of Homeland Security] submits the report under section 1970 [132 Stat. 3612], the Administrator [of the Transportation Security Administration] may increase the number of State and local surface and maritime transportation canines by not more than 70 explosives detection canine teams.

"(2) ADDITIONAL TEAMS.—Beginning on the date the Inspector General of the Department submits the report under section 1970, the Secretary may increase the State and local surface and maritime transportation canines up to 200 explosives detection canine teams unless more are identified in the risk-based surface transportation security strategy under section 1964 [enacting provisions set out as a note under section 114 of Title 49, Transportation], consistent with section 1965 [enacting provisions set out as a note under section 114 of Title 49] or with the President's most recent budget submitted under section 1105 of title 31, United States Code.

"(3) RECOMMENDATIONS.—Before initiating any increase in the number of explosives detection teams under paragraph (2), the Secretary shall consider any recommendations in the report under section 1970 on the efficacy and management of the explosives detection canine program.

"(c) DEPLOYMENT.—The Secretary shall—

"(1) use the additional explosives detection canine teams, as described in subsection (b)(1), as part of the Department's efforts to strengthen security across the Nation's surface and maritime transportation networks;

"(2) make available explosives detection canine teams to all modes of transportation, subject to the requirements under section 1968 [amending section 1112 of this title and enacting provisions set out as a note under section 114 of Title 49], to address specific vulnerabilities or risks, on an as-needed basis and as otherwise determined appropriate by the Secretary; and

"(3) consider specific needs and training requirements for explosives detection canine teams to be deployed across the Nation's surface and maritime transportation networks, including in venues of multiple modes of transportation, as the Secretary considers appropriate.

"(d) AUTHORIZATION.—There are authorized to be appropriated to the Secretary to the extent of appropriations to carry out this section for each of fiscal years 2019 through 2021."

[For definition of "explosives detection canine teams" as used in section 1971 of Pub. L. 115–254, set out above, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.]

§1117. Roles of the Department of Homeland Security and the Department of Transportation

The Secretary of Homeland Security is the principal Federal official responsible for transportation security. The roles and responsibilities of the Department of Homeland Security and the Department of Transportation in carrying out this chapter are the roles and responsibilities of such Departments pursuant to the Aviation and Transportation Security Act (Public Law 107–71); the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458); the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7; The [1] Homeland Security Act of 2002 [6 U.S.C. 101 et seq.]; The [1] National Response Plan; Executive Order No. 13416:

Strengthening Surface Transportation Security, dated December 5, 2006; the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities, dated September 28, 2004, and any and all subsequent annexes to this Memorandum of Understanding; and any other relevant agreements between the two Departments.

(Pub. L. 110–53, title XIII, §1310, Aug. 3, 2007, 121 Stat. 400.)

EDITORIAL NOTES

REFERENCES IN TEXT

This chapter, referred to in text, was in the original a reference to titles XII, XIII, XIV, and XV of Pub. L. 110–53, which enacted this chapter, amended section 1992 of Title 18, Crimes and Criminal Procedure, section 70105 of Title 46, Shipping, and sections 114, 5103a, 14504, 20106, 20109, 24301, 28101, 31105, and 46301 of Title 49, Transportation, enacted provisions set out as notes under section 1101 of this title and sections 114, 13908, and 14504 of Title 49, and amended provisions set out as a note under section 14504 of Title 49. For complete classification of titles XII to XV to the Code, see Tables.

The Aviation and Transportation Security Act, referred to in text, is Pub. L. 107–71, Nov. 19, 2001, 115 Stat. 597. For complete classification of this Act to the Code, see Short Title of 2001 Amendment note set out under section 40101 of Title 49, Transportation, and Tables.

The Intelligence Reform and Terrorism Prevention Act of 2004, referred to in text, is Pub. L. 108–458, Dec. 17, 2004, 118 Stat. 3638. For complete classification of this Act to the Code, see Tables.

The Homeland Security Act of 2002, referred to in text, is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, which is classified principally to chapter 1 (§101 et seq.) of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

Executive Order No. 13416, referred to in text, is set out as a note under section 1101 of this title.

[1] So in original. Probably should not be capitalized.

§1118. Biometrics expansion

(a) In general

The Administrator and the Commissioner of U.S. Customs and Border Protection shall consult with each other on the deployment of biometric technologies.

(b) Rule of construction

Nothing in this section shall be construed to permit the Commissioner of U.S. Customs and Border Protection to facilitate or expand the deployment of biometric technologies, or otherwise collect, use, or retain biometrics, not authorized by any provision of or amendment made by the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638) or the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 121 Stat. 266).

(c) Report required

Not later than 270 days after October 5, 2018, the Secretary shall submit to the appropriate committees of Congress, and to any Member of Congress upon the request of that Member, a report that includes specific assessments from the Administrator and the Commissioner of U.S. Customs and Border Protection with respect to the following:

(1) The operational and security impact of using biometric technology to identify travelers.

(2) The potential effects on privacy of the expansion of the use of biometric technology under paragraph (1), including methods proposed or implemented to mitigate any risks to privacy identified by the Administrator or the Commissioner related to the active or passive collection of biometric data.

(3) Methods to analyze and address any matching performance errors related to race, gender, or age identified by the Administrator with respect to the use of biometric technology, including the

deployment of facial recognition technology; [1]

(4) With respect to the biometric entry-exit program, the following:

(A) Assessments of—

(i) the error rates, including the rates of false positives and false negatives, and accuracy of biometric technologies;

(ii) the effects of biometric technologies, to ensure that such technologies do not unduly burden categories of travelers, such as a certain race, gender, or nationality;

(iii) the extent to which and how biometric technologies could address instances of travelers to the United States overstaying their visas, including—

(I) an estimate of how often biometric matches are contained in an existing database;

(II) an estimate of the rate at which travelers using fraudulent credentials identifications are accurately rejected; and

(III) an assessment of what percentage of the detection of fraudulent identifications could have been accomplished using conventional methods;

(iv) the effects on privacy of the use of biometric technologies, including methods to mitigate any risks to privacy identified by the Administrator or the Commissioner of U.S. Customs and Border Protection related to the active or passive collection of biometric data; and

(v) the number of individuals who stay in the United States after the expiration of their visas each year.

(B) A description of—

(i) all audits performed to assess—

(I) error rates in the use of biometric technologies; or

(II) whether the use of biometric technologies and error rates in the use of such technologies disproportionately affect a certain race, gender, or nationality; and

(ii) the results of the audits described in clause (i).

(C) A description of the process by which domestic travelers are able to opt-out of scanning using biometric technologies.

(D) A description of—

(i) what traveler data is collected through scanning using biometric technologies, what agencies have access to such data, and how long the agencies possess such data;

(ii) specific actions that the Department and other relevant Federal departments and agencies take to safeguard such data; and

(iii) a short-term goal for the prompt deletion of the data of individual United States citizens after such data is used to verify traveler identities.

(d) Publication of assessments

The Secretary, the Administrator, and the Commissioner shall, if practicable, publish a public version of the assessment required by subsection (c)(2) on the Internet website of the TSA and of the U.S. Customs and Border Protection.

(Pub. L. 115–254, div. K, title I, §1919, Oct. 5, 2018, 132 Stat. 3559.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Intelligence Reform and Terrorism Prevention Act of 2004, referred to in subsec. (b), is Pub. L. 108–458, Dec. 17, 2004, 118 Stat. 3638. For complete classification of this Act to the Code, see Tables.

The Implementing Recommendations of the 9/11 Commission Act of 2007, referred to in subsec. (b), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was enacted as part of the TSA Modernization Act and also as part of the FAA Reauthorization Act of 2018, and not as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of "Administrator", "appropriate committees of Congress", "Department", "Secretary", and "TSA" as used in this section, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.

[1] *So in original. The semicolon probably should be a period.*

§1119. Voluntary use of credentialing

(a) In general

An applicable individual who is subject to credentialing or a background investigation may satisfy that requirement by obtaining a valid transportation security card.

(b) Issuance of cards

The Secretary of Homeland Security—

(1) shall expand the transportation security card program, consistent with section 70105 of title 46, to allow an applicable individual who is subject to credentialing or a background investigation to apply for a transportation security card; and

(2) may charge reasonable fees, in accordance with section 469(a) of this title, for providing the necessary credentialing and background investigation.

(c) Vetting

The Administrator shall develop and implement a plan to utilize, in addition to any background check required for initial issue, the Federal Bureau of Investigation's Rap Back Service and other vetting tools as appropriate, including the No-Fly and Selectee lists, to get immediate notification of any criminal activity relating to any person with a valid transportation security card.

(d) Definitions

In this section:

(1) Applicable individual who is subject to credentialing or a background investigation

The term "applicable individual who is subject to credentialing or a background investigation" means only an individual who—

(A) because of employment is regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard and is required to have a background records check to obtain a hazardous materials endorsement on a commercial driver's license issued by a State under section 5103a of title 49; or

(B) is required to have a credential and background records check under section 622(d)(2) [1] of this title at a facility with activities that are regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard.

(2) Valid transportation security card

The term "valid transportation security card" means a transportation security card that is—

(A) issued under section 70105 of title 46;

(B) not expired;

(C) shows [2] no signs of tampering; and

(D) bears [2] a photograph of the individual representing such card.

(Pub. L. 115–254, div. K, title I, §1977, Oct. 5, 2018, 132 Stat. 3617.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 622 of this title, referred to in subsec. (d)(1)(B), was omitted from the Code.

CODIFICATION

Section was enacted as part of the TSA Modernization Act and also as part of the FAA Reauthorization Act of 2018, and not as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITION

For definition of "Administrator" as used in this section, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.

[1] *See References in Text note below.*

[2] *So in original.*

SUBCHAPTER III—PUBLIC TRANSPORTATION SECURITY

§1131. Definitions

For purposes of this subchapter, the following terms apply:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means the Committee on Banking, Housing, and Urban Affairs, and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) Department

The term "Department" means the Department of Homeland Security.

(3) Disadvantaged businesses concerns

The term "disadvantaged business concerns" means small businesses that are owned and controlled by socially and economically disadvantaged individuals as defined in section [1] 124, title 13, Code of Federal Regulations.

(4) Frontline employee

The term "frontline employee" means an employee of a public transportation agency who is a transit vehicle driver or operator, dispatcher, maintenance and maintenance support employee, station attendant, customer service employee, security employee, or transit police, or any other employee who has direct contact with riders on a regular basis, and any other employee of a public transportation agency that the Secretary determines should receive security training under section 1137 of this title.

(5) Public transportation agency

The term "public transportation agency" means a publicly owned operator of public transportation eligible to receive Federal assistance under chapter 53 of title 49.

(6) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(Pub. L. 110–53, title XIV, §1402, Aug. 3, 2007, 121 Stat. 400.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

For short title of this subchapter as the "National Transit Systems Security Act of 2007", see section 1401 of Pub. L. 110–53, set out as a note under section 1101 of this title.

[1] *So in original. Probably should be "part".*

§1132. Findings

Congress finds that—

(1) 182 public transportation systems throughout the world have been primary targets of terrorist attacks;

(2) more than 6,000 public transportation agencies operate in the United States;

(3) people use public transportation vehicles 33,000,000 times each day;

(4) the Federal Transit Administration has invested $93,800,000,000 since 1992 for construction and improvements;

(5) the Federal investment in transit security has been insufficient; and

(6) greater Federal investment in transit security improvements per passenger boarding is necessary to better protect the American people, given transit's vital importance in creating mobility and promoting our Nation's economy.

(Pub. L. 110–53, title XIV, §1403, Aug. 3, 2007, 121 Stat. 401.)

§1133. National Strategy for Public Transportation Security

(a) National Strategy

Not later than 9 months after August 3, 2007, and based upon the previous and ongoing security assessments conducted by the Department and the Department of Transportation, the Secretary, consistent with and as required by section 114(t) [1] of title 49, shall develop and implement the modal plan for public transportation, entitled the "National Strategy for Public Transportation Security".

(b) Purpose

(1) Guidelines

In developing the National Strategy for Public Transportation Security, the Secretary shall establish guidelines for public transportation security that—

(A) minimize security threats to public transportation systems; and

(B) maximize the abilities of public transportation systems to mitigate damage resulting from terrorist attack or other major incident.

(2) Assessments and consultations

In developing the National Strategy for Public Transportation Security, the Secretary shall—

(A) use established and ongoing public transportation security assessments as the basis of the National Strategy for Public Transportation Security; and

(B) consult with all relevant stakeholders, including public transportation agencies, nonprofit labor organizations representing public transportation employees, emergency responders, public safety officials, and other relevant parties.

(c) Contents

In the National Strategy for Public Transportation Security, the Secretary shall describe prioritized goals, objectives, policies, actions, and schedules to improve the security of public transportation.

(d) Responsibilities

The Secretary shall include in the National Strategy for Public Transportation Security a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, tribal governments, and appropriate stakeholders. The plan shall also include—

(1) the identification of, and a plan to address, gaps and unnecessary overlaps in the roles, responsibilities, and authorities of Federal agencies; and

(2) a process for coordinating existing or future security strategies and plans for public transportation, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7; Executive Order No. 13416: Strengthening Surface Transportation Security dated December 5, 2006; the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities dated September 28, 2004; and subsequent annexes and agreements.

(e) Adequacy of existing plans and strategies

In developing the National Strategy for Public Transportation Security, the Secretary shall use relevant existing risk assessments and strategies developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) [1] of title 49 or Homeland Security Presidential Directive–7.

(f) Funding

There is authorized to be appropriated to the Secretary to carry out this section $2,000,000 for fiscal year 2008.

(Pub. L. 110–53, title XIV, §1404, Aug. 3, 2007, 121 Stat. 401.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(t) of title 49, referred to in subsecs. (a) and (e), was redesignated section 114(s) of title 49 by Pub. L. 110–161, div. E, title V, §568(a), Dec. 26, 2007, 121 Stat. 2092.

Executive Order No. 13416, referred to in subsec. (d)(2), is set out as a note under section 1101 of this title.

[1] *See References in Text note below.*

§1134. Security assessments and plans

(a) Public transportation security assessments

(1) Submission

Not later than 30 days after August 3, 2007, the Administrator of the Federal Transit Administration of the Department of Transportation shall submit all public transportation security assessments and all other relevant information to the Secretary.

(2) Secretarial review

Not later than 60 days after receiving the submission under paragraph (1), the Secretary shall review and augment the security assessments received, and conduct additional security assessments as necessary to ensure that at a minimum, all high risk public transportation agencies, as determined by the Secretary, will have a completed security assessment.

(3) Content

The Secretary shall ensure that each completed security assessment includes—

(A) identification of critical assets, infrastructure, and systems and their vulnerabilities; and

(B) identification of any other security weaknesses, including weaknesses in emergency response planning and employee training.

(b) Bus and rural public transportation systems

Not later than 180 days after August 3, 2007, the Secretary shall—

(1) conduct security assessments, based on a representative sample, to determine the specific needs of—

(A) local bus-only public transportation systems; and

(B) public transportation systems that receive funds under section 5311 of title 49; and

(2) make the representative assessments available for use by similarly situated systems.

(c) Security plans

(1) Requirement for plan

(A) High risk agencies

The Secretary shall require public transportation agencies determined by the Secretary to be at high risk for terrorism to develop a comprehensive security plan. The Secretary shall provide technical assistance and guidance to public transportation agencies in preparing and implementing security plans under this section.

(B) Other agencies

Provided that no public transportation agency that has not been designated high risk shall be required to develop a security plan, the Secretary may also establish a security program for public transportation agencies not designated high risk by the Secretary, to assist those public transportation agencies which request assistance, including—

(i) guidance to assist such agencies in conducting security assessments and preparing and implementing security plans; and

(ii) a process for the Secretary to review and approve such assessments and plans, as appropriate.

(2) Contents of plan

The Secretary shall ensure that security plans include, as appropriate—

(A) a prioritized list of all items included in the public transportation agency's security assessment that have not yet been addressed;

(B) a detailed list of any additional capital and operational improvements identified by the Department or the public transportation agency and a certification of the public transportation agency's technical capacity for operating and maintaining any security equipment that may be identified in such list;

(C) specific procedures to be implemented or used by the public transportation agency in response to a terrorist attack, including evacuation and passenger communication plans and appropriate evacuation and communication measures for the elderly and individuals with disabilities;

(D) a coordinated response plan that establishes procedures for appropriate interaction with State and local law enforcement agencies, emergency responders, and Federal officials in order to coordinate security measures and plans for response in the event of a terrorist attack or other major incident;

(E) a strategy and timeline for conducting training under section 1137 of this title;

(F) plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident;

(G) plans for providing service capabilities throughout the system in the event of a terrorist attack or other major incident in the city or region which the public transportation system serves;

(H) methods to mitigate damage within a public transportation system in case of an attack on the system, including a plan for communication and coordination with emergency responders; and

(I) other actions or procedures as the Secretary determines are appropriate to address the security of the public transportation system.

(3) Review

Not later than 6 months after receiving the plans required under this section, the Secretary shall—

(A) review each security plan submitted;

(B) require the public transportation agency to make any amendments needed to ensure that the plan meets the requirements of this section; and

(C) approve any security plan that meets the requirements of this section.

(4) Exemption

The Secretary shall not require a public transportation agency to develop a security plan under paragraph (1) if the agency does not receive a grant under section 1135 of this title.

(5) Waiver

The Secretary may waive the exemption provided in paragraph (4) to require a public transportation agency to develop a security plan under paragraph (1) in the absence of grant funds under section 1135 of this title if not less than 3 days after making the determination the Secretary provides the appropriate congressional committees and the public transportation agency written notification detailing the need for the security plan, the reasons grant funding has not been made available, and the reason the agency has been designated high risk.

(d) Consistency with other plans

The Secretary shall ensure that the security plans developed by public transportation agencies under this section are consistent with the security assessments developed by the Department and the National Strategy for Public Transportation Security developed under section 1133 of this title.

(e) Updates

Not later than September 30, 2008, and annually thereafter, the Secretary shall—

(1) update the security assessments referred to in subsection (a);

(2) update the security improvement priorities required under subsection (f); and

(3) require public transportation agencies to update the security plans required under subsection (c) as appropriate.

(f) Security improvement priorities

(1) In general

Beginning in fiscal year 2008 and each fiscal year thereafter, the Secretary, after consultation with management and nonprofit employee labor organizations representing public transportation employees as appropriate, and with appropriate State and local officials, shall utilize the information developed or received in this section to establish security improvement priorities unique to each individual public transportation agency that has been assessed.

(2) Allocations

The Secretary shall use the security improvement priorities established in paragraph (1) as the basis for allocating risk-based grant funds under section 1135 of this title, unless the Secretary notifies the appropriate congressional committees that the Secretary has determined an adjustment is necessary to respond to an urgent threat or other significant national security factors.

(g) Shared facilities

The Secretary shall encourage the development and implementation of coordinated assessments and security plans to the extent a public transportation agency shares facilities (such as tunnels, bridges, stations, or platforms) with another public transportation agency, a freight or passenger

railroad carrier, or over-the-road bus operator that are geographically close or otherwise co-located.

(h) Nondisclosure of information

(1) Submission of information to Congress

Nothing in this section shall be construed as authorizing the withholding of any information from Congress.

(2) Disclosure of independently furnished information

Nothing in this section shall be construed as affecting any authority or obligation of a Federal agency to disclose any record or information that the Federal agency obtains from a public transportation agency under any other Federal law.

(i) Determination

In response to a petition by a public transportation agency or at the discretion of the Secretary, the Secretary may recognize existing procedures, protocols, and standards of a public transportation agency that the Secretary determines meet all or part of the requirements of this section regarding security assessments or security plans.

(Pub. L. 110–53, title XIV, §1405, Aug. 3, 2007, 121 Stat. 402.)

§1135. Public transportation security assistance

(a) Security assistance program

(1) In general

The Secretary shall establish a program for making grants to eligible public transportation agencies for security improvements described in subsection (b).

(2) Eligibility

A public transportation agency is eligible for a grant under this section if the Secretary has performed a security assessment or the agency has developed a security plan under section 1134 of this title. Grant funds shall only be awarded for permissible uses under subsection (b) to—

(A) address items included in a security assessment; or

(B) further a security plan.

(b) Uses of funds

A recipient of a grant under subsection (a) shall use the grant funds for one or more of the following:

(1) Capital uses of funds, including—

(A) tunnel protection systems;

(B) perimeter protection systems, including access control, installation of improved lighting, fencing, and barricades;

(C) redundant critical operations control systems;

(D) chemical, biological, radiological, or explosive detection systems, including the acquisition of canines used for such detection;

(E) surveillance equipment;

(F) communications equipment, including mobile service equipment to provide access to wireless Enhanced 911 (E911) emergency services in an underground fixed guideway system;

(G) emergency response equipment, including personal protective equipment;

(H) fire suppression and decontamination equipment;

(I) global positioning or tracking and recovery equipment, and other automated-vehicle-locator-type system equipment;

(J) evacuation improvements;

(K) purchase and placement of bomb-resistant trash cans throughout public transportation facilities, including subway exits, entrances, and tunnels;

(L) capital costs associated with security awareness, security preparedness, and security response training, including training under section 1137 of this title and exercises under section 1136 of this title;

(M) security improvements for public transportation systems, including extensions thereto, in final design or under construction;

(N) security improvements for stations and other public transportation infrastructure, including stations and other public transportation infrastructure owned by State or local governments; and

(O) other capital security improvements determined appropriate by the Secretary.

(2) Operating uses of funds, including—

(A) security training and associated backfill, including training under section 1137 of this title and training developed by institutions of higher education and by nonprofit employee labor organizations, for public transportation employees, including frontline employees;

(B) live or simulated exercises under section 1136 of this title;

(C) public awareness campaigns for enhanced public transportation security;

(D) canine patrols for chemical, radiological, biological, or explosives detection;

(E) development of security plans under section 1134 of this title;

(F) overtime reimbursement including reimbursement of State, local, and tribal governments, for costs for enhanced security personnel during significant national and international public events;

(G) operational costs, including reimbursement of State, local, and tribal governments for costs for personnel assigned to full-time or part-time security or counterterrorism duties related to public transportation, provided that this expense totals no more than 10 percent of the total grant funds received by a public transportation agency in any 1 year; and

(H) other operational security costs determined appropriate by the Secretary, excluding routine, ongoing personnel costs, other than those set forth in this section.

(c) Department of Homeland Security responsibilities

In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants under this section, including application requirements;

(2) pursuant to subsection (a)(2), select the recipients of grants based solely on risk; and

(3) pursuant to subsection (b), establish the priorities for which grant funds may be used under this section.

(d) Distribution of grants

Not later than 90 days after August 3, 2007, the Secretary and the Secretary of Transportation shall determine the most effective and efficient way to distribute grant funds to the recipients of grants determined by the Secretary under subsection (a). Subject to the determination made by the Secretaries, the Secretary may transfer funds to the Secretary of Transportation for the purposes of disbursing funds to the grant recipient.

(e) Subject to certain terms and conditions

Except as otherwise specifically provided in this section, a grant provided under this section shall be subject to the terms and conditions applicable to a grant made under section 5307 of title 49, as in effect on January 1, 2007, and such other terms and conditions as are determined necessary by the Secretary.

(f) Limitation on uses of funds

Grants made under this section may not be used to make any State or local government cost-sharing contribution under any other Federal law.

(g) Annual reports

Each recipient of a grant under this section shall report annually to the Secretary on the use of the

grant funds.

(h) Guidelines

Before distribution of funds to recipients of grants, the Secretary shall issue guidelines to ensure that, to the extent that recipients of grants under this section use contractors or subcontractors, such recipients shall use small, minority, women-owned, or disadvantaged business concerns as contractors or subcontractors to the extent practicable.

(i) Coordination with State homeland security plans

In establishing security improvement priorities under section 1134 of this title and in awarding grants for capital security improvements and operational security improvements under subsection (b), the Secretary shall act consistently with relevant State homeland security plans.

(j) Multistate transportation systems

In cases in which a public transportation system operates in more than one State, the Secretary shall give appropriate consideration to the risks of the entire system, including those portions of the States into which the system crosses, in establishing security improvement priorities under section 1134 of this title and in awarding grants for capital security improvements and operational security improvements under subsection (b).

(k) Congressional notification

Not later than 3 days before the award of any grant under this section, the Secretary shall notify simultaneously, the appropriate congressional committees of the intent to award such grant.

(l) Return of misspent grant funds

The Secretary shall establish a process to require the return of any misspent grant funds received under this section determined to have been spent for a purpose other than those specified in the grant award.

(m) Periods of performance

(1) In general

Except as provided in paragraph (2), funds provided pursuant to a grant awarded under this section for a use specified in subsection (b) shall remain available for use by a grant recipient for a period of not fewer than 36 months.

(2) Exception

Funds provided pursuant to a grant awarded under this section for a use specified in subparagraph (M) or (N) of subsection (b)(1) shall remain available for use by a grant recipient for a period of not fewer than 48 months.

(n) Authorization of appropriations

(1) There are authorized to be appropriated to the Secretary to make grants under this section—

(A) such sums as are necessary for fiscal year 2007;

(B) $650,000,000 for fiscal year 2008, except that not more than 50 percent of such funds may be used for operational costs under subsection (b)(2);

(C) $750,000,000 for fiscal year 2009, except that not more than 30 percent of such funds may be used for operational costs under subsection (b)(2);

(D) $900,000,000 for fiscal year 2010, except that not more than 20 percent of such funds may be used for operational costs under subsection (b)(2); and

(E) $1,100,000,000 for fiscal year 2011, except that not more than 10 percent of such funds may be used for operational costs under subsection (b)(2).

(2) PERIOD OF AVAILABILITY.—Sums appropriated to carry out this section shall remain available until expended.

(3) WAIVER.—The Secretary may waive the limitation on operational costs specified in subparagraphs (B) through (E) of paragraph (1) if the Secretary determines that such a waiver is

required in the interest of national security, and if the Secretary provides a written justification to the appropriate congressional committees prior to any such action.

(4) EFFECTIVE DATE.—Funds provided for fiscal year 2007 transit security grants under Public Law 110–28 shall be allocated based on security assessments that are in existence as of August 3, 2007.

(Pub. L. 110–53, title XIV, §1406, Aug. 3, 2007, 121 Stat. 405; Pub. L. 117–81, div. F, title LXIV, §§6420, 6421, Dec. 27, 2021, 135 Stat. 2418.)

EDITORIAL NOTES

REFERENCES IN TEXT

Public Law 110–28, referred to in subsec. (n)(4), is Pub. L. 110–28, May 25, 2007, 121 Stat. 112, known as the U.S. Troop Readinesss, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2021—Subsec. (b)(2)(A). Pub. L. 117–81, §6420, inserted "and associated backfill" after "security training".

Subsecs. (m), (n). Pub. L. 117–81, §6421, added subsec. (m) and redesignated former subsec. (m) as (n).

§1136. Security exercises

(a) In general

The Secretary shall establish a program for conducting security exercises for public transportation agencies for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism.

(b) Covered entities

Entities to be assessed under the program shall include—

(1) Federal, State, and local agencies and tribal governments;

(2) public transportation agencies;

(3) governmental and nongovernmental emergency response providers and law enforcement personnel, including transit police; and

(4) any other organization or entity that the Secretary determines appropriate.

(c) Requirements

The Secretary shall ensure that the program—

(1) requires, for public transportation agencies which the Secretary deems appropriate, exercises to be conducted that are—

(A) scaled and tailored to the needs of specific public transportation systems, and include taking into account the needs of the elderly and individuals with disabilities;

(B) live;

(C) coordinated with appropriate officials;

(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(E) inclusive, as appropriate, of frontline employees and managers; and

(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(2) provides that exercises described in paragraph (1) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to learn best practices, which shall be shared with appropriate Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, law enforcement personnel, including railroad and transit police, and appropriate stakeholders; and

(C) followed by remedial action by covered entities in response to lessons learned;

(3) involves individuals in neighborhoods around the infrastructure of a public transportation system; and

(4) assists State, local, and tribal governments and public transportation agencies in designing, implementing, and evaluating exercises that conform to the requirements of paragraph (2).

(d) National Exercise Program

The Secretary shall ensure that the exercise program developed under subsection (a) is a component of the National Exercise Program established under section 748 of this title.

(e) Ferry system exemption

This section does not apply to any ferry system for which drills are required to be conducted pursuant to section 70103 of title 46.

(Pub. L. 110–53, title XIV, §1407, Aug. 3, 2007, 121 Stat. 408.)

§1137. Public transportation security training program

(a) In general

Not later than 90 days after August 3, 2007, the Secretary shall develop and issue detailed interim final regulations, and not later than 1 year after August 3, 2007, the Secretary shall develop and issue detailed final regulations, for a public transportation security training program to prepare public transportation employees, including frontline employees, for potential security threats and conditions.

(b) Consultation

The Secretary shall develop the interim final and final regulations under subsection (a) in consultation with—

(1) appropriate law enforcement, fire service, security, and terrorism experts;

(2) representatives of public transportation agencies; and

(3) nonprofit employee labor organizations representing public transportation employees or emergency response personnel.

(c) Program elements

The interim final and final regulations developed under subsection (a) shall require security training programs to include, at a minimum, elements to address the following:

(1) Determination of the seriousness of any occurrence or threat.

(2) Crew and passenger communication and coordination.

(3) Appropriate responses to defend oneself, including using nonlethal defense devices.

(4) Use of personal protective devices and other protective equipment.

(5) Evacuation procedures for passengers and employees, including individuals with disabilities and the elderly.

(6) Training related to behavioral and psychological understanding of, and responses to, terrorist incidents, including the ability to cope with hijacker behavior, and passenger responses.

(7) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(8) Recognition and reporting of dangerous substances and suspicious packages, persons, and situations.

(9) Understanding security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers and for on scene interaction

with such emergency response providers.

(10) Operation and maintenance of security equipment and systems.

(11) Other security training activities that the Secretary deems appropriate.

(d) Required programs

(1) Development and submission to Secretary

Not later than 90 days after a public transportation agency meets the requirements under subsection (e), each such public transportation agency shall develop a security training program in accordance with the regulations developed under subsection (a) and submit the program to the Secretary for approval.

(2) Approval

Not later than 60 days after receiving a security training program proposal under this subsection, the Secretary shall approve the program or require the public transportation agency that developed the program to make any revisions to the program that the Secretary determines necessary for the program to meet the requirements of the regulations. A public transportation agency shall respond to the Secretary's comments within 30 days after receiving them.

(3) Training

Not later than 1 year after the Secretary approves a security training program proposal in accordance with this subsection, the public transportation agency that developed the program shall complete the training of all employees covered under the program.

(4) Updates of regulations and program revisions

The Secretary shall periodically review and update, as appropriate, the training regulations issued under subsection (a) to reflect new or changing security threats. Each public transportation agency shall revise its training program accordingly and provide additional training as necessary to its workers within a reasonable time after the regulations are updated.

(e) Applicability

A public transportation agency that receives a grant award under this subchapter shall be required to develop and implement a security training program pursuant to this section.

(f) Long-term training requirement

Any public transportation agency required to develop a security training program pursuant to this section shall provide routine and ongoing training for employees covered under the program, regardless of whether the public transportation agency receives subsequent grant awards.

(g) National Training Program

The Secretary shall ensure that the training program developed under subsection (a) is a component of the National Training Program established under section 748 of this title.

(h) Ferry exemption

This section shall not apply to any ferry system for which training is required to be conducted pursuant to section 70103 of title 46.

(i) Report

Not later than 2 years after the date of issuance of the final regulation, the Comptroller General shall review implementation of the training program, including interviewing a representative sample of public transportation agencies and employees, and report to the appropriate congressional committees, on the number of reviews conducted and the results. The Comptroller General may submit the report in both classified and redacted formats as necessary.

(Pub. L. 110–53, title XIV, §1408, Aug. 3, 2007, 121 Stat. 409.)

§1137a. Local law enforcement security training

(a) In general

The Secretary of Homeland Security, in consultation with public and private sector stakeholders, may in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, develop, through the Federal Law Enforcement Training Centers, a training program to enhance the protection, preparedness, and response capabilities of law enforcement agencies with respect to threats of terrorism and other threats, including targeted violence, at a surface transportation asset.

(b) Requirements

If the Secretary of Homeland Security develops the training program described in subsection (a), such training program shall—

(1) be informed by current information regarding tactics used by terrorists and others engaging in targeted violence;

(2) include tactical instruction tailored to the diverse nature of the surface transportation asset operational environment; and

(3) prioritize training officers from law enforcement agencies that are eligible for or receive grants under sections [1] 2003 or [1] 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and [1] 605) and officers employed by railroad carriers that operate passenger service, including interstate passenger service.

(c) Report

If the Secretary of Homeland Security develops the training program described in subsection (a), not later than one year after the date on which the Secretary first implements the program, and annually thereafter during each year the Secretary carries out the program, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the program. Each such report shall include, for the year covered by the report—

(1) a description of the curriculum for the training and any changes to such curriculum;

(2) an identification of any contracts entered into for the development or provision of training under the program;

(3) information on the law enforcement agencies the personnel of which received the training, and for each such agency, the number of participants; and

(4) a description of the measures used to ensure the program was carried out to provide for protections of privacy rights, civil rights, and civil liberties.

(d) Definitions

In this section:

(1) The term "public and private sector stakeholders" has the meaning given such term in section 114(t)(1)(c) [2] of title 49.

(2) The term "surface transportation asset" includes facilities, equipment, or systems used to provide transportation services by—

(A) a public transportation agency (as such term is defined in section 1131(5) of this title);

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49);

(C) an owner or operator of—

(i) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as such term is defined in section 1151(4) of this title); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(3) The term "targeted violence" means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(4) The term "terrorism" means the terms—

(A) domestic terrorism (as such term is defined in section 2331(5) of title 18); and

(B) international terrorism (as such term is defined in section 2331(1) of title 18).

(Pub. L. 117–81, div. F, title LXIV, §6419, Dec. 27, 2021, 135 Stat. 2417.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2022, and not as part of the National Transit Systems Security Act of 2007 which comprises this subchapter.

[1] So in original.

[2] So in original. Probably should be "114(t)(1)(C)".

§1138. Public transportation research and development

(a) Establishment of research and development program

The Secretary shall carry out a research and development program through the Homeland Security Advanced Research Projects Agency in the Science and Technology Directorate and in consultation with the Transportation Security Administration and with the Federal Transit Administration, for the purpose of improving the security of public transportation systems.

(b) Grants and contracts authorized

The Secretary shall award grants or contracts to public or private entities to conduct research and demonstrate technologies and methods to reduce and deter terrorist threats or mitigate damages resulting from terrorist attacks against public transportation systems.

(c) Use of funds

Grants or contracts awarded under subsection (a)—

(1) shall be coordinated with activities of the Homeland Security Advanced Research Projects Agency; and

(2) may be used to—

(A) research chemical, biological, radiological, or explosive detection systems that do not significantly impede passenger access;

(B) research imaging technologies;

(C) conduct product evaluations and testing;

(D) improve security and redundancy for critical communications, electrical power, and computer and train control systems;

(E) develop technologies for securing tunnels, transit bridges and aerial structures;

(F) research technologies that mitigate damages in the event of a cyber attack; and

(G) research other technologies or methods for reducing or deterring terrorist attacks against public transportation systems, or mitigating damage from such attacks.

(d) Privacy and civil rights and civil liberties issues

(1) Consultation

In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, as appropriate, and in accordance with section 142 of this title.

(2) Privacy impact assessments

In accordance with sections 142 and 345 of this title, the Chief Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed under this section.

(e) Reporting requirement

Each entity that is awarded a grant or contract under this section shall report annually to the Department on the use of grant or contract funds received under this section to ensure that the awards made are expended in accordance with the purposes of this subchapter and the priorities developed by the Secretary.

(f) Coordination

The Secretary shall ensure that the research is consistent with the priorities established in the National Strategy for Public Transportation Security and is coordinated, to the extent practicable, with other Federal, State, local, tribal, and private sector public transportation, railroad, commuter railroad, and over-the-road bus research initiatives to leverage resources and avoid unnecessary duplicative efforts.

(g) Return of misspent grant or contract funds

If the Secretary determines that a grantee or contractor used any portion of the grant or contract funds received under this section for a purpose other than the allowable uses specified under subsection (c), the grantee or contractor shall return any amount so used to the Treasury of the United States.

(h) Authorization of appropriations

There are authorized to be appropriated to the Secretary to make grants under this section—

(1) such sums as necessary for fiscal year 2007;
(2) $25,000,000 for fiscal year 2008;
(3) $25,000,000 for fiscal year 2009;
(4) $25,000,000 for fiscal year 2010; and
(5) $25,000,000 for fiscal year 2011.

(Pub. L. 110–53, title XIV, §1409, Aug. 3, 2007, 121 Stat. 411.)

§1139. Information sharing

(a) Intelligence sharing

The Secretary shall ensure that the Department of Transportation receives appropriate and timely notification of all credible terrorist threats against public transportation assets in the United States.

(b) Information Sharing and Analysis Center

(1) Authorization

The Secretary shall provide for the reasonable costs of the Information Sharing and Analysis Center for Public Transportation (referred to in this subsection as the "ISAC").

(2) Participation

The Secretary—

(A) shall require public transportation agencies that the Secretary determines to be at high risk of terrorist attack to participate in the ISAC;

(B) shall encourage all other public transportation agencies to participate in the ISAC;

(C) shall encourage the participation of nonprofit employee labor organizations representing public transportation employees, as appropriate; and

(D) shall not charge a fee for participating in the ISAC.

(c) Report

The Comptroller General shall report, not less than 3 years after August 3, 2007, to the appropriate congressional committees, as to the value and efficacy of the ISAC along with any other public transportation information-sharing programs ongoing at the Department. The report shall include an analysis of the user satisfaction of public transportation agencies on the state of information-sharing and the value that each system provides the user, the costs and benefits of all centers and programs,

the coordination among centers and programs, how each center or program contributes to implementing the information sharing plan under section 1203,[1] and analysis of the extent to which the ISAC is duplicative with the Department's information-sharing program.

(d) Authorization

(1) In general

There are authorized to be appropriated to the Secretary to carry out this section—

(A) $600,000 for fiscal year 2008;

(B) $600,000 for fiscal year 2009;

(C) $600,000 for fiscal year 2010; and

(D) such sums as may be necessary for 2011, provided the report required in subsection (c) of this section has been submitted to Congress.

(2) Availability of funds

Such sums shall remain available until expended.

(Pub. L. 110–53, title XIV, §1410, Aug. 3, 2007, 121 Stat. 412.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 1203, referred to in subsec. (c), is section 1203 of title XII of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 383, which amended section 114 of Title 49, Transportation, and enacted provisions set out as a note under section 114 of Title 49.

[1] *See References in Text note below.*

§1140. Threat assessments

Not later than 1 year after August 3, 2007, the Secretary shall complete a name-based security background check against the consolidated terrorist watchlist and an immigration status check for all public transportation frontline employees, similar to the threat assessment screening program required for facility employees and longshoremen by the Commandant of the Coast Guard under Coast Guard Notice USCG–2006–24189 (71 Fed. Reg. 25066 (April 8, 2006)).

(Pub. L. 110–53, title XIV, §1411, Aug. 3, 2007, 121 Stat. 413.)

§1141. Reporting requirements

(a) Annual report to Congress

(1) In general

Not later than March 31 of each year, the Secretary shall submit a report, containing the information described in paragraph (2), to the appropriate congressional committees.

(2) Contents

The report submitted under paragraph (1) shall include—

(A) a description of the implementation of the provisions of this subchapter;

(B) the amount of funds appropriated to carry out the provisions of this subchapter that have not been expended or obligated;

(C) the National Strategy for Public Transportation Security required under section 1133 of this title;

(D) an estimate of the cost to implement the National Strategy for Public Transportation Security which shall break out the aggregated total cost of needed capital and operational

security improvements for fiscal years 2008–2018; and

(E) the state of public transportation security in the United States, which shall include detailing the status of security assessments, the progress being made around the country in developing prioritized lists of security improvements necessary to make public transportation facilities and passengers more secure, the progress being made by agencies in developing security plans and how those plans differ from the security assessments and a prioritized list of security improvements being compiled by other agencies, as well as a random sample of an equal number of large- and small-scale projects currently underway.

(3) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(b) Annual report to Governors

(1) In general

Not later than March 31 of each year, the Secretary shall submit a report to the Governor of each State with a public transportation agency that has received a grant under this Act.

(2) Contents

The report submitted under paragraph (1) shall specify—

(A) the amount of grant funds distributed to each such public transportation agency; and

(B) the use of such grant funds.

(Pub. L. 110–53, title XIV, §1412, Aug. 3, 2007, 121 Stat. 413.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (b)(1), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266, known as the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted this chapter and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

§1142. Public transportation employee protections

(a) In general

A public transportation agency, a contractor or a subcontractor of such agency, or an officer or employee of such agency, shall not discharge, demote, suspend, reprimand, or in any other way discriminate against an employee if such discrimination is due, in whole or in part, to the employee's lawful, good faith act done, or perceived by the employer to have been done or about to be done—

(1) to provide information, directly cause information to be provided, or otherwise directly assist in any investigation regarding any conduct which the employee reasonably believes constitutes a violation of any Federal law, rule, or regulation relating to public transportation safety or security, or fraud, waste, or abuse of Federal grants or other public funds intended to be used for public transportation safety or security, if the information or assistance is provided to or an investigation stemming from the provided information is conducted by—

(A) a Federal, State, or local regulatory or law enforcement agency (including an office of the Inspector General under chapter 4 of title 5; [1]

(B) any Member of Congress, any Committee of Congress, or the Government Accountability Office; or

(C) a person with supervisory authority over the employee or such other person who has the authority to investigate, discover, or terminate the misconduct;

(2) to refuse to violate or assist in the violation of any Federal law, rule, or regulation relating to

public transportation safety or security;

(3) to file a complaint or directly cause to be brought a proceeding related to the enforcement of this section or to testify in that proceeding;

(4) to cooperate with a safety or security investigation by the Secretary of Transportation, the Secretary of Homeland Security, or the National Transportation Safety Board; or

(5) to furnish information to the Secretary of Transportation, the Secretary of Homeland Security, the National Transportation Safety Board, or any Federal, State, or local regulatory or law enforcement agency as to the facts relating to any accident or incident resulting in injury or death to an individual or damage to property occurring in connection with public transportation.

(b) Hazardous safety or security conditions

(1) A public transportation agency, or a contractor or a subcontractor of such agency, or an officer or employee of such agency, shall not discharge, demote, suspend, reprimand, or in any other way discriminate against an employee for—

(A) reporting a hazardous safety or security condition;

(B) refusing to work when confronted by a hazardous safety or security condition related to the performance of the employee's duties, if the conditions described in paragraph (2) exist; or

(C) refusing to authorize the use of any safety- or security-related equipment, track, or structures, if the employee is responsible for the inspection or repair of the equipment, track, or structures, when the employee believes that the equipment, track, or structures are in a hazardous safety or security condition, if the conditions described in paragraph (2) of this subsection exist.

(2) A refusal is protected under paragraph (1)(B) and (C) if—

(A) the refusal is made in good faith and no reasonable alternative to the refusal is available to the employee;

(B) a reasonable individual in the circumstances then confronting the employee would conclude that—

(i) the hazardous condition presents an imminent danger of death or serious injury; and

(ii) the urgency of the situation does not allow sufficient time to eliminate the danger without such refusal; and

(C) the employee, where possible, has notified the public transportation agency of the existence of the hazardous condition and the intention not to perform further work, or not to authorize the use of the hazardous equipment, track, or structures, unless the condition is corrected immediately or the equipment, track, or structures are repaired properly or replaced.

(3) In this subsection, only subsection (b)(1)(A) shall apply to security personnel, including transit police, employed or utilized by a public transportation agency to protect riders, equipment, assets, or facilities.

(c) Enforcement action

(1) Filing and notification

A person who believes that he or she has been discharged or otherwise discriminated against by any person in violation of subsection (a) or (b) may, not later than 180 days after the date on which such violation occurs, file (or have any person file on his or her behalf) a complaint with the Secretary of Labor alleging such discharge or discrimination. Upon receipt of a complaint filed under this paragraph, the Secretary of Labor shall notify, in writing, the person named in the complaint and the person's employer of the filing of the complaint, of the allegations contained in the complaint, of the substance of evidence supporting the complaint, and of the opportunities that will be afforded to such person under paragraph (2).

(2) Investigation; preliminary order

(A) In general

Not later than 60 days after the date of receipt of a complaint filed under paragraph (1) and

after affording the person named in the complaint an opportunity to submit to the Secretary of Labor a written response to the complaint and an opportunity to meet with a representative of the Secretary of Labor to present statements from witnesses, the Secretary of Labor shall conduct an investigation and determine whether there is reasonable cause to believe that the complaint has merit and notify, in writing, the complainant and the person alleged to have committed a violation of subsection (a) or (b) of the Secretary of Labor's findings. If the Secretary of Labor concludes that there is a reasonable cause to believe that a violation of subsection (a) or (b) has occurred, the Secretary of Labor shall accompany the Secretary of Labor's findings with a preliminary order providing the relief prescribed by paragraph (3)(B). Not later than 30 days after the date of notification of findings under this paragraph, either the person alleged to have committed the violation or the complainant may file objections to the findings or preliminary order, or both, and request a hearing on the record. The filing of such objections shall not operate to stay any reinstatement remedy contained in the preliminary order. Such hearings shall be conducted expeditiously. If a hearing is not requested in such 30-day period, the preliminary order shall be deemed a final order that is not subject to judicial review.

(B) Requirements

(i) Required showing by complainant

The Secretary of Labor shall dismiss a complaint filed under this subsection and shall not conduct an investigation otherwise required under subparagraph (A) unless the complainant makes a prima facie showing that any behavior described in subsection (a) or (b) was a contributing factor in the unfavorable personnel action alleged in the complaint.

(ii) Showing by employer

Notwithstanding a finding by the Secretary of Labor that the complainant has made the showing required under clause (i), no investigation otherwise required under paragraph (A) shall be conducted if the employer demonstrates, by clear and convincing evidence, that the employer would have taken the same unfavorable personnel action in the absence of that behavior.

(iii) Criteria for determination by Secretary of Labor

The Secretary of Labor may determine that a violation of subsection (a) or (b) has occurred only if the complainant demonstrates that any behavior described in subsection (a) or (b) was a contributing factor in the unfavorable personnel action alleged in the complaint.

(iv) Prohibition

Relief may not be ordered under paragraph (A) if the employer demonstrates by clear and convincing evidence that the employer would have taken the same unfavorable personnel action in the absence of that behavior.

(3) Final order

(A) Deadline for issuance; settlement agreements

Not later than 120 days after the date of conclusion of a hearing under paragraph (2), the Secretary of Labor shall issue a final order providing the relief prescribed by this paragraph or denying the complaint. At any time before issuance of a final order, a proceeding under this subsection may be terminated on the basis of a settlement agreement entered into by the Secretary of Labor, the complainant, and the person alleged to have committed the violation.

(B) Remedy

If, in response to a complaint filed under paragraph (1), the Secretary of Labor determines that a violation of subsection (a) or (b) has occurred, the Secretary of Labor shall order the person who committed such violation to—

(i) take affirmative action to abate the violation; and

(ii) provide the remedies described in subsection (d).

(C) Order

If an order is issued under subparagraph (B), the Secretary of Labor, at the request of the complainant, shall assess against the person against whom the order is issued a sum equal to the aggregate amount of all costs and expenses (including attorney and expert witness fees) reasonably incurred, as determined by the Secretary of Labor, by the complainant for, or in connection with, bringing the complaint upon which the order was issued.

(D) Frivolous complaints

If the Secretary of Labor finds that a complaint under paragraph (1) is frivolous or has been brought in bad faith, the Secretary of Labor may award to the prevailing employer reasonable attorney fees not exceeding $1,000.

(4) Review

(A) Appeal to Court of Appeals

Any person adversely affected or aggrieved by an order issued under paragraph (3) may obtain review of the order in the United States Court of Appeals for the circuit in which the violation, with respect to which the order was issued, allegedly occurred or the circuit in which the complainant resided on the date of such violation. The petition for review must be filed not later than 60 days after the date of the issuance of the final order of the Secretary of Labor. Review shall conform to chapter 7 of title 5. The commencement of proceedings under this subparagraph shall not, unless ordered by the court, operate as a stay of the order.

(B) Limitation on collateral attack

An order of the Secretary of Labor with respect to which review could have been obtained under subparagraph (A) shall not be subject to judicial review in any criminal or other civil proceeding.

(5) Enforcement of order by Secretary of Labor

Whenever any person has failed to comply with an order issued under paragraph (3), the Secretary of Labor may file a civil action in the United States district court for the district in which the violation was found to occur to enforce such order. In actions brought under this paragraph, the district courts shall have jurisdiction to grant all appropriate relief including, but not limited to, injunctive relief and compensatory damages.

(6) Enforcement of order by parties

(A) Commencement of action

A person on whose behalf an order was issued under paragraph (3) may commence a civil action against the person to whom such order was issued to require compliance with such order. The appropriate United States district court shall have jurisdiction, without regard to the amount in controversy or the citizenship of the parties, to enforce such order.

(B) Attorney fees

The court, in issuing any final order under this paragraph, may award costs of litigation (including reasonable attorney and expert witness fees) to any party whenever the court determines such award is appropriate.

(7) De novo review

With respect to a complaint under paragraph (1), if the Secretary of Labor has not issued a final decision within 210 days after the filing of the complaint and if the delay is not due to the bad faith of the employee, the employee may bring an original action at law or equity for de novo review in the appropriate district court of the United States, which shall have jurisdiction over such an action without regard to the amount in controversy, and which action shall, at the request of either party to such action, be tried by the court with a jury. The action shall be governed by the same legal burdens of proof specified in paragraph (2)(B) for review by the Secretary of Labor.

(d) Remedies

(1) In general

An employee prevailing in any action under subsection (c) shall be entitled to all relief necessary to make the employee whole.

(2) Damages

Relief in an action under subsection (c) (including an action described in (c)(7)) [2] shall include—

(A) reinstatement with the same seniority status that the employee would have had, but for the discrimination;

(B) any backpay, with interest; and

(C) compensatory damages, including compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees.

(3) Possible relief

Relief in any action under subsection (c) may include punitive damages in an amount not to exceed $250,000.

(e) Election of remedies

An employee may not seek protection under both this section and another provision of law for the same allegedly unlawful act of the public transportation agency.

(f) No preemption

Nothing in this section preempts or diminishes any other safeguards against discrimination, demotion, discharge, suspension, threats, harassment, reprimand, retaliation, or any other manner of discrimination provided by Federal or State law.

(g) Rights retained by employee

Nothing in this section shall be construed to diminish the rights, privileges, or remedies of any employee under any Federal or State law or under any collective bargaining agreement. The rights and remedies in this section may not be waived by any agreement, policy, form, or condition of employment.

(h) Disclosure of identity

(1) Except as provided in paragraph (2) of this subsection, or with the written consent of the employee, the Secretary of Transportation or the Secretary of Homeland Security may not disclose the name of an employee who has provided information described in subsection (a)(1).

(2) The Secretary of Transportation or the Secretary of Homeland Security shall disclose to the Attorney General the name of an employee described in paragraph (1) of this subsection if the matter is referred to the Attorney General for enforcement. The Secretary making such disclosure shall provide reasonable advance notice to the affected employee if disclosure of that person's identity or identifying information is to occur.

(i) Process for reporting security problems to the Department of Homeland Security

(1) Establishment of process

The Secretary shall establish through regulations after an opportunity for notice and comment, and provide information to the public regarding, a process by which any person may submit a report to the Secretary regarding public transportation security problems, deficiencies, or vulnerabilities.

(2) Acknowledgment of receipt

If a report submitted under paragraph (1) identifies the person making the report, the Secretary shall respond promptly to such person and acknowledge receipt of the report.

(3) Steps to address problem

The Secretary shall review and consider the information provided in any report submitted under

paragraph (1) and shall take appropriate steps to address any problems or deficiencies identified.

(Pub. L. 110–53, title XIV, §1413, Aug. 3, 2007, 121 Stat. 414; Pub. L. 117–286, §4(b)(22), Dec. 27, 2022, 136 Stat. 4345.)

EDITORIAL NOTES

AMENDMENTS

2022—Subsec. (a)(1)(A). Pub. L. 117–286 substituted "chapter 4 of title 5;" for "the Inspector General Act of 1978 (5 U.S.C. App.; Public Law 95–452);".

[1] So in original. The semicolon probably should be preceded by a closing parenthesis.

[2] So in original. Probably should be "subsection (c)(7))".

§1143. Security background checks of covered individuals for public transportation

(a) Definitions

In this section, the following definitions apply:

(1) Security background check

The term "security background check" means reviewing the following for the purpose of identifying individuals who may pose a threat to transportation security, national security, or of terrorism:

(A) Relevant criminal history databases.

(B) In the case of an alien (as defined in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3))), the relevant databases to determine the status of the alien under the immigration laws of the United States.

(C) Other relevant information or databases, as determined by the Secretary.

(2) Covered individual

The term "covered individual" means an employee of a public transportation agency or a contractor or subcontractor of a public transportation agency.

(b) Guidance

(1) Any guidance, recommendations, suggested action items, or any other widely disseminated voluntary action item issued by the Secretary to a public transportation agency or a contractor or subcontractor of a public transportation agency relating to performing a security background check of a covered individual shall contain recommendations on the appropriate scope and application of such a security background check, including the time period covered, the types of disqualifying offenses, and a redress process for adversely impacted covered individuals consistent with subsections (c) and (d) of this section.

(2) Not later than 60 days after August 3, 2007, any guidance, recommendations, suggested action items, or any other widely disseminated voluntary action item issued by the Secretary prior to August 3, 2007, to a public transportation agency or a contractor or subcontractor of a public transportation agency relating to performing a security background check of a covered individual shall be updated in compliance with paragraph (b)(1).

(3) If a public transportation agency or a contractor or subcontractor of a public transportation agency performs a security background check on a covered individual to fulfill guidance issued by the Secretary under paragraph (1) or (2), the Secretary shall not consider such guidance fulfilled unless an adequate redress process as described in subsection (d) is provided to covered individuals.

(c) Requirements

If the Secretary issues a rule, regulation or directive requiring a public transportation agency or contractor or subcontractor of a public transportation agency to perform a security background check of a covered individual, then the Secretary shall prohibit a public transportation agency or contractor or subcontractor of a public transportation agency from making an adverse employment decision, including removal or suspension of the employee, due to such rule, regulation, or directive with respect to a covered individual unless the public transportation agency or contractor or subcontractor of a public transportation agency determines that the covered individual—

(1) has been convicted of, has been found not guilty of by reason of insanity, or is under want, warrant, or indictment for a permanent disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations;

(2) was convicted of or found not guilty by reason of insanity of an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, within 7 years of the date that the public transportation agency or contractor or subcontractor of the public transportation agency performs the security background check; or

(3) was incarcerated for an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, and released from incarceration within 5 years of the date that the public transportation agency or contractor or subcontractor of a public transportation agency performs the security background check.

(d) Redress process

If the Secretary issues a rule, regulation, or directive requiring a public transportation agency or contractor or subcontractor of a public transportation agency to perform a security background check of a covered individual, the Secretary shall—

(1) provide an adequate redress process for a covered individual subjected to an adverse employment decision, including removal or suspension of the employee, due to such rule, regulation, or directive that is consistent with the appeals and waiver process established for applicants for commercial motor vehicle hazardous materials endorsements and transportation workers at ports, as required by section 70105(c) of title 49; [1] and

(2) have the authority to order an appropriate remedy, including reinstatement of the covered individual, should the Secretary determine that a public transportation agency or contractor or subcontractor of a public transportation agency wrongfully made an adverse employment decision regarding a covered individual pursuant to such rule, regulation, or directive.

(e) False statements

A public transportation agency or a contractor or subcontractor of a public transportation agency may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary related to security background check requirements for covered individuals when conducting a security background check. Not later than 1 year after August 3, 2007, the Secretary shall issue a regulation that prohibits a public transportation agency or a contractor or subcontractor of a public transportation agency from knowingly misrepresenting to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary related to security background check requirements for covered individuals when conducting a security background check.

(f) Rights and responsibilities

Nothing in this section shall be construed to abridge a public transportation agency's or a contractor or subcontractor of a public transportation agency's rights or responsibilities to make adverse employment decisions permitted by other Federal, State, or local laws. Nothing in the [2] section shall be construed to abridge rights and responsibilities of covered individuals, a public transportation agency, or a contractor or subcontractor of a public transportation agency under any other Federal, State, or local laws or collective bargaining agreement.

(g) No preemption of Federal or State law

Nothing in this section shall be construed to preempt a Federal, State, or local law that requires criminal history background checks, immigration status checks, or other background checks of covered individuals.

(h) Statutory construction

Nothing in this section shall be construed to affect the process for review established under section 70105(c) of title 46, including regulations issued pursuant to such section.

(Pub. L. 110–53, title XIV, §1414, Aug. 3, 2007, 121 Stat. 419.)

[1] *So in original. Probably should be title "46;".*

[2] *So in original. Probably should be "this".*

§1144. Limitation on fines and civil penalties

(a) Inspectors

Surface transportation inspectors shall be prohibited from issuing fines to public transportation agencies for violations of the Department's regulations or orders except through the process described in subsection (b).

(b) Civil penalties

The Secretary shall be prohibited from assessing civil penalties against public transportation agencies for violations of the Department's regulations or orders, except in accordance with the following:

(1) In the case of a public transportation agency that is found to be in violation of a regulation or order issued by the Secretary, the Secretary shall seek correction of the violation through a written notice to the public transportation agency and shall give the public transportation agency reasonable opportunity to correct the violation or propose an alternative means of compliance acceptable to the Secretary.

(2) If the public transportation agency does not correct the violation or propose an alternative means of compliance acceptable to the Secretary within a reasonable time period that is specified in the written notice, the Secretary may take any action authorized in section 114 of title 49.

(c) Limitation on Secretary

The Secretary shall not initiate civil enforcement actions for violations of administrative and procedural requirements pertaining to the application for and expenditure of funds awarded under transportation security grant programs under this subchapter.

(Pub. L. 110–53, title XIV, §1415, Aug. 3, 2007, 121 Stat. 422.)

SUBCHAPTER IV—SURFACE TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

§1151. Definitions

In this subchapter, the following definitions apply:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(3) Department

The term "Department" means the Department of Homeland Security.

(4) Over-the-road bus

The term "over-the-road bus" means a bus characterized by an elevated passenger deck located over a baggage compartment.

(5) Over-the-road bus frontline employees

In this section,[1] the term "over-the-road bus frontline employees" means over-the-road bus drivers, security personnel, dispatchers, maintenance and maintenance support personnel, ticket agents, other terminal employees, and other employees of an over-the-road bus operator or terminal owner or operator that the Secretary determines should receive security training under this subchapter.

(6) Railroad frontline employees

In this section,[1] the term "railroad frontline employees" means security personnel, dispatchers, locomotive engineers, conductors, trainmen, other onboard employees, maintenance and maintenance support personnel, bridge tenders, and any other employees of railroad carriers that the Secretary determines should receive security training under this subchapter.

(7) Railroad

The term "railroad" has the meaning that term has in section 20102 of title 49.

(8) Railroad carrier

The term "railroad carrier" has the meaning that term has in section 20102 of title 49.

(9) State

The term "State" means any one of the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(10) Terrorism

The term "terrorism" has the meaning that term has in section 101 of this title.

(11) Transportation

The term "transportation", as used with respect to an over-the-road bus, means the movement of passengers or property by an over-the-road bus—

(A) in the jurisdiction of the United States between a place in a State and a place outside the State (including a place outside the United States); or

(B) in a State that affects trade, traffic, and transportation described in subparagraph (A).

(12) United States

The term "United States" means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(13) Security-sensitive material

The term "security-sensitive material" means a material, or a group or class of material, in a particular amount and form that the Secretary, in consultation with the Secretary of Transportation, determines, through a rulemaking with opportunity for public comment, poses a

significant risk to national security while being transported in commerce due to the potential use of the material in an act of terrorism. In making such a designation, the Secretary shall, at a minimum, consider the following:

(A) Class 7 radioactive materials.

(B) Division 1.1, 1.2, or 1.3 explosives.

(C) Materials poisonous or toxic by inhalation, including Division 2.3 gases and Division 6.1 materials.

(D) A select agent or toxin regulated by the Centers for Disease Control and Prevention under part 73 of title 42, Code of Federal Regulations.

(14) Disadvantaged business concerns

The term "disadvantaged business concerns" means small businesses that are owned and controlled by socially and economically disadvantaged individuals as defined in section 124,[2] of title 13, Code of Federal Regulations.

(15) Amtrak

The term "Amtrak" means the National Railroad Passenger Corporation.

(Pub. L. 110–53, title XV, §1501, Aug. 3, 2007, 121 Stat. 422.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title XV of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 422, which enacted this subchapter, amended section 1992 of Title 18, Crimes and Criminal Procedure, and sections 114, 5103a, 14504, 20106, 20109, 24301, 28101, and 31105 of Title 49, Transportation, enacted provisions set out as notes under sections 13908 and 14504 of Title 49, and amended provisions set out as a note under section 14504 of Title 49. For complete classification of title XV to the Code, see Tables.

[1] So in original. "In this section," probably should not appear.

[2] So in original. Probably should be "part 124,".

§1152. Oversight and grant procedures

(a) Secretarial oversight

The Secretary, in coordination with [1] Secretary of Transportation for grants awarded to Amtrak, shall establish necessary procedures, including monitoring and audits, to ensure that grants made under this subchapter are expended in accordance with the purposes of this subchapter and the priorities and other criteria developed by the Secretary.

(b) Additional audits and reviews

The Secretary, and the Secretary of Transportation for grants awarded to Amtrak, may award contracts to undertake additional audits and reviews of the safety, security, procurement, management, and financial compliance of a recipient of amounts under this subchapter.

(c) Procedures for grant award

Not later than 180 days after August 3, 2007, the Secretary shall prescribe procedures and schedules for the awarding of grants under this subchapter, including application and qualification procedures, and a record of decision on applicant eligibility. The procedures shall include the execution of a grant agreement between the grant recipient and the Secretary and shall be consistent, to the extent practicable, with the grant procedures established under section 70107(i) and (j) of title 46.

(d) Additional authority

(1) Issuance

The Secretary may issue non-binding letters of intent to recipients of a grant under this subchapter, to commit funding from future budget authority of an amount, not more than the Federal Government's share of the project's cost, for a capital improvement project.

(2) Schedule

The letter of intent under this subsection shall establish a schedule under which the Secretary will reimburse the recipient for the Government's share of the project's costs, as amounts become available, if the recipient, after the Secretary issues that letter, carries out the project without receiving amounts under a grant issued under this subchapter.

(3) Notice to Secretary

A recipient that has been issued a letter of intent under this section shall notify the Secretary of the recipient's intent to carry out a project before the project begins.

(4) Notice to Congress

The Secretary shall transmit to the appropriate congressional committees a written notification at least 5 days before the issuance of a letter of intent under this subsection.

(5) Limitations

A letter of intent issued under this subsection is not an obligation of the Federal Government under section 1501 of title 31, and the letter is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(e) Return of misspent grant funds

As part of the grant agreement under subsection (c), the Secretary shall require grant applicants to return any misspent grant funds received under this subchapter that the Secretary considers to have been spent for a purpose other than those specified in the grant award. The Secretary shall take all necessary actions to recover such funds.

(f) Congressional notification

Not later than 5 days before the award of any grant is made under this subchapter, the Secretary shall notify the appropriate congressional committees of the intent to award such grant.

(g) Guidelines

The Secretary shall ensure, to the extent practicable, that grant recipients under this subchapter who use contractors or subcontractors use small, minority, women-owned, or disadvantaged business concerns as contractors or subcontractors when appropriate.

(Pub. L. 110–53, title XV, §1502, Aug. 3, 2007, 121 Stat. 424.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this title", meaning title XV of Pub. L. 110–53, which is classified principally to this subchapter. For complete classification of title XV to the Code, see References in Text note under section 1151 of this title and Tables.

[1] *So in original. The word "the" probably should appear.*

§1153. Authorization of appropriations

There are authorized to be appropriated to the Secretary of Transportation to carry out section

1165 of this title—

(1) $38,000,000 for fiscal year 2008;
(2) $40,000,000 for fiscal year 2009;
(3) $55,000,000 for fiscal year 2010; and
(4) $70,000,000 for fiscal year 2011.

(Pub. L. 110–53, title XV, §1503(b), Aug. 3, 2007, 121 Stat. 425.)

§1154. Public awareness

Not later than 180 days after August 3, 2007, the Secretary shall develop a national plan for railroad and over-the-road bus security public outreach and awareness. Such a plan shall be designed to increase awareness of measures that the general public, passengers, and employees of railroad carriers and over-the-road bus operators can take to increase the security of the national railroad and over-the-road bus transportation systems. Such a plan shall also provide outreach to railroad carriers and over-the-road bus operators and their employees to improve their awareness of available technologies, ongoing research and development efforts, and available Federal funding sources to improve security. Not later than 9 months after August 3, 2007, the Secretary shall implement the plan developed under this section.

(Pub. L. 110–53, title XV, §1504, Aug. 3, 2007, 121 Stat. 425.)

§1155. Security awareness program

(a) Establishment

The Administrator shall establish a program to promote surface transportation security through the training of surface transportation operators and frontline employees on each of the skills identified in subsection (c).

(b) Application

The program established under subsection (a) shall apply to all modes of surface transportation, including public transportation, rail, highway, motor carrier, and pipeline.

(c) Training

The program established under subsection (a) shall cover, at a minimum, the skills necessary to recognize, assess, and respond to suspicious items or actions that could indicate a threat to transportation.

(d) Assessment

(1) In general

The Administrator shall conduct an assessment of current training programs for surface transportation operators and frontline employees.

(2) Contents

The assessment shall identify—

(A) whether other training is being provided, either voluntarily or in response to other Federal requirements; and

(B) whether there are any gaps in existing training.

(e) Updates

The Administrator shall ensure the program established under subsection (a) is updated as necessary to address changes in risk and terrorist methods and to close any gaps identified in the assessment under subsection (d).

(f) Suspicious activity reporting

(1) In general

The Secretary shall maintain a national telephone number for an individual to use to report suspicious activity under this section to the Administration.

(2) Procedures

The Administrator shall establish procedures for the Administration—

(A) to review and follow-up, as necessary, on each report received under paragraph (1); and

(B) to share, as necessary and in accordance with law, the report with appropriate Federal, State, local, and tribal entities.

(3) Rule of construction

Nothing in this section may be construed to—

(A) replace or affect in any way the use of 9–1–1 services in an emergency; or

(B) replace or affect in any way the security training program requirements specified in sections 1137, 1167, and 1184 of this title.

(g) Definition of frontline employee

In this section, the term "frontline employee" includes—

(1) an employee of a public transportation agency who is a transit vehicle driver or operator, dispatcher, maintenance and maintenance support employee, station attendant, customer service employee, security employee, or transit police, or any other employee who has direct contact with riders on a regular basis, and any other employee of a public transportation agency that the Administrator determines should receive security training under this section or that is receiving security training under other law;

(2) over-the-road bus drivers, security personnel, dispatchers, maintenance and maintenance support personnel, ticket agents, other terminal employees, and other employees of an over-the-road bus operator or terminal owner or operator that the Administrator determines should receive security training under this section or that is receiving security training under other law; or

(3) security personnel, dispatchers, locomotive engineers, conductors, trainmen, other onboard employees, maintenance and maintenance support personnel, bridge tenders, and any other employees of railroad carriers that the Administrator determines should receive security training under this section or that is receiving security training under other law.

(Pub. L. 115–254, div. K, title I, §1976, Oct. 5, 2018, 132 Stat. 3616.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the TSA Modernization Act and also as part of the FAA Reauthorization Act of 2018, and not as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITIONS

For definitions of "Administrator" and "Secretary" as used in this section, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.

§1156. Nuclear material and explosive detection technology

The Secretary, in coordination with the Director of the National Institute of Standards and Technology and the head of each relevant Federal department or agency researching nuclear material detection systems or explosive detection systems, shall research, facilitate, and, to the extent practicable, deploy next generation technologies, including active neutron interrogation, to detect nuclear material and explosives in transportation systems and transportation facilities.

(Pub. L. 115–254, div. K, title I, §1984, Oct. 5, 2018, 132 Stat. 3621.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the TSA Modernization Act and also as part of the FAA Reauthorization Act of 2018, and not as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

DEFINITION

For definition of "Secretary" as used in this section, see section 1902 of Pub. L. 115–254, set out as a note under section 101 of Title 49, Transportation.

PART B—RAILROAD SECURITY

§1161. Railroad transportation security risk assessment and National Strategy

(a) Risk assessment

The Secretary shall establish a Federal task force, including the Transportation Security Administration and other agencies within the Department, the Department of Transportation, and other appropriate Federal agencies, to complete, within 6 months of August 3, 2007, a nationwide risk assessment of a terrorist attack on railroad carriers. The assessment shall include—

(1) a methodology for conducting the risk assessment, including timelines, that addresses how the Department will work with the entities described in subsection (c) and make use of existing Federal expertise within the Department, the Department of Transportation, and other appropriate agencies;

(2) identification and evaluation of critical assets and infrastructure, including tunnels used by railroad carriers in high-threat urban areas;

(3) identification of risks to those assets and infrastructure;

(4) identification of risks that are specific to the transportation of hazardous materials via railroad;

(5) identification of risks to passenger and cargo security, transportation infrastructure protection systems, operations, communications systems, and any other area identified by the assessment;

(6) an assessment of employee training and emergency response planning;

(7) an assessment of public and private operational recovery plans, taking into account the plans for the maritime sector required under section 70103 of title 46, to expedite, to the maximum extent practicable, the return of an adversely affected railroad transportation system or facility to its normal performance level after a major terrorist attack or other security event on that system or facility; and

(8) an account of actions taken or planned by both public and private entities to address identified railroad security issues and an assessment of the effective integration of such actions.

(b) National Strategy

(1) Requirement

Not later than 9 months after August 3, 2007, and based upon the assessment conducted under subsection (a), the Secretary, consistent with and as required by section 114(t) [1] of title 49, shall develop and implement the modal plan for railroad transportation, entitled the "National Strategy

for Railroad Transportation Security".

(2) Contents

The modal plan shall include prioritized goals, actions, objectives, policies, mechanisms, and schedules for, at a minimum—

(A) improving the security of railroad tunnels, railroad bridges, railroad switching and car storage areas, other railroad infrastructure and facilities, information systems, and other areas identified by the Secretary as posing significant railroad-related risks to public safety and the movement of interstate commerce, taking into account the impact that any proposed security measure might have on the provision of railroad service or on operations served or otherwise affected by railroad service;

(B) deploying equipment and personnel to detect security threats, including those posed by explosives and hazardous chemical, biological, and radioactive substances, and any appropriate countermeasures;

(C) consistent with section 1167 of this title, training railroad employees in terrorism prevention, preparedness, passenger evacuation, and response activities;

(D) conducting public outreach campaigns for railroads regarding security, including educational initiatives designed to inform the public on how to prevent, prepare for, respond to, and recover from a terrorist attack on railroad transportation;

(E) providing additional railroad security support for railroads at high or severe threat levels of alert;

(F) ensuring, in coordination with freight and intercity and commuter passenger railroads, the continued movement of freight and passengers in the event of an attack affecting the railroad system, including the possibility of rerouting traffic due to the loss of critical infrastructure, such as a bridge, tunnel, yard, or station;

(G) coordinating existing and planned railroad security initiatives undertaken by the public and private sectors;

(H) assessing—

(i) the usefulness of covert testing of railroad security systems;

(ii) the ability to integrate security into infrastructure design; and

(iii) the implementation of random searches of passengers and baggage; and

(I) identifying the immediate and long-term costs of measures that may be required to address those risks and public and private sector sources to fund such measures.

(3) Responsibilities

The Secretary shall include in the modal plan a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, government-sponsored entities, tribal governments, and appropriate stakeholders described in subsection (c). The plan shall also include—

(A) the identification of, and a plan to address, gaps and unnecessary overlaps in the roles, responsibilities, and authorities described in this paragraph;

(B) a methodology for how the Department will work with the entities described in subsection (c), and make use of existing Federal expertise within the Department, the Department of Transportation, and other appropriate agencies;

(C) a process for facilitating security clearances for the purpose of intelligence and information sharing with the entities described in subsection (c), as appropriate;

(D) a strategy and timeline, coordinated with the research and development program established under section 1168 of this title, for the Department, the Department of Transportation, other appropriate Federal agencies and private entities to research and develop new technologies for securing railroad systems; and

(E) a process for coordinating existing or future security strategies and plans for railroad transportation, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7; Executive Order No. 13416: "Strengthening Surface

Transportation Security" dated December 5, 2006; the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities dated September 28, 2004, and any and all subsequent annexes to this Memorandum of Understanding, and any other relevant agreements between the two Departments.

(c) Consultation with stakeholders

In developing the National Strategy required under this section, the Secretary shall consult with railroad management, nonprofit employee organizations representing railroad employees, owners or lessors of railroad cars used to transport hazardous materials, emergency responders, offerors of security-sensitive materials, public safety officials, and other relevant parties.

(d) Adequacy of existing plans and strategies

In developing the risk assessment and National Strategy required under this section, the Secretary shall utilize relevant existing plans, strategies, and risk assessments developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) [1] of title 49 or Homeland Security Presidential Directive–7, and, as appropriate, assessments developed by other public and private stakeholders.

(e) Report

(1) Contents

Not later than 1 year after August 3, 2007, the Secretary shall transmit to the appropriate congressional committees a report containing—

(A) the assessment and the National Strategy required by this section; and

(B) an estimate of the cost to implement the National Strategy.

(2) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(f) Annual updates

Consistent with the requirements of section 114(t) [1] of title 49, the Secretary shall update the assessment and National Strategy each year and transmit a report, which may be submitted in both classified and redacted formats, to the appropriate congressional committees containing the updated assessment and recommendations.

(g) Funding

Out of funds appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section $5,000,000 for fiscal year 2008.

(Pub. L. 110–53, title XV, §1511, Aug. 3, 2007, 121 Stat. 426.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(t) of title 49, referred to in subsecs. (b)(1), (d), and (f), was redesignated section 114(s) of title 49 by Pub. L. 110–161, div. E, title V, §568(a), Dec. 26, 2007, 121 Stat. 2092.

Executive Order No. 13416, referred to in subsec. (b)(3)(E), is set out as a note under section 1101 of this title.

Section 114(w) of title 49, referred to in subsec. (g), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1162. Railroad carrier assessments and plans

(a) In general

Not later than 12 months after August 3, 2007, the Secretary shall issue regulations that—

(1) require each railroad carrier assigned to a high-risk tier under this section to—

(A) conduct a vulnerability assessment in accordance with subsections (c) and (d); and

(B) to [1] prepare, submit to the Secretary for approval, and implement a security plan in accordance with this section that addresses security performance requirements; and

(2) establish standards and guidelines, based on and consistent with the risk assessment and National Strategy for Railroad Transportation Security developed under section 1161 of this title, for developing and implementing the vulnerability assessments and security plans for railroad carriers assigned to high-risk tiers.

(b) Non high-risk programs

The Secretary may establish a security program for railroad carriers not assigned to a high-risk tier, including—

(1) guidance for such carriers in conducting vulnerability assessments and preparing and implementing security plans, as determined appropriate by the Secretary; and

(2) a process to review and approve such assessments and plans, as appropriate.

(c) Deadline for submission

Not later than 9 months after the date of issuance of the regulations under subsection (a), the vulnerability assessments and security plans required by such regulations for railroad carriers assigned to a high-risk tier shall be completed and submitted to the Secretary for review and approval.

(d) Vulnerability assessments

(1) Requirements

The Secretary shall provide technical assistance and guidance to railroad carriers in conducting vulnerability assessments under this section and shall require that each vulnerability assessment of a railroad carrier assigned to a high-risk tier under this section, include, as applicable—

(A) identification and evaluation of critical railroad carrier assets and infrastructure, including platforms, stations, intermodal terminals, tunnels, bridges, switching and storage areas, and information systems as appropriate;

(B) identification of the vulnerabilities to those assets and infrastructure;

(C) identification of strengths and weaknesses in—

(i) physical security;

(ii) passenger and cargo security, including the security of security-sensitive materials being transported by railroad or stored on railroad property;

(iii) programmable electronic devices, computers, or other automated systems which are used in providing the transportation;

(iv) alarms, cameras, and other protection systems;

(v) communications systems and utilities needed for railroad security purposes, including dispatching and notification systems;

(vi) emergency response planning;

(vii) employee training; and

(viii) such other matters as the Secretary determines appropriate; and

(D) identification of redundant and backup systems required to ensure the continued operation of critical elements of a railroad carrier's system in the event of an attack or other incident, including disruption of commercial electric power or communications network.

(2) Threat information

The Secretary shall provide in a timely manner to the appropriate employees of a railroad carrier, as designated by the railroad carrier, threat information that is relevant to the carrier when

preparing and submitting a vulnerability assessment and security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in railroad security.

(e) Security plans

(1) Requirements

The Secretary shall provide technical assistance and guidance to railroad carriers in preparing and implementing security plans under this section, and shall require that each security plan of a railroad carrier assigned to a high-risk tier under this section include, as applicable—

(A) identification of a security coordinator having authority—

(i) to implement security actions under the plan;

(ii) to coordinate security improvements; and

(iii) to receive immediate communications from appropriate Federal officials regarding railroad security;

(B) a list of needed capital and operational improvements;

(C) procedures to be implemented or used by the railroad carrier in response to a terrorist attack, including evacuation and passenger communication plans that include individuals with disabilities as appropriate;

(D) identification of steps taken with State and local law enforcement agencies, emergency responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

(E) a strategy and timeline for conducting training under section 1167 of this title;

(F) enhanced security measures to be taken by the railroad carrier when the Secretary declares a period of heightened security risk;

(G) plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident;

(H) a strategy for implementing enhanced security for shipments of security-sensitive materials, including plans for quickly locating and securing such shipments in the event of a terrorist attack or security incident; and

(I) such other actions or procedures as the Secretary determines are appropriate to address the security of railroad carriers.

(2) Security coordinator requirements

The Secretary shall require that the individual serving as the security coordinator identified in paragraph (1)(A) is a citizen of the United States. The Secretary may waive this requirement with respect to an individual if the Secretary determines that it is appropriate to do so based on a background check of the individual and a review of the consolidated terrorist watchlist.

(3) Consistency with other plans

The Secretary shall ensure that the security plans developed by railroad carriers under this section are consistent with the risk assessment and National Strategy for Railroad Transportation Security developed under section 1161 of this title.

(f) Deadline for review process

Not later than 6 months after receiving the assessments and plans required under this section, the Secretary shall—

(1) review each vulnerability assessment and security plan submitted to the Secretary in accordance with subsection (c);

(2) require amendments to any security plan that does not meet the requirements of this section; and

(3) approve any vulnerability assessment or security plan that meets the requirements of this section.

(g) Interim security measures

The Secretary may require railroad carriers, during the period before the deadline established under subsection (c), to submit a security plan under subsection (e) to implement any necessary interim security measures essential to providing adequate security of the railroad carrier's system. An interim plan required under this subsection will be superseded by a plan required under subsection (e).

(h) Tier assignment

Utilizing the risk assessment and National Strategy for Railroad Transportation Security required under section 1161 of this title, the Secretary shall assign each railroad carrier to a risk-based tier established by the Secretary:

(1) Provision of information

The Secretary may request, and a railroad carrier shall provide, information necessary for the Secretary to assign a railroad carrier to the appropriate tier under this subsection.

(2) Notification

Not later than 60 days after the date a railroad carrier is assigned to a tier under this subsection, the Secretary shall notify the railroad carrier of the tier to which it is assigned and the reasons for such assignment.

(3) High-risk tiers

At least one of the tiers established by the Secretary under this subsection shall be designated a tier for high-risk railroad carriers.

(4) Reassignment

The Secretary may reassign a railroad carrier to another tier, as appropriate, in response to changes in risk. The Secretary shall notify the railroad carrier not later than 60 days after such reassignment and provide the railroad carrier with the reasons for such reassignment.

(i) Nondisclosure of information

(1) Submission of information to Congress

Nothing in this section shall be construed as authorizing the withholding of any information from Congress.

(2) Disclosure of independently furnished information

Nothing in this section shall be construed as affecting any authority or obligation of a Federal agency to disclose any record or information that the Federal agency obtains from a railroad carrier under any other Federal law.

(j) Existing procedures, protocols and standards

(1) Determination

In response to a petition by a railroad carrier or at the discretion of the Secretary, the Secretary may determine that existing procedures, protocols, and standards meet all or part of the requirements of this section, including regulations issued under subsection (a), regarding vulnerability assessments and security plans.

(2) Election

Upon review and written determination by the Secretary that existing procedures, protocols, or standards of a railroad carrier satisfy the requirements of this section, the railroad carrier may elect to comply with those procedures, protocols, or standards instead of the requirements of this section.

(3) Partial approval

If the Secretary determines that the existing procedures, protocols, or standards of a railroad carrier satisfy only part of the requirements of this section, the Secretary may accept such submission, but shall require submission by the railroad carrier of any additional information

relevant to the vulnerability assessment and security plan of the railroad carrier to ensure that the remaining requirements of this section are fulfilled.

(4) Notification

If the Secretary determines that particular existing procedures, protocols, or standards of a railroad carrier under this subsection do not satisfy the requirements of this section, the Secretary shall provide to the railroad carrier a written notification that includes an explanation of the determination.

(5) Review

Nothing in this subsection shall relieve the Secretary of the obligation—

(A) to review the vulnerability assessment and security plan submitted by a railroad carrier under this section; and

(B) to approve or disapprove each submission on an individual basis.

(k) Periodic evaluation by railroad carriers required

(1) Submission of evaluation

Not later than 3 years after the date on which a vulnerability assessment or security plan required to be submitted to the Secretary under subsection (c) is approved, and at least once every 5 years thereafter (or on such a schedule as the Secretary may establish by regulation), a railroad carrier who submitted a vulnerability assessment and security plan and who is still assigned to the high-risk tier must also submit to the Secretary an evaluation of the adequacy of the vulnerability assessment and security plan that includes a description of any material changes made to the vulnerability assessment or security plan.

(2) Review of evaluation

Not later than 180 days after the date on which an evaluation is submitted, the Secretary shall review the evaluation and notify the railroad carrier submitting the evaluation of the Secretary's approval or disapproval of the evaluation.

(l) Shared facilities

The Secretary may permit under this section the development and implementation of coordinated vulnerability assessments and security plans to the extent that a railroad carrier shares facilities with, or is colocated with, other transportation entities or providers that are required to develop vulnerability assessments and security plans under Federal law.

(m) Consultation

In carrying out this section, the Secretary shall consult with railroad carriers, nonprofit employee labor organizations representation railroad employees, and public safety and law enforcement officials.

(Pub. L. 110–53, title XV, §1512, Aug. 3, 2007, 121 Stat. 429.)

[1] *So in original. The word "to" probably should not appear.*

§1163. Railroad security assistance

(a) Security improvement grants

(1) The Secretary, in consultation with the Administrator of the Transportation Security Administration and other appropriate agencies or officials, is authorized to make grants to railroad carriers, the Alaska Railroad, security-sensitive materials offerors who ship by railroad, owners of railroad cars used in the transportation of security-sensitive materials, State and local governments (for railroad passenger facilities and infrastructure not owned by Amtrak), and Amtrak for intercity passenger railroad and freight railroad security improvements described in subsection (b) as approved by the Secretary.

(2) A railroad carrier is eligible for a grant under this section if the carrier has completed a vulnerability assessment and developed a security plan that the Secretary has approved in accordance with section 1162 of this title.

(3) A recipient of a grant under this section may use grant funds only for permissible uses under subsection (b) to further a railroad security plan that meets the requirements of paragraph (2).

(4) Notwithstanding the requirement for eligibility and uses of funds in paragraphs (2) and (3), a railroad carrier is eligible for a grant under this section if the applicant uses the funds solely for the development of assessments or security plans under section 1162 of this title.

(5) Notwithstanding the requirements for eligibility and uses of funds in paragraphs (2) and (3), prior to the earlier of 1 year after the date of issuance of final regulations requiring vulnerability assessments and security plans under section 1162 of this title or 3 years after August 3, 2007, the Secretary may award grants under this section for rail security improvements listed under subsection (b) based upon railroad carrier vulnerability assessments and security plans that the Secretary determines are sufficient for the purposes of this section but have not been approved by the Secretary in accordance with section 1162 of this title.

(b) Uses of funds

A recipient of a grant under this section shall use the grant funds for one or more of the following:

(1) Security and redundancy for critical communications, computer, and train control systems essential for secure railroad operations, including communications interoperability where appropriate with relevant outside agencies and entities.

(2) Accommodation of railroad cargo or passenger security inspection facilities, related infrastructure, and operations at or near United States international borders or other ports of entry.

(3) The security of security-sensitive materials transportation by railroad.

(4) Chemical, biological, radiological, or explosive detection, including canine patrols for such detection.

(5) The security and preparedness of intercity passenger railroad stations, trains, and infrastructure, including security capital improvement projects that the Secretary determines enhance railroad station security.

(6) Technologies to reduce the vulnerabilities of railroad cars, including structural modification of railroad cars transporting security-sensitive materials to improve their resistance to acts of terrorism.

(7) The sharing of intelligence and information about security threats and preparedness, including connectivity to the National Terrorist Screening Center.

(8) To obtain train tracking and communications equipment, including equipment that is interoperable with Federal, State, and local agencies and tribal governments.

(9) To hire, train, and employ police, security, and preparedness officers, including canine units, assigned to full-time security or counterterrorism duties related to railroad transportation.

(10) Overtime reimbursement, including reimbursement of State, local, and tribal governments for costs, for enhanced security personnel assigned to duties related to railroad security during periods of high or severe threat levels and National Special Security Events or other periods of heightened security as determined by the Secretary.

(11) Perimeter protection systems, including access control, installation of improved lighting, fencing, and barricades at railroad facilities.

(12) Tunnel protection systems.

(13) Passenger evacuation and evacuation-related capital improvements.

(14) Railroad security inspection technologies, including verified visual inspection technologies using hand-held readers.

(15) Surveillance equipment.

(16) Cargo or passenger screening equipment.

(17) Emergency response equipment, including fire suppression and decontamination equipment, personal protective equipment, and defibrillators.

(18) Operating and capital costs associated with security awareness, preparedness, and response training, including training under section 1167 of this title, and training developed by universities,

institutions of higher education, and nonprofit employee labor organizations, for railroad employees, including frontline employees.

(19) Live or simulated exercises, including exercises described in section 1166 of this title.

(20) Public awareness campaigns for enhanced railroad security.

(21) Development of assessments or security plans under section 1162 of this title.

(22) Other security improvements—

(A) identified, required, or recommended under sections 1161 and 1162 of this title, including infrastructure, facilities, and equipment upgrades; or

(B) that the Secretary considers appropriate.

(c) Department of Homeland Security responsibilities

In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants;

(2) establish priorities for uses of funds for grant recipients;

(3) award the funds authorized by this section based on risk, as identified by the plans required under sections 1161 and 1162 of this title, or assessment or plan described in subsection (a)(5);

(4) take into account whether stations or facilities are used by commuter railroad passengers as well as intercity railroad passengers in reviewing grant applications;

(5) encourage non-Federal financial participation in projects funded by grants; and

(6) not later than 5 business days after awarding a grant to Amtrak under this section, transfer grant funds to the Secretary of Transportation to be disbursed to Amtrak.

(d) Multiyear awards

Grant funds awarded under this section may be awarded for projects that span multiple years.

(e) Limitation on uses of funds

A grant made under this section may not be used to make any State or local government cost-sharing contribution under any other Federal law.

(f) Annual reports

Each recipient of a grant under this section shall report annually to the Secretary on the use of grant funds.

(g) Non-Federal match study

Not later than 240 days after August 3, 2007, the Secretary shall provide a report to the appropriate congressional committees on the feasibility and appropriateness of requiring a non-Federal match for grants awarded to freight railroad carriers and other private entities under this section.

(h) Subject to certain standards

A recipient of a grant under this section and sections 1164 and 1165 of this title shall be required to comply with the standards of section 24312 of title 49, as in effect on January 1, 2007, with respect to the project in the same manner as Amtrak is required to comply with such standards for construction work financed under an agreement made under section 24308(a) of that title.

(i) Authorization of appropriations

(1) In general

Out of funds appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section—

(A) $300,000,000 for fiscal year 2008;

(B) $300,000,000 for fiscal year 2009;

(C) $300,000,000 for fiscal year 2010; and

(D) $300,000,000 for fiscal year 2011.

(2) Period of availability

Sums appropriated to carry out this section shall remain available until expended.

(Pub. L. 110–53, title XV, §1513, Aug. 3, 2007, 121 Stat. 433; Pub. L. 115–254, div. K, title I, §1973(a), Oct. 5, 2018, 132 Stat. 3614.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (i)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

AMENDMENTS

2018—Subsec. (b)(1). Pub. L. 115–254, §1973(a)(1), substituted ", including communications interoperability where appropriate with relevant outside agencies and entities." for period at end.

Subsec. (b)(5). Pub. L. 115–254, §1973(a)(2), substituted "security and preparedness of" for "security of".

Subsec. (b)(7). Pub. L. 115–254, §1973(a)(3), substituted "security threats and preparedness, including connectivity to the National Terrorist Screening Center" for "security threats".

Subsec. (b)(9). Pub. L. 115–254, §1973(a)(4), substituted ", security, and preparedness officers" for "and security officers".

[1] *See References in Text note below.*

§1164. Systemwide Amtrak security upgrades

(a) In general

(1) Grants

Subject to subsection (b), the Secretary, in consultation with the Administrator of the Transportation Security Administration, is authorized to make grants to Amtrak in accordance with the provisions of this section.

(2) General purposes

The Secretary may make such grants for the purposes of—

(A) protecting underwater and underground assets and systems;

(B) protecting high-risk and high-consequence assets identified through systemwide risk assessments;

(C) providing counterterrorism or security training;

(D) providing both visible and unpredictable deterrence; and

(E) conducting emergency preparedness drills and exercises.

(3) Specific projects

The Secretary shall make such grants—

(A) to secure major tunnel access points and ensure tunnel integrity in New York, New Jersey, Maryland, and Washington, DC;

(B) to secure Amtrak trains;

(C) to secure Amtrak stations;

(D) to obtain a watchlist identification system approved by the Secretary, or to connect to the National Terrorism Screening Center watchlist;

(E) to obtain train tracking and interoperable communications systems that are coordinated with Federal, State, and local agencies and tribal governments to the maximum extent possible;

(F) to hire, train, and employ police and security officers, including canine units, assigned to full-time security or counterterrorism duties related to railroad transportation;

(G) for operating and capital costs associated with security awareness, preparedness, and response training, including training under section 1167 of this title, and training developed by universities, institutions of higher education, and nonprofit employee labor organizations, for railroad employees, including frontline employees;

(H) for live or simulated exercises, including exercises described in section 1166 of this title;

(I) for improvements to passenger verification systems;

(J) for improvements to employee and contractor verification systems, including identity verification technology; or

(K) for improvements to the security of Amtrak computer systems, including cybersecurity assessments and programs.

(b) Conditions

The Secretary shall award grants to Amtrak under this section for projects contained in a systemwide security plan approved by the Secretary developed pursuant to section 1162 of this title. Not later than 5 business days after awarding a grant to Amtrak under this section, the Secretary shall transfer the grant funds to the Secretary of Transportation to be disbursed to Amtrak.

(c) Equitable geographic allocation

The Secretary shall ensure that, subject to meeting the highest security needs on Amtrak's entire system and consistent with the risk assessment required under section 1161 of this title and Amtrak's vulnerability assessment and security plan developed under section 1162 of this title, stations and facilities located outside of the Northeast Corridor receive an equitable share of the security funds authorized by this section.

(d) Availability of funds

(1) In general

Out of funds appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary and the Administrator of the Transportation Security Administration to carry out this section—

(A) $150,000,000 for fiscal year 2008;

(B) $150,000,000 for fiscal year 2009;

(C) $175,000,000 for fiscal year 2010; and

(D) $175,000,000 for fiscal year 2011.

(2) Availability of appropriated funds

Amounts appropriated pursuant to paragraph (1) shall remain available until expended.

(Pub. L. 110–53, title XV, §1514, Aug. 3, 2007, 121 Stat. 435; Pub. L. 115–254, div. K, title I, §1973(b), Oct. 5, 2018, 132 Stat. 3614.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (d)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

AMENDMENTS

2018—Subsec. (a)(3)(D). Pub. L. 115–254, §1973(b)(1), inserted ", or to connect to the National Terrorism Screening Center watchlist" after "Secretary".

Subsec. (a)(3)(I) to (K). Pub. L. 115–254, §1973(b)(2)–(4), added subpars. (I) to (K).

STATUTORY NOTES AND RELATED SUBSIDIARIES

PASSENGER RAIL VETTING

Pub. L. 115–254, div. K, title I, §1974, Oct. 5, 2018, 132 Stat. 3615, provided that:

"(a) IN GENERAL.—Not later than 180 days after the date on which the Amtrak Board of Directors submits a request to the Administrator [of the Transportation Security Administration], the Administrator shall issue a decision on the use by Amtrak of the Transportation Security Administration's Secure Flight Program or a similar passenger vetting system to enhance passenger rail security.

"(b) CONSIDERATIONS.—In making a decision under subsection (a), the Administrator shall—

"(1) consider the technological, privacy, operational, and security impacts of such a decision; and

"(2) describe such impacts in any strategic plan developed under subsection (c).

"(c) STRATEGIC PLAN.—If the Administrator decides to grant the request by Amtrak under subsection (a), the decision shall include a strategic plan for working with rail stakeholders to enhance passenger rail security by—

"(1) vetting passengers using terrorist watch lists maintained by the Federal Government or a similar passenger vetting system maintained by the Transportation Security Administration; and

"(2) where applicable and in consultation with the Commissioner of U.S. Customs and Border Protection, assessing whether the vetting process should be integrated into preclearance operations established under section 813 of the Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4432).

"(d) NOTICES.—The Administrator shall notify the appropriate committees of Congress [Committees on Commerce, Science and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] of any decision made under subsection (a) and the details of the strategic plan under subsection (c).

"(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit the Administrator's authority to set the access to, or terms and conditions of using, the Secure Flight Program or a similar passenger vetting system."

[1] *See References in Text note below.*

§1165. Fire and life safety improvements

(a) Life-safety needs

There are authorized to be appropriated to the Secretary of Transportation for making grants to Amtrak for the purpose of carrying out projects to make fire and life safety improvements to Amtrak tunnels on the Northeast Corridor the following amounts:

(1) For the 6 New York and New Jersey tunnels to provide ventilation, electrical, and fire safety technology improvements, emergency communication and lighting systems, and emergency access and egress for passengers—

(A) $25,000,000 for fiscal year 2008;
(B) $30,000,000 for fiscal year 2009;
(C) $45,000,000 for fiscal year 2010; and
(D) $60,000,000 for fiscal year 2011.

(2) For the Baltimore Potomac Tunnel and the Union Tunnel, together, to provide adequate drainage and ventilation, communication, lighting, standpipe, and passenger egress improvements—

(A) $5,000,000 for fiscal year 2008;
(B) $5,000,000 for fiscal year 2009;
(C) $5,000,000 for fiscal year 2010; and
(D) $5,000,000 for fiscal year 2011.

(3) For the Union Station tunnels in the District of Columbia to improve ventilation, communication, lighting, and passenger egress improvements—

(A) $5,000,000 for fiscal year 2008;
(B) $5,000,000 for fiscal year 2009;
(C) $5,000,000 for fiscal year 2010; and
(D) $5,000,000 for fiscal year 2011.

(b) Infrastructure upgrades

Out of funds appropriated pursuant to section 1153 of this title, there shall be made available to the Secretary of Transportation for fiscal year 2008, $3,000,000 for the preliminary design of options for a new tunnel on a different alignment to augment the capacity of the existing Baltimore tunnels.

(c) Availability of amounts

Amounts appropriated pursuant to this section shall remain available until expended.

(d) Plans required

The Secretary of Transportation may not make amounts available to Amtrak for obligation or expenditure under subsection (a)—

(1) until Amtrak has submitted to the Secretary of Transportation, and the Secretary of Transportation has approved, an engineering and financial plan for such projects; and

(2) unless, for each project funded pursuant to this section, the Secretary of Transportation has approved a project management plan prepared by Amtrak.

(e) Review of plans

(1) In general

The Secretary of Transportation shall complete the review of a plan required under subsection (d) and approve or disapprove the plan within 45 days after the date on which each such plan is submitted by Amtrak.

(2) Incomplete or deficient plan

If the Secretary of Transportation determines that a plan is incomplete or deficient, the Secretary of Transportation shall notify Amtrak of the incomplete items or deficiencies and Amtrak shall, within 30 days after receiving the Secretary of Transportation's notification, submit a modified plan for the Secretary of Transportation's review.

(3) Approval of plan

Within 15 days after receiving additional information on items previously included in the plan, and within 45 days after receiving items newly included in a modified plan, the Secretary of Transportation shall either approve the modified plan, or if the Secretary of Transportation finds the plan is still incomplete or deficient, the Secretary of Transportation shall—

(A) identify in writing to the appropriate congressional committees the portions of the plan the Secretary finds incomplete or deficient;

(B) approve all other portions of the plan;

(C) obligate the funds associated with those portions; and

(D) execute an agreement with Amtrak within 15 days thereafter on a process for resolving the remaining portions of the plan.

(f) Financial contribution from other tunnel users

The Secretary of Transportation, taking into account the need for the timely completion of all portions of the tunnel projects described in subsection (a), shall—

(1) consider the extent to which railroad carriers other than Amtrak use or plan to use the tunnels;

(2) consider the feasibility of seeking a financial contribution from those other railroad carriers toward the costs of the projects; and

(3) obtain financial contributions or commitments from such other railroad carriers at levels reflecting the extent of their use or planned use of the tunnels, if feasible.

(Pub. L. 110–53, title XV, §1515, Aug. 3, 2007, 121 Stat. 437.)

§1166. Railroad carrier exercises

(a) In general

The Secretary shall establish a program for conducting security exercises for railroad carriers for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate, respond to, and recover from acts of terrorism.

(b) Covered entities

Entities to be assessed under the program shall include—

(1) Federal, State, and local agencies and tribal governments;

(2) railroad carriers;

(3) governmental and nongovernmental emergency response providers, law enforcement agencies, and railroad and transit police, as appropriate; and

(4) any other organization or entity that the Secretary determines appropriate.

(c) Requirements

The Secretary shall ensure that the program—

(1) consolidates existing security exercises for railroad carriers administered by the Department and the Department of Transportation, as jointly determined by the Secretary and the Secretary of Transportation, unless the Secretary waives this consolidation requirement as appropriate;

(2) consists of exercises that are—

(A) scaled and tailored to the needs of the carrier, including addressing the needs of the elderly and individuals with disabilities;

(B) live, in the case of the most at-risk facilities to a terrorist attack;

(C) coordinated with appropriate officials;

(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(E) inclusive, as appropriate, of railroad frontline employees; and

(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(3) provides that exercises described in paragraph (2) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to identify best practices, which shall be shared, as appropriate, with railroad carriers, nonprofit employee organizations that represent railroad carrier employees, Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, law enforcement personnel, including railroad carrier and transit police, and other stakeholders; and

(C) used to develop recommendations, as appropriate, from the Secretary to railroad carriers on remedial action to be taken in response to lessons learned;

(4) allows for proper advanced notification of communities and local governments in which exercises are held, as appropriate; and

(5) assists State, local, and tribal governments and railroad carriers in designing, implementing, and evaluating additional exercises that conform to the requirements of paragraph (1) [1].

(d) National Exercise Program

The Secretary shall ensure that the exercise program developed under subsection (c) is a component of the National Exercise Program established under section 748 of this title.

(Pub. L. 110–53, title XV, §1516, Aug. 3, 2007, 121 Stat. 438.)

[1] *So in original. Probably should be "(2)".*

§1167. Railroad security training program

(a) In general

Not later than 6 months after August 3, 2007, the Secretary shall develop and issue regulations for a training program to prepare railroad frontline employees for potential security threats and conditions. The regulations shall take into consideration any current security training requirements or

best practices.

(b) Consultation

The Secretary shall develop the regulations under subsection (a) in consultation with—

(1) appropriate law enforcement, fire service, emergency response, security, and terrorism experts;

(2) railroad carriers;

(3) railroad shippers; and

(4) nonprofit employee labor organizations representing railroad employees or emergency response personnel.

(c) Program elements

The regulations developed under subsection (a) shall require security training programs described in subsection (a) to include, at a minimum, elements to address the following, as applicable:

(1) Determination of the seriousness of any occurrence or threat.

(2) Crew and passenger communication and coordination.

(3) Appropriate responses to defend or protect oneself.

(4) Use of personal and other protective equipment.

(5) Evacuation procedures for passengers and railroad employees, including individuals with disabilities and the elderly.

(6) Psychology, behavior, and methods of terrorists, including observation and analysis.

(7) Training related to psychological responses to terrorist incidents, including the ability to cope with hijacker behavior and passenger responses.

(8) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(9) Recognition and reporting of dangerous substances, suspicious packages, and situations.

(10) Understanding security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers and for on-scene interaction with such emergency response providers.

(11) Operation and maintenance of security equipment and systems.

(12) Other security training activities that the Secretary considers appropriate.

(d) Required programs

(1) Development and submission to Secretary

Not later than 90 days after the Secretary issues regulations under subsection (a), each railroad carrier shall develop a security training program in accordance with this section and submit the program to the Secretary for approval.

(2) Approval or disapproval

Not later than 60 days after receiving a security training program proposal under this subsection, the Secretary shall approve the program or require the railroad carrier that developed the program to make any revisions to the program that the Secretary considers necessary for the program to meet the requirements of this section. A railroad carrier shall respond to the Secretary's comments within 30 days after receiving them.

(3) Training

Not later than 1 year after the Secretary approves a security training program in accordance with this subsection, the railroad carrier that developed the program shall complete the training of all railroad frontline employees who were hired by a carrier more than 30 days preceding such date. For such employees employed less than 30 days by a carrier preceding such date, training shall be completed within the first 60 days of employment.

(4) Updates of regulations and program revisions

The Secretary shall periodically review and update as appropriate the training regulations issued under subsection (a) to reflect new or changing security threats. Each railroad carrier shall revise

its training program accordingly and provide additional training as necessary to its frontline employees within a reasonable time after the regulations are updated.

(e) National Training Program

The Secretary shall ensure that the training program developed under subsection (a) is a component of the National Training Program established under section 748 of this title.

(f) Reporting requirements

Not later than 2 years after the date of regulation issuance, the Secretary shall review implementation of the training program of a representative sample of railroad carriers and railroad frontline employees, and report to the appropriate congressional committees on the number of reviews conducted and the results of such reviews. The Secretary may submit the report in both classified and redacted formats as necessary.

(g) Other employees

The Secretary shall issue guidance and best practices for a railroad shipper employee security program containing the elements listed under subsection (c).

(Pub. L. 110–53, title XV, §1517, Aug. 3, 2007, 121 Stat. 439.)

§1168. Railroad security research and development

(a) Establishment of research and development program

The Secretary, acting through the Under Secretary for Science and Technology and the Administrator of the Transportation Security Administration, shall carry out a research and development program for the purpose of improving the security of railroad transportation systems.

(b) Eligible projects

The research and development program may include projects—

(1) to reduce the vulnerability of passenger trains, stations, and equipment to explosives and hazardous chemical, biological, and radioactive substances, including the development of technology to screen passengers in large numbers at peak commuting times with minimal interference and disruption;

(2) to test new emergency response and recovery techniques and technologies, including those used at international borders;

(3) to develop improved railroad security technologies, including—

(A) technologies for sealing or modifying railroad tank cars;

(B) automatic inspection of railroad cars;

(C) communication-based train control systems;

(D) emergency response training, including training in a tunnel environment;

(E) security and redundancy for critical communications, electrical power, computer, and train control systems; and

(F) technologies for securing bridges and tunnels;

(4) to test wayside detectors that can detect tampering;

(5) to support enhanced security for the transportation of security-sensitive materials by railroad;

(6) to mitigate damages in the event of a cyber attack; and

(7) to address other vulnerabilities and risks identified by the Secretary.

(c) Coordination with other research initiatives

The Secretary—

(1) shall ensure that the research and development program is consistent with the National Strategy for Railroad Transportation Security developed under section 1161 of this title and any other transportation security research and development programs required by this Act;

(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

(A) the Department of Transportation, including University Transportation Centers and other institutes, centers, and simulators funded by the Department of Transportation;

(B) the National Academy of Sciences;

(C) the Technical Support Working Group;

(D) other Federal departments and agencies; and

(E) other Federal and private research laboratories, research entities, and universities and institutions of higher education, including Historically Black Colleges and Universities, Hispanic Serving Institutions, or Indian Tribally Controlled Colleges and Universities;

(3) shall carry out any research and development project authorized by this section through a reimbursable agreement with an appropriate Federal agency, if the agency—

(A) is currently sponsoring a research and development project in a similar area; or

(B) has a unique facility or capability that would be useful in carrying out the project;

(4) may award grants, or enter into cooperative agreements, contracts, other transactions, or reimbursable agreements to the entities described in paragraph (2) and the eligible grant recipients under section 1163 of this title; and

(5) shall make reasonable efforts to enter into memoranda of understanding, contracts, grants, cooperative agreements, or other transactions with railroad carriers willing to contribute both physical space and other resources.

(d) Privacy and civil rights and civil liberties issues

(1) Consultation

In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department as appropriate and in accordance with section 142 of this title.

(2) Privacy impact assessments

In accordance with sections 142 and 345 of this title, the Chief Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed under this section that the Secretary determines could have an impact on privacy, civil rights, or civil liberties.

(e) Authorization of appropriations

(1) In general

Out of funds appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section—

(A) $33,000,000 for fiscal year 2008;

(B) $33,000,000 for fiscal year 2009;

(C) $33,000,000 for fiscal year 2010; and

(D) $33,000,000 for fiscal year 2011.

(2) Period of availability

Such sums shall remain available until expended.

(Pub. L. 110–53, title XV, §1518, Aug. 3, 2007, 121 Stat. 441.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (c)(1), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266, known as the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted this chapter and

enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

Section 114(w) of title 49, referred to in subsec. (e)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1169. Railroad tank car security testing

(a) Railroad tank car vulnerability assessment

(1) Assessment

The Secretary shall assess the likely methods of a deliberate terrorist attack against a railroad tank car used to transport toxic-inhalation-hazard materials, and for each method assessed, the degree to which it may be successful in causing death, injury, or serious adverse effects to human health, the environment, critical infrastructure, national security, the national economy, or public welfare.

(2) Threats

In carrying out paragraph (1), the Secretary shall consider the most current threat information as to likely methods of a successful terrorist attack on a railroad tank car transporting toxic-inhalation-hazard materials, and may consider the following:

(A) Explosive devices placed along the tracks or attached to a railroad tank car.

(B) The use of missiles, grenades, rockets, mortars, or other high-caliber weapons against a railroad tank car.

(3) Physical testing

In developing the assessment required under paragraph (1), the Secretary shall conduct physical testing of the vulnerability of railroad tank cars used to transport toxic-inhalation-hazard materials to different methods of a deliberate attack, using technical information and criteria to evaluate the structural integrity of railroad tank cars.

(4) Report

Not later than 30 days after the completion of the assessment under paragraph (1), the Secretary shall provide to the appropriate congressional committees a report, in the appropriate format, on such assessment.

(b) Railroad tank car dispersion modeling

(1) In general

The Secretary, acting through the National Infrastructure Simulation and Analysis Center, shall conduct an air dispersion modeling analysis of release scenarios of toxic-inhalation-hazard materials resulting from a terrorist attack on a loaded railroad tank car carrying such materials in urban and rural environments.

(2) Considerations

The analysis under this subsection shall take into account the following considerations:

(A) The most likely means of attack and the resulting dispersal rate.

(B) Different times of day, to account for differences in cloud coverage and other atmospheric conditions in the environment being modeled.

(C) Differences in population size and density.

(D) Historically accurate wind speeds, temperatures, and wind directions.

(E) Differences in dispersal rates or other relevant factors related to whether a railroad tank car is in motion or stationary.

(F) Emergency response procedures by local officials.

(G) Any other considerations the Secretary believes would develop an accurate, plausible dispersion model for toxic-inhalation-hazard materials released from a railroad tank car as a result of a terrorist act.

(3) Consultation

In conducting the dispersion modeling under paragraph (1), the Secretary shall consult with the Secretary of Transportation, hazardous materials experts, railroad carriers, nonprofit employee labor organizations representing railroad employees, appropriate State, local, and tribal officials, and other Federal agencies, as appropriate.

(4) Information sharing

Upon completion of the analysis required under paragraph (1), the Secretary shall share the information developed with the appropriate stakeholders, given appropriate information protection provisions as may be required by the Secretary.

(5) Report

Not later than 30 days after completion of all dispersion analyses under paragraph (1), the Secretary shall submit to the appropriate congressional committees a report detailing the Secretary's conclusions and findings in an appropriate format.

(Pub. L. 110–53, title XV, §1519, Aug. 3, 2007, 121 Stat. 443.)

§1170. Security background checks of covered individuals

(a) Definitions

In this section, the following definitions apply:

(1) Security background check

The term "security background check" means reviewing, for the purpose of identifying individuals who may pose a threat to transportation security or national security, or of terrorism—

(A) relevant criminal history databases;

(B) in the case of an alien (as defined in the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)),[1] the relevant databases to determine the status of the alien under the immigration laws of the United States; and

(C) other relevant information or databases, as determined by the Secretary.

(2) Covered individual

The term "covered individual" means an employee of a railroad carrier or a contractor or subcontractor of a railroad carrier.

(b) Guidance

(1) Any guidance, recommendations, suggested action items, or any other widely disseminated voluntary action items issued by the Secretary to a railroad carrier or a contractor or subcontractor of a railroad carrier relating to performing a security background check of a covered individual shall contain recommendations on the appropriate scope and application of such a security background check, including the time period covered, the types of disqualifying offenses, and a redress process for adversely impacted covered individuals consistent with subsections (c) and (d) of this section.

(2) Within 60 days after August 3, 2007, any guidance, recommendations, suggested action items, or any other widely disseminated voluntary action item issued by the Secretary prior to August 3, 2007, to a railroad carrier or a contractor or subcontractor of a railroad carrier relating to performing a security background check of a covered individual shall be updated in compliance with paragraph (1).

(3) If a railroad carrier or a contractor or subcontractor of a railroad carrier performs a security background check on a covered individual to fulfill guidance issued by the Secretary under paragraph (1) or (2), the Secretary shall not consider such guidance fulfilled unless an adequate

redress process as described in subsection (d) is provided to covered individuals.

(c) Requirements

If the Secretary issues a rule, regulation, or directive requiring a railroad carrier or contractor or subcontractor of a railroad carrier to perform a security background check of a covered individual, then the Secretary shall prohibit the railroad carrier or contractor or subcontractor of a railroad carrier from making an adverse employment decision, including removal or suspension of the covered individual, due to such rule, regulation, or directive with respect to a covered individual unless the railroad carrier or contractor or subcontractor of a railroad carrier determines that the covered individual—

(1) has been convicted of, has been found not guilty by reason of insanity, or is under want, warrant, or indictment for a permanent disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations;

(2) was convicted of or found not guilty by reason of insanity of an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, within 7 years of the date that the railroad carrier or contractor or subcontractor of a railroad carrier performs the security background check; or

(3) was incarcerated for an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, and released from incarceration within 5 years of the date that the railroad carrier or contractor or subcontractor of a railroad carrier performs the security background check.

(d) Redress process

If the Secretary issues a rule, regulation, or directive requiring a railroad carrier or contractor or subcontractor of a railroad carrier to perform a security background check of a covered individual, the Secretary shall—

(1) provide an adequate redress process for a covered individual subjected to an adverse employment decision, including removal or suspension of the employee, due to such rule, regulation, or directive that is consistent with the appeals and waiver process established for applicants for commercial motor vehicle hazardous materials endorsements and transportation employees at ports, as required by section 70105(c) of title 46; and

(2) have the authority to order an appropriate remedy, including reinstatement of the covered individual, should the Secretary determine that a railroad carrier or contractor or subcontractor of a railroad carrier wrongfully made an adverse employment decision regarding a covered individual pursuant to such rule, regulation, or directive.

(e) False statements

A railroad carrier or a contractor or subcontractor of a railroad carrier may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary related to security background check requirements for covered individuals when conducting a security background check. Not later than 1 year after August 3, 2007, the Secretary shall issue a regulation that prohibits a railroad carrier or a contractor or subcontractor of a railroad carrier from knowingly misrepresenting to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary related to security background check requirements for covered individuals when conducting a security background check.

(f) Rights and responsibilities

Nothing in this section shall be construed to abridge a railroad carrier's or a contractor or subcontractor of a railroad carrier's rights or responsibilities to make adverse employment decisions permitted by other Federal, State, or local laws. Nothing in the section shall be construed to abridge rights and responsibilities of covered individuals, a railroad carrier, or a contractor or subcontractor of a railroad carrier, under any other Federal, State, or local laws or under any collective bargaining agreement.

(g) No preemption of Federal or State law

Nothing in this section shall be construed to preempt a Federal, State, or local law that requires criminal history background checks, immigration status checks, or other background checks, of covered individuals.

(h) Statutory construction

Nothing in this section shall be construed to affect the process for review established under section 70105(c) of title 46, including regulations issued pursuant to such section.

(Pub. L. 110–53, title XV, §1522, Aug. 3, 2007, 121 Stat. 448.)

EDITORIAL NOTES

REFERENCES IN TEXT

The Immigration and Nationality Act, referred to in subsec. (a)(1)(B), is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 et seq.) of Title 8, Aliens and Nationality. The term "alien" is defined in section 101(a)(3) of the Act which is classified to section 1101(a)(3) of Title 8. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

[1] *So in original. Another closing parenthesis probably should precede the comma.*

§1171. International railroad security program

(a) In general

(1) The Secretary shall develop a system to detect both undeclared passengers and contraband, with a primary focus on the detection of nuclear and radiological materials entering the United States by railroad.

(2) SYSTEM REQUIREMENTS.—In developing the system under paragraph (1), the Secretary may, in consultation with the Domestic Nuclear Detection Office,[1] Customs and Border Protection, and the Transportation Security Administration—

(A) deploy radiation detection equipment and nonintrusive imaging equipment at locations where railroad shipments cross an international border to enter the United States;

(B) consider the integration of radiation detection technologies with other nonintrusive inspection technologies where feasible;

(C) ensure appropriate training, operations, and response protocols are established for Federal, State, and local personnel;

(D) implement alternative procedures to check railroad shipments at locations where the deployment of nonintrusive inspection imaging equipment is determined to not be practicable;

(E) ensure, to the extent practicable, that such technologies deployed can detect terrorists or weapons, including weapons of mass destruction; and

(F) take other actions, as appropriate, to develop the system.

(b) Additional information

The Secretary shall—

(1) identify and seek the submission of additional data elements for improved high-risk targeting related to the movement of cargo through the international supply chain utilizing a railroad prior to importation into the United States;

(2) utilize data collected and maintained by the Secretary of Transportation in the targeting of high-risk cargo identified under paragraph (1); and

(3) analyze the data provided in this subsection to identify high-risk cargo for inspection.

(c) Report to Congress

Not later than September 30, 2008, the Secretary shall transmit to the appropriate congressional

committees a report that describes the progress of the system being developed under subsection (a).

(d) Definitions

In this section:

(1) International supply chain

The term "international supply chain" means the end-to-end process for shipping goods to or from the United States, beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination.

(2) Radiation detection equipment

The term "radiation detection equipment" means any technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

(3) Inspection

The term "inspection" means the comprehensive process used by Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws.

(Pub. L. 110–53, title XV, §1524, Aug. 3, 2007, 121 Stat. 451.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Domestic Nuclear Detection Office deemed to be a reference to the Countering Weapons of Mass Destruction Office, see section 2(b)(1)(A) of Pub. L. 115–387, set out as a note under section 591 of this title.

[1] *See Change of Name note below.*

§1172. Railroad security enhancements; Model State legislation

Not later than November 2, 2007, the Secretary of Transportation shall develop and make available to States model legislation to address the problem of entities that claim to be railroad carriers in order to establish and run a police force when the entities do not in fact provide railroad transportation. In developing the model State legislation the Secretary shall solicit the input of the States, railroads carriers, and railroad carrier employees. The Secretary shall review and, if necessary, revise such model State legislation periodically.

(Pub. L. 110–53, title XV, §1526(b), Aug. 3, 2007, 121 Stat. 452.)

PART C—OVER-THE-ROAD BUS AND TRUCKING SECURITY

§1181. Over-the-road bus security assessments and plans

(a) In general

Not later than 18 months after August 3, 2007, the Secretary shall issue regulations that—

(1) require each over-the-road bus operator assigned to a high-risk tier under this section—

(A) to conduct a vulnerability assessment in accordance with subsections (c) and (d); and

(B) to prepare, submit to the Secretary for approval, and implement a security plan in accordance with subsection (e); and

(2) establish standards and guidelines for developing and implementing the vulnerability

assessments and security plans for carriers assigned to high-risk tiers consistent with this section.

(b) Non high-risk programs

The Secretary may establish a security program for over-the-road bus operators not assigned to a high-risk tier, including—

(1) guidance for such operators in conducting vulnerability assessments and preparing and implementing security plans, as determined appropriate by the Secretary; and

(2) a process to review and approve such assessments and plans, as appropriate.

(c) Deadline for submission

Not later than 9 months after the date of issuance of the regulations under subsection (a), the vulnerability assessments and security plans required by such regulations for over-the-road bus operators assigned to a high-risk tier shall be completed and submitted to the Secretary for review and approval.

(d) Vulnerability assessments

(1) Requirements

The Secretary shall provide technical assistance and guidance to over-the-road bus operators in conducting vulnerability assessments under this section and shall require that each vulnerability assessment of an operator assigned to a high-risk tier under this section includes, as appropriate—

(A) identification and evaluation of critical assets and infrastructure, including platforms, stations, terminals, and information systems;

(B) identification of the vulnerabilities to those assets and infrastructure; and

(C) identification of weaknesses in—

(i) physical security;

(ii) passenger and cargo security;

(iii) the security of programmable electronic devices, computers, or other automated systems which are used in providing over-the-road bus transportation;

(iv) alarms, cameras, and other protection systems;

(v) communications systems and utilities needed for over-the-road bus security purposes, including dispatching systems;

(vi) emergency response planning;

(vii) employee training; and

(viii) such other matters as the Secretary determines appropriate.

(2) Threat information

The Secretary shall provide in a timely manner to the appropriate employees of an over-the-road bus operator, as designated by the over-the-road bus operator, threat information that is relevant to the operator when preparing and submitting a vulnerability assessment and security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in over-the-road bus security.

(e) Security plans

(1) Requirements

The Secretary shall provide technical assistance and guidance to over-the-road bus operators in preparing and implementing security plans under this section and shall require that each security plan of an over-the-road bus operator assigned to a high-risk tier under this section includes, as appropriate—

(A) the identification of a security coordinator having authority—

(i) to implement security actions under the plan;

(ii) to coordinate security improvements; and

(iii) to receive communications from appropriate Federal officials regarding over-the-road bus security;

(B) a list of needed capital and operational improvements;

(C) procedures to be implemented or used by the over-the-road bus operator in response to a terrorist attack, including evacuation and passenger communication plans that include individuals with disabilities, as appropriate;

(D) the identification of steps taken with State and local law enforcement agencies, emergency responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

(E) a strategy and timeline for conducting training under section 1184 of this title;

(F) enhanced security measures to be taken by the over-the-road bus operator when the Secretary declares a period of heightened security risk;

(G) plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the over-the-road bus operator's system in the event of a terrorist attack or other incident; and

(H) such other actions or procedures as the Secretary determines are appropriate to address the security of over-the-road bus operators.

(2) Security coordinator requirements

The Secretary shall require that the individual serving as the security coordinator identified in paragraph (1)(A) is a citizen of the United States. The Secretary may waive this requirement with respect to an individual if the Secretary determines that it is appropriate to do so based on a background check of the individual and a review of the consolidated terrorist watchlist.

(f) Deadline for review process

Not later than 6 months after receiving the assessments and plans required under this section, the Secretary shall—

(1) review each vulnerability assessment and security plan submitted to the Secretary in accordance with subsection (c);

(2) require amendments to any security plan that does not meet the requirements of this section; and

(3) approve any vulnerability assessment or security plan that meets the requirements of this section.

(g) Interim security measures

The Secretary may require over-the-road bus operators, during the period before the deadline established under subsection (c), to submit a security plan to implement any necessary interim security measures essential to providing adequate security of the over-the-road bus operator's system. An interim plan required under this subsection shall be superseded by a plan required under subsection (c).

(h) Tier assignment

The Secretary shall assign each over-the-road bus operator to a risk-based tier established by the Secretary:

(1) Provision of information

The Secretary may request, and an over-the-road bus operator shall provide, information necessary for the Secretary to assign an over-the-road bus operator to the appropriate tier under this subsection.

(2) Notification

Not later than 60 days after the date an over-the-road bus operator is assigned to a tier under this section, the Secretary shall notify the operator of the tier to which it is assigned and the reasons for such assignment.

(3) High-risk tiers

At least one of the tiers established by the Secretary under this section shall be a tier designated for high-risk over-the-road bus operators.

(4) Reassignment

The Secretary may reassign an over-the-road bus operator to another tier, as appropriate, in response to changes in risk and the Secretary shall notify the over-the-road bus operator within 60 days after such reassignment and provide the operator with the reasons for such reassignment.

(i) Existing procedures, protocols, and standards

(1) Determination

In response to a petition by an over-the-road bus operator or at the discretion of the Secretary, the Secretary may determine that existing procedures, protocols, and standards meet all or part of the requirements of this section regarding vulnerability assessments and security plans.

(2) Election

Upon review and written determination by the Secretary that existing procedures, protocols, or standards of an over-the-road bus operator satisfy the requirements of this section, the over-the-road bus operator may elect to comply with those procedures, protocols, or standards instead of the requirements of this section.

(3) Partial approval

If the Secretary determines that the existing procedures, protocols, or standards of an over-the-road bus operator satisfy only part of the requirements of this section, the Secretary may accept such submission, but shall require submission by the operator of any additional information relevant to the vulnerability assessment and security plan of the operator to ensure that the remaining requirements of this section are fulfilled.

(4) Notification

If the Secretary determines that particular existing procedures, protocols, or standards of an over-the-road bus operator under this subsection do not satisfy the requirements of this section, the Secretary shall provide to the operator a written notification that includes an explanation of the reasons for nonacceptance.

(5) Review

Nothing in this subsection shall relieve the Secretary of the obligation—

(A) to review the vulnerability assessment and security plan submitted by an over-the-road bus operator under this section; and

(B) to approve or disapprove each submission on an individual basis.

(j) Periodic evaluation by over-the-road bus provider required

(1) Submission of evaluation

Not later than 3 years after the date on which a vulnerability assessment or security plan required to be submitted to the Secretary under subsection (c) is approved, and at least once every 5 years thereafter (or on such a schedule as the Secretary may establish by regulation), an over-the-road bus operator who submitted a vulnerability assessment and security plan and who is still assigned to the high-risk tier shall also submit to the Secretary an evaluation of the adequacy of the vulnerability assessment and security plan that includes a description of any material changes made to the vulnerability assessment or security plan.

(2) Review of evaluation

Not later than 180 days after the date on which an evaluation is submitted, the Secretary shall review the evaluation and notify the over-the-road bus operator submitting the evaluation of the Secretary's approval or disapproval of the evaluation.

(k) Shared facilities

The Secretary may permit under this section the development and implementation of coordinated vulnerability assessments and security plans to the extent that an over-the-road bus operator shares facilities with, or is colocated with, other transportation entities or providers that are required to

develop vulnerability assessments and security plans under Federal law.

(l) Nondisclosure of information

(1) Submission of information to Congress

Nothing in this section shall be construed as authorizing the withholding of any information from Congress.

(2) Disclosure of independently furnished information

Nothing in this section shall be construed as affecting any authority or obligation of a Federal agency to disclose any record or information that the Federal agency obtains from an over-the-road bus operator under any other Federal law.

(Pub. L. 110–53, title XV, §1531, Aug. 3, 2007, 121 Stat. 454.)

§1182. Over-the-road bus security assistance

(a) In general

The Secretary shall establish a program for making grants to eligible private operators providing transportation by an over-the-road bus for security improvements described in subsection (b).

(b) Uses of funds

A recipient of a grant received under subsection (a) shall use the grant funds for one or more of the following:

(1) Constructing and modifying terminals, garages, and facilities, including terminals and other over-the-road bus facilities owned by State or local governments, to increase their security.

(2) Modifying over-the-road buses to increase their security.

(3) Protecting or isolating the driver of an over-the-road bus.

(4) Acquiring, upgrading, installing, or operating equipment, software, or accessorial services for collection, storage, or exchange of passenger and driver information through ticketing systems or other means and for information links with government agencies, for security purposes.

(5) Installing cameras and video surveillance equipment on over-the-road buses and at terminals, garages, and over-the-road bus facilities.

(6) Establishing and improving an emergency communications system linking drivers and over-the-road buses to the recipient's operations center or linking the operations center to law enforcement and emergency personnel.

(7) Implementing and operating passenger screening programs for weapons and explosives.

(8) Public awareness campaigns for enhanced over-the-road bus security.

(9) Operating and capital costs associated with over-the-road bus security awareness, preparedness, and response training, including training under section 1184 of this title and training developed by institutions of higher education and by nonprofit employee labor organizations, for over-the-road bus employees, including frontline employees.

(10) Chemical, biological, radiological, or explosive detection, including canine patrols for such detection.

(11) Overtime reimbursement, including reimbursement of State, local, and tribal governments for costs, for enhanced security personnel assigned to duties related to over-the-road bus security during periods of high or severe threat levels, National Special Security Events, or other periods of heightened security as determined by the Secretary.

(12) Live or simulated exercises, including those described in section 1183 of this title.

(13) Operational costs to hire, train, and employ police and security officers, including canine units, assigned to full-time security or counterterrorism duties related to over-the-road bus transportation, including reimbursement of State, local, and tribal government costs for such personnel.

(14) Development of assessments or security plans under section 1181 of this title.

(15) Such other improvements as the Secretary considers appropriate.

(c) Due consideration

In making grants under this section, the Secretary shall prioritize grant funding based on security risks to bus passengers and the ability of a project to reduce, or enhance response to, that risk, and shall not penalize private operators of over-the-road buses that have taken measures to enhance over-the-road bus transportation security prior to September 11, 2001.

(d) Department of Homeland Security responsibilities

In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants under this section, including application requirements;

(2) select grant recipients;

(3) award the funds authorized by this section based on risk, as identified by the plans required under section 1181 of this title or assessment or plan described in subsection (f)(2); and

(4) pursuant to subsection (c), establish priorities for the use of funds for grant recipients.

(e) Distribution of grants

Not later than 90 days after August 3, 2007, the Secretary and the Secretary of Transportation shall determine the most effective and efficient way to distribute grant funds to the recipients of grants determined by the Secretary under subsection (a). Subject to the determination made by the Secretaries, the Secretary may transfer funds to the Secretary of Transportation for the purposes of disbursing funds to the grant recipient.

(f) Eligibility

(1) A private operator providing transportation by an over-the-road bus is eligible for a grant under this section if the operator has completed a vulnerability assessment and developed a security plan that the Secretary has approved under section 1181 of this title. Grant funds may only be used for permissible uses under subsection (b) to further an over-the-road bus security plan.

(2) Notwithstanding the requirements for eligibility and uses in paragraph (1), prior to the earlier of 1 year after the date of issuance of final regulations requiring vulnerability assessments and security plans under section 1181 of this title or 3 years after August 3, 2007, the Secretary may award grants under this section for over-the-road bus security improvements listed under subsection (b) based upon over-the-road bus vulnerability assessments and security plans that the Secretary deems are sufficient for the purposes of this section but have not been approved by the Secretary in accordance with section 1181 of this title.

(g) Subject to certain terms and conditions

Except as otherwise specifically provided in this section, a grant made under this section shall be subject to the terms and conditions applicable to subrecipients who provide over-the-road bus transportation under section 5311(f) of title 49 and such other terms and conditions as are determined necessary by the Secretary.

(h) Limitation on uses of funds

A grant made under this section may not be used to make any State or local government cost-sharing contribution under any other Federal law.

(i) Annual reports

Each recipient of a grant under this section shall report annually to the Secretary and on the use of such grant funds.

(j) Consultation

In carrying out this section, the Secretary shall consult with over-the-road bus operators and nonprofit employee labor organizations representing over-the-road bus employees, public safety and law enforcement officials.

(k) Authorization

(1) In general

From the amounts appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to make grants under this section—

(A) $12,000,000 for fiscal year 2008;
(B) $25,000,000 for fiscal year 2009;
(C) $25,000,000 for fiscal year 2010; and
(D) $25,000,000 for fiscal year 2011.

(2) Period of availability

Sums appropriated to carry out this section shall remain available until expended.

(Pub. L. 110–53, title XV, §1532, Aug. 3, 2007, 121 Stat. 457.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (k)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1183. Over-the-road bus exercises

(a) In general

The Secretary shall establish a program for conducting security exercises for over-the-road bus transportation for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate, respond to, and recover from acts of terrorism.

(b) Covered entities

Entities to be assessed under the program shall include—

(1) Federal, State, and local agencies and tribal governments;
(2) over-the-road bus operators and over-the-road bus terminal owners and operators;
(3) governmental and nongovernmental emergency response providers and law enforcement agencies; and
(4) any other organization or entity that the Secretary determines appropriate.

(c) Requirements

The Secretary shall ensure that the program—

(1) consolidates existing security exercises for over-the-road bus operators and terminals administered by the Department and the Department of Transportation, as jointly determined by the Secretary and the Secretary of Transportation, unless the Secretary waives this consolidation requirement, as appropriate;
(2) consists of exercises that are—
(A) scaled and tailored to the needs of the over-the-road bus operators and terminals, including addressing the needs of the elderly and individuals with disabilities;
(B) live, in the case of the most at-risk facilities to a terrorist attack;
(C) coordinated with appropriate officials;
(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;
(E) inclusive, as appropriate, of over-the-road bus frontline employees; and
(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(3) provides that exercises described in paragraph (2) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to identify best practices, which shall be shared, as appropriate, with operators providing over-the-road bus transportation, nonprofit employee organizations that represent over-the-road bus employees, Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, and law enforcement personnel; and

(C) used to develop recommendations, as appropriate, provided to over-the-road bus operators and terminal owners and operators on remedial action to be taken in response to lessons learned;

(4) allows for proper advanced notification of communities and local governments in which exercises are held, as appropriate; and

(5) assists State, local, and tribal governments and over-the-road bus operators and terminal owners and operators in designing, implementing, and evaluating additional exercises that conform to the requirements of paragraph (2).

(d) National Exercise Program

The Secretary shall ensure that the exercise program developed under subsection (c) is consistent with the National Exercise Program established under section 748 of this title.

(Pub. L. 110–53, title XV, §1533, Aug. 3, 2007, 121 Stat. 460.)

§1184. Over-the-road bus security training program

(a) In general

Not later than 6 months after August 3, 2007, the Secretary shall develop and issue regulations for an over-the-road bus training program to prepare over-the-road bus frontline employees for potential security threats and conditions. The regulations shall take into consideration any current security training requirements or best practices.

(b) Consultation

The Secretary shall develop regulations under subsection (a) in consultation with—

(1) appropriate law enforcement, fire service, emergency response, security, and terrorism experts;

(2) operators providing over-the-road bus transportation; and

(3) nonprofit employee labor organizations representing over-the-road bus employees and emergency response personnel.

(c) Program elements

The regulations developed under subsection (a) shall require security training programs, to include, at a minimum, elements to address the following, as applicable:

(1) Determination of the seriousness of any occurrence or threat.

(2) Driver and passenger communication and coordination.

(3) Appropriate responses to defend or protect oneself.

(4) Use of personal and other protective equipment.

(5) Evacuation procedures for passengers and over-the-road bus employees, including individuals with disabilities and the elderly.

(6) Psychology, behavior, and methods of terrorists, including observation and analysis.

(7) Training related to psychological responses to terrorist incidents, including the ability to cope with hijacker behavior and passenger responses.

(8) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(9) Recognition and reporting of dangerous substances, suspicious packages, and situations.

(10) Understanding security incident procedures, including procedures for communicating with

emergency response providers and for on-scene interaction with such emergency response providers.

(11) Operation and maintenance of security equipment and systems.

(12) Other security training activities that the Secretary considers appropriate.

(d) Required programs

(1) Development and submission to Secretary

Not later than 90 days after the Secretary issues the regulations under subsection (a), each over-the-road bus operator shall develop a security training program in accordance with such regulations and submit the program to the Secretary for approval.

(2) Approval

Not later than 60 days after receiving a security training program under this subsection, the Secretary shall approve the program or require the over-the-road bus operator that developed the program to make any revisions to the program that the Secretary considers necessary for the program to meet the requirements of the regulations. An over-the-road bus operator shall respond to the Secretary's comments not later than 30 days after receiving them.

(3) Training

Not later than 1 year after the Secretary approves a security training program in accordance with this subsection, the over-the-road bus operator that developed the program shall complete the training of all over-the-road bus frontline employees who were hired by the operator more than 30 days preceding such date. For such employees employed less than 30 days by an operator preceding such date, training shall be completed within the first 60 days of employment.

(4) Updates of regulations and program revisions

The Secretary shall periodically review and update, as appropriate, the training regulations issued under subsection (a) to reflect new or changing security threats. Each over-the-road bus operator shall revise its training program accordingly and provide additional training as necessary to its employees within a reasonable time after the regulations are updated.

(e) National Training Program

The Secretary shall ensure that the training program developed under subsection (a) is a component of the National Training Program established under section 748 of this title.

(f) Reporting requirements

Not later than 2 years after the date of regulation issuance, the Secretary shall review implementation of the training program of a representative sample of over-the-road bus operators and over-the-road bus frontline employees, and report to the appropriate congressional committees of such reviews. The Secretary may submit the report in both classified and redacted formats as necessary.

(Pub. L. 110–53, title XV, §1534, Aug. 3, 2007, 121 Stat. 461.)

§1185. Over-the-road bus security research and development

(a) Establishment of research and development program

The Secretary, acting through the Under Secretary for Science and Technology and the Administrator of the Transportation Security Administration, shall carry out a research and development program for the purpose of improving the security of over-the-road buses.

(b) Eligible projects

The research and development program may include projects—

(1) to reduce the vulnerability of over-the-road buses, stations, terminals, and equipment to explosives and hazardous chemical, biological, and radioactive substances, including the

development of technology to screen passengers in large numbers with minimal interference and disruption;

(2) to test new emergency response and recovery techniques and technologies, including those used at international borders;

(3) to develop improved technologies, including those for—

(A) emergency response training, including training in a tunnel environment, if appropriate; and

(B) security and redundancy for critical communications, electrical power, computer, and over-the-road bus control systems; and

(4) to address other vulnerabilities and risks identified by the Secretary.

(c) Coordination with other research initiatives

The Secretary—

(1) shall ensure that the research and development program is consistent with the other transportation security research and development programs required by this Act;

(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

(A) the Department of Transportation, including University Transportation Centers and other institutes, centers, and simulators funded by the Department of Transportation;

(B) the National Academy of Sciences;

(C) the Technical Support Working Group;

(D) other Federal departments and agencies; and

(E) other Federal and private research laboratories, research entities, and institutions of higher education, including Historically Black Colleges and Universities, Hispanic Serving Institutions, and Indian Tribally Controlled Colleges and Universities;

(3) shall carry out any research and development project authorized by this section through a reimbursable agreement with an appropriate Federal agency, if the agency—

(A) is currently sponsoring a research and development project in a similar area; or

(B) has a unique facility or capability that would be useful in carrying out the project;

(4) may award grants and enter into cooperative agreements, contracts, other transactions, or reimbursable agreements to the entities described in paragraph (2) and eligible recipients under section 1182 of this title; and

(5) shall make reasonable efforts to enter into memoranda of understanding, contracts, grants, cooperative agreements, or other transactions with private operators providing over-the-road bus transportation willing to contribute assets, physical space, and other resources.

(d) Privacy and civil rights and civil liberties issues

(1) Consultation

In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department as appropriate and in accordance with section 142 of this title.

(2) Privacy impact assessments

In accordance with sections 142 and 345 of this title, the Chief Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed under this section that the Secretary determines could have an impact on privacy, civil rights, or civil liberties.

(e) Authorization of appropriations

(1) In general

From the amounts appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section—

(A) $2,000,000 for fiscal year 2008;
(B) $2,000,000 for fiscal year 2009;
(C) $2,000,000 for fiscal year 2010; and
(D) $2,000,000 for fiscal year 2011.

(2) Period of availability

Such sums shall remain available until expended.

(Pub. L. 110–53, title XV, §1535, Aug. 3, 2007, 121 Stat. 462.)

EDITORIAL NOTES

REFERENCES IN TEXT

This Act, referred to in subsec. (c)(1), is Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 266, known as the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted this chapter and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title of 2007 Amendment note set out under section 101 of this title and Tables.

Section 114(w) of title 49, referred to in subsec. (e)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1186. Memorandum of Understanding annex

Not later than 1 year after August 3, 2007, the Secretary of Transportation and the Secretary shall execute and develop an annex to the Memorandum of Understanding between the two departments signed on September 28, 2004, governing the specific roles, delineations of responsibilities, resources, and commitments of the Department of Transportation and the Department of Homeland Security, respectively, in addressing motor carrier transportation security matters, including over-the-road bus security matters, and shall cover the processes the Departments will follow to promote communications, efficiency, and nonduplication of effort.

(Pub. L. 110–53, title XV, §1541, Aug. 3, 2007, 121 Stat. 469.)

PART D—HAZARDOUS MATERIAL AND PIPELINE SECURITY

§1201. Railroad routing of security-sensitive materials

(a) In general

Not later than 9 months after August 3, 2007, the Secretary of Transportation, in consultation with the Secretary, shall publish a final rule based on the Pipeline and Hazardous Materials Safety Administration's Notice of Proposed Rulemaking published on December 21, 2006, entitled "Hazardous Materials: Enhancing Railroad Transportation Safety and Security for Hazardous Materials Shipments". The final rule shall incorporate the requirements of this section and, as appropriate, public comments received during the comment period of the rulemaking.

(b) Security-sensitive materials commodity data

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to, no later than 90 days after the end of each calendar year, compile security-sensitive materials commodity data. Such data must be collected by

route, line segment, or series of line segments, as aggregated by the railroad carrier. Within the railroad carrier selected route, the commodity data must identify the geographic location of the route and the total number of shipments by the United Nations identification number for the security-sensitive materials.

(c) Railroad transportation route analysis for security-sensitive materials

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to, for each calendar year, provide a written analysis of the safety and security risks for the transportation routes identified in the security-sensitive materials commodity data collected as required by subsection (b). The safety and security risks present shall be analyzed for the route, railroad facilities, railroad storage facilities, and high-consequence targets along or in proximity to the route.

(d) Alternative route analysis for security-sensitive materials

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to—

(1) for each calendar year—

(A) identify practicable alternative routes over which the railroad carrier has authority to operate as compared to the current route for such a shipment analyzed under subsection (c); and

(B) perform a safety and security risk assessment of the alternative route for comparison to the route analysis specified in subsection (c);

(2) ensure that the analysis under paragraph (1) includes—

(A) identification of safety and security risks for an alternative route;

(B) comparison of those risks identified under subparagraph (A) to the primary railroad transportation route, including the risk of a catastrophic release from a shipment traveling along the alternate route compared to the primary route;

(C) any remediation or mitigation measures implemented on the primary or alternative route; and

(D) potential economic effects of using an alternative route; and

(3) consider when determining the practicable alternative routes under paragraph (1)(A) the use of interchange agreements with other railroad carriers.

(e) Alternative route selection for security-sensitive materials

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to use the analysis required by subsections (c) and (d) to select the safest and most secure route to be used in transporting security-sensitive materials.

(f) Review

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to annually review and select the practicable route posing the least overall safety and security risk in accordance with this section. The railroad carrier must retain in writing all route review and selection decision documentation and restrict the distribution, disclosure, and availability of information contained in the route analysis to appropriate persons. This documentation should include, but is not limited to, comparative analyses, charts, graphics, or railroad system maps.

(g) Retrospective analysis

The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to, not less than once every 3 years, analyze the route selection determinations required under this section. Such an analysis shall include a comprehensive, systemwide review of all operational changes, infrastructure modifications, traffic adjustments, changes in the nature of high-consequence targets located along or in proximity to the

route, or other changes affecting the safety and security of the movements of security-sensitive materials that were implemented since the previous analysis was completed.

(h) Consultation

In carrying out subsection (c), railroad carriers transporting security-sensitive materials in commerce shall seek relevant information from State, local, and tribal officials, as appropriate, regarding security risks to high-consequence targets along or in proximity to a route used by a railroad carrier to transport security-sensitive materials.

(i) Definitions

In this section:

(1) The term "route" includes storage facilities and trackage used by railroad cars in transportation in commerce.

(2) The term "high-consequence target" means a property, natural resource, location, area, or other target designated by the Secretary that is a viable terrorist target of national significance, which may include a facility or specific critical infrastructure, the attack of which by railroad could result in—

(A) catastrophic loss of life;

(B) significant damage to national security or defense capabilities; or

(C) national economic harm.

(Pub. L. 110–53, title XV, §1551, Aug. 3, 2007, 121 Stat. 469.)

§1202. Railroad security-sensitive material tracking

(a) Communications

(1) In general

In conjunction with the research and development program established under section 1168 of this title and consistent with the results of research relating to wireless and other tracking technologies, the Secretary, in consultation with the Administrator of the Transportation Security Administration, shall develop a program that will encourage the equipping of railroad cars transporting security-sensitive materials, as defined in section 1151 of this title, with technology that provides—

(A) car position location and tracking capabilities; and

(B) notification of railroad car depressurization, breach, unsafe temperature, or release of hazardous materials, as appropriate.

(2) Coordination

In developing the program required by paragraph (1), the Secretary shall—

(A) consult with the Secretary of Transportation to coordinate the program with any ongoing or planned efforts for railroad car tracking at the Department of Transportation; and

(B) ensure that the program is consistent with recommendations and findings of the Department of Homeland Security's hazardous material railroad tank car tracking pilot programs.

(b) Funding

From the amounts appropriated pursuant to [1] 114(w) [2] of title 49, there shall be made available to the Secretary to carry out this section—

(1) $3,000,000 for fiscal year 2008;

(2) $3,000,000 for fiscal year 2009; and

(3) $3,000,000 for fiscal year 2010.

(Pub. L. 110–53, title XV, §1552, Aug. 3, 2007, 121 Stat. 471.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (b), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *So in original. Probably should be followed by "section".*

[2] *See References in Text note below.*

§1203. Hazardous materials highway routing

(a) Route plan guidance

Not later than 1 year after August 3, 2007, the Secretary of Transportation, in consultation with the Secretary, shall—

(1) document existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier, and develop a framework for using a geographic information system-based approach to characterize routes in the national hazardous materials route registry;

(2) assess and characterize existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier for the purpose of identifying measurable criteria for selecting routes based on safety and security concerns;

(3) analyze current route-related hazardous materials regulations in the United States, Canada, and Mexico to identify cross-border differences and conflicting regulations;

(4) document the safety and security concerns of the public, motor carriers, and State, local, territorial, and tribal governments about the highway routing of hazardous materials;

(5) prepare guidance materials for State officials to assist them in identifying and reducing both safety concerns and security risks when designating highway routes for hazardous materials consistent with the 13 safety-based nonradioactive materials routing criteria and radioactive materials routing criteria in subpart C part 397 of title 49, Code of Federal Regulations;

(6) develop a tool that will enable State officials to examine potential routes for the highway transportation of hazardous materials, assess specific security risks associated with each route, and explore alternative mitigation measures; and

(7) transmit to the appropriate congressional committees a report on the actions taken to fulfill paragraphs (1) through (6) and any recommended changes to the routing requirements for the highway transportation of hazardous materials in part 397 of title 49, Code of Federal Regulations.

(b) Route plans

(1) Assessment

Not later than 1 year after August 3, 2007, the Secretary of Transportation shall complete an assessment of the safety and national security benefits achieved under existing requirements for route plans, in written or electronic format, for explosives and radioactive materials. The assessment shall, at a minimum—

(A) compare the percentage of Department of Transportation recordable incidents and the severity of such incidents for shipments of explosives and radioactive materials for which such route plans are required with the percentage of recordable incidents and the severity of such incidents for shipments of explosives and radioactive materials not subject to such route plans; and

(B) quantify the security and safety benefits, feasibility, and costs of requiring each motor carrier that is required to have a hazardous material safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry such a route plan that meets the requirements of section 397.101 of that title when transporting the type and quantity of

hazardous materials described in section 385.403, taking into account the various segments of the motor carrier industry, including tank truck, truckload and less than truckload carriers.

(2) Report

Not later than 1 year after August 3, 2007, the Secretary of Transportation shall submit a report to the appropriate congressional committees containing the findings and conclusions of the assessment.

(c) Requirement

The Secretary shall require motor carriers that have a hazardous material safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry a route plan, in written or electronic format, that meets the requirements of section 397.101 of that title when transporting the type and quantity of hazardous materials described in section 385.403 if the Secretary determines, under the assessment required in subsection (b), that such a requirement would enhance security and safety without imposing unreasonable costs or burdens upon motor carriers.

(Pub. L. 110–53, title XV, §1553, Aug. 3, 2007, 121 Stat. 472.)

§1204. Motor carrier security-sensitive material tracking

(a) Communications

(1) In general

Not later than 6 months after August 3, 2007, consistent with the findings of the Transportation Security Administration's hazardous materials truck security pilot program, the Secretary, through the Administrator of the Transportation Security Administration and in consultation with the Secretary of Transportation, shall develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides—

(A) frequent or continuous communications;

(B) vehicle position location and tracking capabilities; and

(C) a feature that allows a driver of such vehicles to broadcast an emergency distress signal.

(2) Considerations

In developing the program required by paragraph (1), the Secretary shall—

(A) consult with the Secretary of Transportation to coordinate the program with any ongoing or planned efforts for motor carrier or security-sensitive materials tracking at the Department of Transportation;

(B) take into consideration the recommendations and findings of the report on the hazardous material safety and security operational field test released by the Federal Motor Carrier Safety Administration on November 11, 2004; and

(C) evaluate—

(i) any new information related to the costs and benefits of deploying, equipping, and utilizing tracking technology, including portable tracking technology, for motor carriers transporting security-sensitive materials not included in the hazardous material safety and security operational field test report released by the Federal Motor Carrier Safety Administration on November 11, 2004;

(ii) the ability of tracking technology to resist tampering and disabling;

(iii) the capability of tracking technology to collect, display, and store information regarding the movement of shipments of security-sensitive materials by commercial motor vehicles;

(iv) the appropriate range of contact intervals between the tracking technology and a commercial motor vehicle transporting security-sensitive materials;

(v) technology that allows the installation by a motor carrier of concealed electronic devices on commercial motor vehicles that can be activated by law enforcement authorities to

disable the vehicle or alert emergency response resources to locate and recover security-sensitive materials in the event of loss or theft of such materials;

(vi) whether installation of the technology described in clause (v) should be incorporated into the program under paragraph (1);

(vii) the costs, benefits, and practicality of such technology described in clause (v) in the context of the overall benefit to national security, including commerce in transportation; and

(viii) other systems and information the Secretary determines appropriate.

(b) Funding

From the amounts appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section—

(1) $7,000,000 for fiscal year 2008 of which $3,000,000 may be used for equipment;
(2) $7,000,000 for fiscal year 2009 of which $3,000,000 may be used for equipment; and
(3) $7,000,000 for fiscal year 2010 of which $3,000,000 may be used for equipment.

(c) Report

Not later than 1 year after the issuance of regulations under subsection (a), the Secretary shall issue a report to the appropriate congressional committees on the program developed and evaluation carried out under this section.

(d) Limitation

The Secretary may not mandate the installation or utilization of a technology described under this section without additional congressional authority provided after August 3, 2007.

(Pub. L. 110–53, title XV, §1554, Aug. 3, 2007, 121 Stat. 473.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (b)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1205. Hazardous materials security inspections and study

(a) In general

The Secretary of Transportation shall consult with the Secretary to limit, to the extent practicable, duplicative reviews of the hazardous materials security plans required under part 172, title 49, Code of Federal Regulations.

(b) Transportation costs study

Within 1 year after August 3, 2007, the Secretary of Transportation, in conjunction with the Secretary, shall study to what extent the insurance, security, and safety costs borne by railroad carriers, motor carriers, pipeline carriers, air carriers, and maritime carriers associated with the transportation of hazardous materials are reflected in the rates paid by offerors of such commodities as compared to the costs and rates, respectively, for the transportation of nonhazardous materials.

(Pub. L. 110–53, title XV, §1555, Aug. 3, 2007, 121 Stat. 475.)

§1206. Use of transportation security card in hazmat licensing

(1) Background check

An individual who has a valid transportation employee identification card issued by the Secretary

under section 70105 of title 46 shall be deemed to have met the background records check required under section 5103a of title 49.

(2) State review

Nothing in this section prevents or preempts a State from conducting a criminal records check of an individual that has applied for a license to operate a motor vehicle transporting in commerce a hazardous material.

(Pub. L. 110–53, title XV, §1556(b), Aug. 3, 2007, 121 Stat. 475.)

§1207. Pipeline security inspections and enforcement

(a) In general

Not later than 9 months after August 3, 2007, consistent with the Annex to the Memorandum of Understanding executed on August 9, 2006, between the Department of Transportation and the Department, the Secretary, in consultation with the Secretary of Transportation, shall establish a program for reviewing pipeline operator adoption of recommendations of the September 5, 2002, Department of Transportation Research and Special Programs Administration's Pipeline Security Information Circular, including the review of pipeline security plans and critical facility inspections.

(b) Review and inspection

Not later than 12 months after August 3, 2007, the Secretary and the Secretary of Transportation shall develop and implement a plan for reviewing the pipeline security plans and an inspection of the critical facilities of the 100 most critical pipeline operators covered by the September 5, 2002, circular, where such facilities have not been inspected for security purposes since September 5, 2002, by either the Department or the Department of Transportation.

(c) Compliance review methodology

In reviewing pipeline operator compliance under subsections (a) and (b), risk assessment methodologies shall be used to prioritize risks and to target inspection and enforcement actions to the highest risk pipeline assets.

(d) Regulations

Not later than 18 months after August 3, 2007, the Secretary and the Secretary of Transportation shall develop and transmit to pipeline operators security recommendations for natural gas and hazardous liquid pipelines and pipeline facilities. If the Secretary determines that regulations are appropriate, the Secretary shall consult with the Secretary of Transportation on the extent of risk and appropriate mitigation measures, and the Secretary or the Secretary of Transportation, consistent with the Annex to the Memorandum of Understanding executed on August 9, 2006, shall promulgate such regulations and carry out necessary inspection and enforcement actions. Any regulations shall incorporate the guidance provided to pipeline operators by the September 5, 2002, Department of Transportation Research and Special Programs Administration's Pipeline Security Information Circular and contain additional requirements as necessary based upon the results of the inspections performed under subsection (b). The regulations shall include the imposition of civil penalties for noncompliance.

(e) Funding

From the amounts appropriated pursuant to section 114(w) [1] of title 49, there shall be made available to the Secretary to carry out this section—

(1) $2,000,000 for fiscal year 2008;
(2) $2,000,000 for fiscal year 2009; and
(3) $2,000,000 for fiscal year 2010.

(Pub. L. 110–53, title XV, §1557, Aug. 3, 2007, 121 Stat. 475.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 114(w) of title 49, referred to in subsec. (e)(1), was redesignated section 114(v) of title 49 by Pub. L. 115–254, div. K, §1904(b)(1)(I), Oct. 5, 2018, 132 Stat. 3545.

[1] *See References in Text note below.*

§1208. Pipeline security and incident recovery plan

(a) In general

The Secretary, in consultation with the Secretary of Transportation and the Administrator of the Pipeline and Hazardous Materials Safety Administration, and in accordance with the Annex to the Memorandum of Understanding executed on August 9, 2006, the National Strategy for Transportation Security, and Homeland Security Presidential Directive–7, shall develop a pipeline security and incident recovery protocols plan. The plan shall include—

(1) for the Government to provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations as determined under section 1207 of this title when—

(A) under severe security threat levels of alert; or

(B) under specific security threat information relating to such pipeline infrastructure or operations exists; and

(2) an incident recovery protocol plan, developed in conjunction with interstate and intrastate transmission and distribution pipeline operators and terminals and facilities operators connected to pipelines, to develop protocols to ensure the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses in the event of an incident affecting the interstate and intrastate natural gas and hazardous liquid transmission and distribution pipeline system, which shall include protocols for restoring essential services supporting pipelines and granting access to pipeline operators for pipeline infrastructure repair, replacement, or bypass following an incident.

(b) Existing private and public sector efforts

The plan shall take into account actions taken or planned by both private and public entities to address identified pipeline security issues and assess the effective integration of such actions.

(c) Consultation

In developing the plan under subsection (a), the Secretary shall consult with the Secretary of Transportation, interstate and intrastate transmission and distribution pipeline operators, nonprofit employee organizations representing pipeline employees, emergency responders, offerors, State pipeline safety agencies, public safety officials, and other relevant parties.

(d) Report

(1) Contents

Not later than 2 years after August 3, 2007, the Secretary shall transmit to the appropriate congressional committees a report containing the plan required by subsection (a), including an estimate of the private and public sector costs to implement any recommendations.

(2) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(Pub. L. 110–53, title XV, §1558, Aug. 3, 2007, 121 Stat. 476.)

CHAPTER 5—BORDER INFRASTRUCTURE AND TECHNOLOGY MODERNIZATION

Sec.
1401. Definitions.
1402 to 1404. Repealed.
1405. Authorization of appropriations.

§1401. Definitions

In this chapter:

(1) Commissioner

The term "Commissioner" means the Commissioner of U.S. Customs and Border Protection of the Department of Homeland Security.

(2) Maquiladora

The term "maquiladora" means an entity located in Mexico that assembles and produces goods from imported parts for export to the United States.

(3) Northern border

The term "northern border" means the international border between the United States and Canada.

(4) Secretary

The term "Secretary" means the Secretary of the Department of Homeland Security.

(5) Southern border

The term "southern border" means the international border between the United States and Mexico.

(Pub. L. 110–161, div. E, title VI, §602, Dec. 26, 2007, 121 Stat. 2094.)

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

Pub. L. 110–161, div. E, title VI, §601, Dec. 26, 2007, 121 Stat. 2094, provided that: "This title [enacting this chapter] may be cited as the 'Border Infrastructure and Technology Modernization Act of 2007'."

§§1402, 1403. Repealed. Pub. L. 113–188, title X, §1001(b), Nov. 26, 2014, 128 Stat. 2022

Section 1402, Pub. L. 110–161, div. E, title VI, §603, Dec. 26, 2007, 121 Stat. 2094, related to the Port of Entry Infrastructure Assessment Study.

Section 1403, Pub. L. 110–161, div. E, title VI, §604, Dec. 26, 2007, 121 Stat. 2095, related to the National Land Border Security Plan.

§1404. Repealed. Pub. L. 114–4, title V, §566, Mar. 4, 2015, 129 Stat. 73

Section, Pub. L. 110–161, div. E, title VI, §605, Dec. 26, 2007, 121 Stat. 2096, related to the port of entry technology demonstration program.

§1405. Authorization of appropriations

(a) In general

In addition to any funds otherwise available, there are authorized to be appropriated such sums as may be necessary to carry out this chapter for fiscal years 2009 through 2013.

(b) International agreements

Funds authorized to be appropriated under this chapter may be used for the implementation of projects described in the Declaration on Embracing Technology and Cooperation to Promote the Secure and Efficient Flow of People and Commerce across our Shared Border between the United States and Mexico, agreed to March 22, 2002, Monterrey, Mexico (commonly known as the Border Partnership Action Plan) or the Smart Border Declaration between the United States and Canada, agreed to December 12, 2001, Ottawa, Canada that are consistent with the provisions of this chapter.

(Pub. L. 110–161, div. E, title VI, §606, Dec. 26, 2007, 121 Stat. 2097.)

CHAPTER 6—CYBERSECURITY

SUBCHAPTER I—CYBERSECURITY INFORMATION SHARING

Sec.
1500. National Cyber Director.
1501. Definitions.
1502. Sharing of information by the Federal Government.
1503. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.
1504. Sharing of cyber threat indicators and defensive measures with the Federal Government.
1505. Protection from liability.
1506. Oversight of government activities.
1507. Construction and preemption.
1508. Report on cybersecurity threats.
1509. Exception to limitation on authority of Secretary of Defense to disseminate certain information.
1510. Effective period.

SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT

1521. Definitions.
1522. Advanced internal defenses.
1523. Federal cybersecurity requirements.
1524. Assessment; reports.
1525. Termination.
1526. Inventory of cryptographic systems; migration to post-quantum cryptography.

SUBCHAPTER III—OTHER CYBER MATTERS

1531. Apprehension and prosecution of international cyber criminals.
1532. Enhancement of emergency services.
1533. Improving cybersecurity in the health care industry.
1534. Cybercrime.

STATUTORY NOTES AND RELATED SUBSIDIARIES

LIMITATION RELATING TO ESTABLISHMENT OR SUPPORT OF CYBERSECURITY UNIT WITH THE RUSSIAN FEDERATION

Pub. L. 116–92, div. E, title LXVII, §6701, Dec. 20, 2019, 133 Stat. 2221, provided that:

"(a) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

"(1) the congressional intelligence committees;

"(2) the Committee on Armed Services of the Senate and the Committee on Armed Services of the

House of Representatives; and

"(3) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

"(b) LIMITATION.—

"(1) IN GENERAL.—No amount may be expended by the Federal Government, other than the Department of Defense, to enter into or implement any bilateral agreement between the United States and the Russian Federation regarding cybersecurity, including the establishment or support of any cybersecurity unit, unless, at least 30 days prior to the conclusion of any such agreement, the Director of National Intelligence submits to the appropriate congressional committees a report on such agreement that includes the elements required by subsection (c).

"(2) DEPARTMENT OF DEFENSE AGREEMENTS.—Any agreement between the Department of Defense and the Russian Federation regarding cybersecurity shall be conducted in accordance with section 1232 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328) [130 Stat. 2488], as amended by section 1231 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91) [131 Stat. 1657].

"(c) ELEMENTS.—If the Director submits a report under subsection (b) with respect to an agreement, such report shall include a discussion of each of the following:

"(1) The purpose of the agreement.

"(2) The nature of any intelligence to be shared pursuant to the agreement.

"(3) The expected value to national security resulting from the implementation of the agreement.

"(4) Such counterintelligence concerns associated with the agreement as the Director may have and such measures as the Director expects to be taken to mitigate such concerns.

"(d) RULE OF CONSTRUCTION.—This section shall not be construed to affect any existing authority of the Director of National Intelligence, the Director of the Central Intelligence Agency, or another head of an element of the intelligence community, to share or receive foreign intelligence on a case-by-case basis."

[For definitions of "congressional intelligence committees" and "intelligence community" as used in section 6701 of div. E of Pub. L. 116–92, set out above, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of Title 50, War and National Defense.]

EXECUTIVE DOCUMENTS

EX. ORD. NO. 13800. STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

Ex. Ord. No. 13800, May 11, 2017, 82 F.R. 22391, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

SECTION 1. *Cybersecurity of Federal Networks*.

(a) *Policy*. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) *Findings*.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) *Risk Management*.

(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and

(B) a plan to:

(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;

(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and

(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:

(1) be completed within 90 days of the date of this order; and

(2) describe the legal, policy, and budgetary considerations relevant to—as well as the technical feasibility and cost effectiveness, including timelines and milestones, of—transitioning all agencies, or a subset of agencies, to:

(aa) one or more consolidated network architectures; and

(bb) shared IT services, including email, cloud, and cybersecurity services.

(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity, including by

making recommendations to ensure consistency with [former] section 227 [now 2209] of the Homeland Security Act ([former] 6 U.S.C. 148) [now 6 U.S.C. 659] and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

SEC. 2. *Cybersecurity of Critical Infrastructure*.

(a) *Policy*. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.

(b) *Support to Critical Infrastructure at Greatest Risk*. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;

(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and

(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) *Supporting Transparency in the Marketplace*. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(d) *Resilience Against Botnets and Other Automated, Distributed Threats*. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) *Assessment of Electricity Disruption Incident Response Capabilities*. The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local,

tribal, and territorial governments, and with others as appropriate, shall jointly assess:

(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) *Department of Defense Warfighting Capabilities and Industrial Base*. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

SEC. 3. *Cybersecurity for the Nation*.

(a) *Policy*. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

(b) *Deterrence and Protection*. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) *International Cooperation*. As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.

(d) *Workforce Development*. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify

foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

SEC. 4. *Definitions*. For the purposes of this order:

(a) The term "appropriate stakeholders" means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term "information technology" (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems of agencies that monitor and control physical equipment and processes.

(c) The term "IT architecture" refers to the integration and implementation of IT within an agency.

(d) The term "network architecture" refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.

SEC. 5. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be construed to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence or law enforcement operations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

EX. ORD. NO. 13870. AMERICA'S CYBERSECURITY WORKFORCE

Ex. Ord. No. 13870, May 2, 2019, 84 F.R. 20523, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to better ensure continued American economic prosperity and national security, it is hereby ordered as follows:

SECTION 1. *Policy*. (a) America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) [set out above], each emphasize [sic] that a superior cybersecurity workforce will promote American prosperity and preserve peace. America's cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and maintain the data, systems, and networks on which our economy and way of life depend. Whether they are employed in the public or private sectors, they are guardians of our national and economic security.

(b) The United States Government must enhance the workforce mobility of America's cybersecurity practitioners to improve America's national cybersecurity. During their careers, America's cybersecurity practitioners will serve in various roles for multiple and diverse entities. United States Government policy must facilitate the seamless movement of cybersecurity practitioners between the public and private sectors, maximizing the contributions made by their diverse skills, experiences, and talents to our Nation.

(c) The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. The United States Government must also recognize and reward the country's highest-performing cybersecurity practitioners and

teams.

(d) The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers—especially when those talents and capabilities can advance our national and economic security. The Nation is experiencing a shortage of cybersecurity talent and capability, and innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities. Training opportunities, such as work-based learning, apprenticeships, and blended learning approaches, must be enhanced for both new workforce entrants and those who are advanced in their careers.

(e) In accordance with Executive Order 13800, the President will continue to hold heads of executive departments and agencies (agencies) accountable for managing cybersecurity risk to their enterprises, which includes ensuring the effectiveness of their cybersecurity workforces.

SEC. 2. *Strengthening the Federal Cybersecurity Workforce*. (a) To grow the cybersecurity capability of the United States Government, increase integration of the Federal cybersecurity workforce, and strengthen the skills of Federal information technology and cybersecurity practitioners, the Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget (OMB) and the Director of the Office of Personnel Management (OPM), shall establish a cybersecurity rotational assignment program, which will serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners. Within 90 days of the date of this order [May 2, 2019], the Secretary of Homeland Security, in consultation with the Directors of OMB and OPM, shall provide a report to the President that describes the proposed program, identifies its resource implications, and recommends actions required for its implementation. The report shall evaluate how to achieve the following objectives, to the extent permitted by applicable law, as part of the program:

(i) The non-reimbursable detail of information technology and cybersecurity employees, who are nominated by their employing agencies, to serve at the Department of Homeland Security (DHS);

(ii) The non-reimbursable detail of experienced cybersecurity DHS employees to other agencies to assist in improving those agencies' cybersecurity risk management;

(iii) The use of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) as the basis for cybersecurity skill requirements for program participants;

(iv) The provision of training curricula and expansion of learning experiences to develop participants' skill levels; and

(v) Peer mentoring to enhance workforce integration.

(b) Consistent with applicable law and to the maximum extent practicable, the Administrator of General Services, in consultation with the Director of OMB and the Secretary of Commerce, shall:

(i) Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services;

(ii) Ensure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the NICE Framework; and

(iii) Provide a report to the President, within 1 year of the date of this order, that describes how the NICE Framework has been incorporated into contracts for information technology and cybersecurity services, evaluates the effectiveness of this approach in improving services provided to the United States Government, and makes recommendations to increase the effective use of the NICE Framework by United States Government contractors.

(c) Within 180 days of the date of this order, the Director of OPM, in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other agencies as appropriate, shall identify a list of cybersecurity aptitude assessments for agencies to use in identifying current employees with the potential to acquire cybersecurity skills for placement in reskilling programs to perform cybersecurity work. Agencies shall incorporate one or more of these assessments into their personnel development programs, as appropriate and consistent with applicable law.

(d) Agencies shall ensure that existing awards and decorations for the uniformed services and civilian personnel recognize performance and achievements in the areas of cybersecurity and cyber-operations, including by ensuring the availability of awards and decorations equivalent to citations issued pursuant to Executive Order 10694 of January 10, 1957 (Authorizing the Secretaries of the Army, Navy, and Air Force To Issue Citations in the Name of the President of the United States to Military and Naval Units for Outstanding Performance in Action) [22 F.R. 253], as amended. Where necessary and appropriate, agencies shall establish new awards and decorations to recognize performance and achievements in the areas of cybersecurity and cyber-operations. The Assistant to the President for National Security Affairs may recommend to agencies that any cyber unified coordination group or similar ad hoc interagency group that has addressed a significant

cybersecurity or cyber-operations-related national security crisis, incident, or effort be recognized for appropriate awards and decorations.

(e) The Secretary of Homeland Security, in consultation with the Secretary of Defense, the Director of the Office of Science and Technology Policy, the Director of OMB, and the heads of other appropriate agencies, shall develop a plan for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines. The plan shall be submitted to the President within 90 days of the date of this order. The first competition shall be held no later than December 31, 2019, and annually thereafter. The plan for the competition shall address the following:

(i) The challenges and benefits of inviting advisers, participants, or observers from non-Federal entities to observe or take part in the competition and recommendations for including them in future competitions, as appropriate;

(ii) How the Department of Energy, through the National Laboratories, in consultation with the Administrator of the United States Digital Service, can provide expert technical advice and assistance to support the competition, as appropriate;

(iii) The parameters for the competition, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate. These parameters should include competition categories involving individual and team events, software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, cyber-physical systems, and other disciplines;

(iv) How to encourage agencies to select their best cybersecurity practitioners as individual and team participants. Such practitioners should include Federal employees and uniformed services personnel from Federal civilian agencies, as well as Department of Defense active duty military personnel, civilians, and those serving in a drilling reserve capacity in the Armed Forces Reserves or National Guard;

(v) The extent to which agencies, as well as uniformed services, may develop a President's Cup awards program that is consistent with applicable law and regulations governing awards and that allows for the provision of cash awards of not less than $25,000. Any such program shall require the agency to establish an awards program before allowing its employees to participate in the President's Cup Cybersecurity Competition. In addition, any such program may not preclude agencies from recognizing winning and non-winning participants through other means, including honorary awards, informal recognition awards, rating-based cash awards, time-off awards, Quality Step Increases, or other agency-based compensation flexibilities as appropriate and consistent with applicable law; and

(vi) How the uniformed services, as appropriate and consistent with applicable law, may designate service members who win these competitions as having skills at a time when there is a critical shortage of such skills within the uniformed services. The plan should also address how the uniformed services may provide winning service members with a combination of bonuses, advancements, and meritorious recognition to be determined by the Secretaries of the agencies concerned.

(f) The Director of OMB shall, in consultation with appropriate agencies, develop annually a list of agencies and subdivisions related to cybersecurity that have a primary function of intelligence, counterintelligence, investigative, or national security work, including descriptions of such functions. The Director of OMB shall provide this list to the President, through the Deputy Assistant to the President for Homeland Security and Counterterrorism (DAPHSCT), every year starting September 1, 2019, for consideration of whether those agencies or subdivisions should be exempted from coverage under the Federal Labor-Management Relations Program, consistent with the requirements of section 7103(b)(1) of title 5, United States Code.

SEC. 3. *Strengthening the Nation's Cybersecurity Workforce*. (a) The Secretary of Commerce and the Secretary of Homeland Security (Secretaries), in coordination with the Secretary of Education and the heads of other agencies as the Secretaries determine is appropriate, shall execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (Workforce Report) developed pursuant to Executive Order 13800. The Secretaries shall develop a consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce. To fulfill the Workforce Report's vision of preparing, growing, and sustaining a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity, priority consideration will be given to the following imperatives:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector

resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

(b) To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly cyber-physical systems for which safety and reliability depend on secure control systems, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Secretary of Homeland Security, in coordination with the Director of OPM and the Secretary of Labor, shall provide a report to the President, through the DAPHSCT, within 180 days of the date of this order that:

(i) Identifies and evaluates skills gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense's platform information technologies; and

(ii) Recommends curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

(c) Within 1 year of the date of this order, the Secretary of Education, in consultation with the DAPHSCT and the National Science Foundation, shall develop and implement, consistent with applicable law, an annual Presidential Cybersecurity Education Award to be presented to one elementary and one secondary school educator per year who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects. In developing and implementing this award, the Secretary of Education shall emphasize demonstrated superior educator accomplishment—without respect to research, scholarship, or technology development—as well as academic achievement by the educator's students.

(d) The Secretary of Commerce, the Secretary of Labor, the Secretary of Education, the Secretary of Homeland Security, and the heads of other appropriate agencies shall encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law. The Secretary of Commerce shall provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

SEC. 4. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

SUBCHAPTER I—CYBERSECURITY INFORMATION SHARING

§1500. National Cyber Director

(a) Establishment

There is established, within the Executive Office of the President, the Office of the National Cyber Director (in this section referred to as the "Office").

(b) National Cyber Director

(1) In general

The Office shall be headed by the National Cyber Director (in this section referred to as the

"Director") who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) Position

The Director shall hold office at the pleasure of the President.

(3) Pay and allowances

The Director shall be entitled to receive the same pay and allowances as are provided for level II of the Executive Schedule under section 5313 of title 5.

(c) Duties of the National Cyber Director

(1) In general

Subject to the authority, direction, and control of the President, the Director shall—

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of—

(i) information security and data protection;

(ii) programs and policies intended to improve the cybersecurity posture of the United States;

(iii) efforts to understand and deter malicious cyber activity;

(iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

(vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and

(vii) such other cybersecurity matters as the President considers appropriate;

(B) offer advice and consultation to the National Security Council and its staff, the Homeland Security Council and its staff, and relevant Federal departments and agencies, for their consideration, relating to the development and coordination of national cyber policy and strategy, including the National Cyber Strategy;

(C) lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy, by—

(i) in coordination with the heads of relevant Federal departments or agencies, monitoring and assessing the effectiveness, including cost-effectiveness, of the implementation of such national cyber policy and strategy by Federal departments and agencies;

(ii) making recommendations, relevant to changes in the organization, personnel, and resource allocation and to policies of Federal departments and agencies, to the heads of relevant Federal departments and agencies in order to implement such national cyber policy and strategy;

(iii) reviewing the annual budget proposals for relevant Federal departments and agencies and advising the heads of such departments and agencies whether such proposals are consistent with such national cyber policy and strategy;

(iv) continuously assessing and making relevant recommendations to the President on the appropriate level of integration and interoperability across the Federal cyber centers;

(v) coordinating with the Attorney General, the Federal Chief Information Officer, the Director of the Office of Management and Budget, the Director of National Intelligence, and the Director of the Cybersecurity and Infrastructure Security Agency, on the streamlining of Federal policies and guidelines, including with respect to implementation of subchapter II of chapter 35 of title 44, and, as appropriate or applicable, regulations relating to cybersecurity;

(vi) reporting annually to the President, the Assistant to the President for National Security Affairs, and Congress on the state of the cybersecurity posture of the United States, the effectiveness of such national cyber policy and strategy, and the status of the implementation of such national cyber policy and strategy by Federal departments and agencies; and

(vii) such other activity as the President considers appropriate to further such national cyber policy and strategy;

(D) lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, including—

(i) ensuring and facilitating coordination among relevant Federal departments and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response, that feature—

(I) clear lines of authority and lines of effort across the Federal Government;

(II) authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government; and

(III) support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States;

(ii) ensuring the exercising of defensive operational plans, processes, and playbooks for incident response;

(iii) ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and

(iv) reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private sector entities, as appropriate;

(E) preparing the response by the Federal Government to cyberattacks and cyber campaigns of significant consequence across Federal departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private sector entities, including—

(i) developing for the approval of the President, in coordination with the Assistant to the President for National Security Affairs and the heads of relevant Federal departments and agencies, operational priorities, requirements, and plans;

(ii) ensuring incident response is executed consistent with the plans described in clause (i); and

(iii) ensuring relevant Federal department and agency consultation with relevant private sector entities in incident response;

(F) coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate;

(G) annually report to Congress on cybersecurity threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law; and

(H) be responsible for such other functions as the President may direct.

(2) Delegation of authority

(A) The Director may—

(i) serve as the senior representative to any organization that the President may establish for the purpose of providing the President advice on cybersecurity;

(ii) subject to subparagraph (B), be included as a participant in preparations for and, when appropriate, the execution of domestic and international summits and other international meetings at which cybersecurity is a major topic;

(iii) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate; and

(iv) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate.

(B) In acting under subparagraph (A)(ii) in the case of a summit or a meeting with an international partner, the Director shall act in coordination with the Secretary of State.

(d) Omitted

(e) Powers of the Director

(1) In general

The Director may, for the purposes of carrying out the functions of the Director under this section—

(A) subject to the civil service and classification laws, select, appoint, employ, and fix the compensation of such officers and employees as are necessary and prescribe their duties, except that not more than 75 individuals may be employed without regard to any provision of law regulating the employment or compensation at rates not to exceed the basic rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5;

(B) employ experts and consultants in accordance with section 3109 of title 5, and compensate individuals so employed for each day (including travel time) at rates not in excess of the maximum rate of basic pay for grade GS–15 as provided in section 5332 of such title, and while such experts and consultants are so serving away from their homes or regular place of business, to pay such employees travel expenses and per diem in lieu of subsistence at rates authorized by section 5703 of such title 5 for persons in Federal Government service employed intermittently;

(C) accept officers or employees of the United States or members of the Armed Forces on a detail from an element of the intelligence community (as such term is defined in section 3003(4) of title 50) or from another element of the Federal Government on a nonreimbursable basis, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed three years;

(D) promulgate such rules and regulations as may be necessary to carry out the functions, powers, and duties vested in the Director;

(E) utilize, with their consent, the services, personnel, and facilities of other Federal agencies;

(F) enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary in the conduct of the work of the Office and on such terms as the Director may determine appropriate, with any Federal agency, or with any public or private person or entity;

(G) accept voluntary and uncompensated services, notwithstanding the provisions of section 1342 of title 31;

(H) adopt an official seal, which shall be judicially noticed; and

(I) provide, where authorized by law, copies of documents to persons at cost, except that any funds so received shall be credited to, and be available for use from, the account from which expenditures relating thereto were made.

(2) Rules of construction regarding details

Nothing in paragraph (1)(C) may be construed as imposing any limitation on any other authority for reimbursable or nonreimbursable details. A nonreimbursable detail made pursuant to such paragraph shall not be considered an augmentation of the appropriations of the receiving element of the Office of the National Cyber Director.

(f) Rules of construction

Nothing in this section may be construed as—

(1) modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency;

(2) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation;

(3) amending a legal restriction that was in effect on the day before January 1, 2021 that

requires a law enforcement agency to keep confidential information learned in the course of a criminal or national security investigation;

(4) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a military operation;

(5) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct any diplomatic or consular activity;

(6) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct an intelligence activity, resource, or operation; or

(7) authorizing the Director or any person acting under the authority of the Director to modify the classification of intelligence information.

(g) Definitions

In this section:

(1) The term "cybersecurity posture" means the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or cyber campaign of significant consequence.

(2) The term "cyber attack and cyber campaign of significant consequence" means an incident or series of incidents that has the purpose or effect of—

(A) causing a significant disruption to the confidentiality, integrity, or availability of a Federal information system;

(B) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(C) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) otherwise constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

(3) The term "incident" has the meaning given such term in section 3552 of title 44.

(4) The term "incident response" means a government or private sector activity that detects, mitigates, or recovers from a cyber attack or cyber campaign of significant consequence.

(5) The term "information security" has the meaning given such term in section 3552 of title 44.

(6) The term "intelligence" has the meaning given such term in section 3003 of title 50.

(Pub. L. 116–283, div. A, title XVII, §1752, Jan. 1, 2021, 134 Stat. 4144; Pub. L. 117–81, div. A, title XV, §1552, Dec. 27, 2021, 135 Stat. 2070.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Cybersecurity Information Sharing Act of 2015 which comprises this subchapter and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

Section is comprised of section 1752 of Pub. L. 116–283. Subsec. (d) of section 1752 of Pub. L. 116–283 amended section 3021 of Title 50, War and National Defense.

AMENDMENTS

2021—Subsec. (e). Pub. L. 117–81, §1552(1), (2), (4), designated existing provisions as par. (1) and inserted heading, redesignated former pars. (1) to (8) as subpars. (A) to (H), respectively, of par. (1) and realigned margins, and added par. (2).

Subsec. (e)(1)(C) to (I). Pub. L. 117–81, §1552(3), added subpar. (C) and redesignated former subpars. (C) to (H) (as redesignated by section 1552(1) of Pub. L. 117–81, see above) as (D) to (I), respectively.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE OF 2022 AMENDMENT

Pub. L. 117–260, §1, Dec. 21, 2022, 136 Stat. 2389, provided that: "This Act [enacting section 1526 of this title and provisions set out as notes under section 1526 of this title] may be cited as the 'Quantum Computing Cybersecurity Preparedness Act'."

§1501. Definitions

In this subchapter:

(1) Agency

The term "agency" has the meaning given the term in section 3502 of title 44.

(2) Antitrust laws

The term "antitrust laws"—

(A) has the meaning given the term in section 12 of title 15;

(B) includes section 45 of title 15 to the extent that section 45 of title 15 applies to unfair methods of competition; and

(C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) or the law referred to in subparagraph (B).

(3) Appropriate Federal entities

The term "appropriate Federal entities" means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) Cybersecurity purpose

The term "cybersecurity purpose" has the meaning given the term in section 650 of this title.

(5) Cybersecurity threat

The term "cybersecurity threat" has the meaning given the term in section 650 of this title.

(6) Cyber threat indicator

The term "cyber threat indicator" has the meaning given the term in section 650 of this title.

(7) Defensive measure

The term "defensive measure" has the meaning given the term in section 650 of this title.

(8) Federal entity

The term "Federal entity" means a department or agency of the United States or any component of such department or agency.

(9) Information system

The term "information system" has the meaning given the term in section 650 of this title.

(10) Local government

The term "local government" means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(11) Malicious cyber command and control

The term "malicious cyber command and control" has the meaning given the term in section 650 of this title.

(12) Malicious reconnaissance

The term "malicious reconnaissance" has the meaning given the term in section 650 of this title.

(13) Monitor

The term "monitor" has the meaning given the term in section 650 of this title.

(14) Non-Federal entity

(A) In general

Except as otherwise provided in this paragraph, the term "non-Federal entity" means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) Inclusions

The term "non-Federal entity" includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) Exclusion

The term "non-Federal entity" does not include a foreign power as defined in section 1801 of title 50.

(15) Private entity

(A) In general

Except as otherwise provided in this paragraph, the term "private entity" means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) Inclusion

The term "private entity" includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) Exclusion

The term "private entity" does not include a foreign power as defined in section 1801 of title 50.

(16) Security control

The term "security control" has the meaning given the term in section 650 of this title.

(17) Security vulnerability

The term "security vulnerability" has the meaning given the term in section 650 of this title.

(18) Tribal

The term "tribal" has the meaning given the term "Indian tribe" in section 5304 of title 25.

(Pub. L. 114–113, div. N, title I, §102, Dec. 18, 2015, 129 Stat. 2936; Pub. L. 117–263, div. G, title LXXI, §7143(b)(4), Dec. 23, 2022, 136 Stat. 3661.)

EDITORIAL NOTES

AMENDMENTS

2022—Pars. (4) to (7). Pub. L. 117–263, §7143(b)(4)(A), added pars. (4) to (7) and struck out former pars. (4) to (7) which defined cybersecurity purpose, cybersecurity threat, cyber threat indicator, and defensive measure, respectively.

Par. (9). Pub. L. 117–263, §7143(b)(4)(B), added par. (9) and struck out former par. (9) which defined information system.

Pars. (11) to (13). Pub. L. 117–263, §7143(b)(4)(C), added pars. (11) to (13) and struck out former pars.

(11) to (13) which defined malicious cyber command and control, malicious reconnaissance, and monitor, respectively.

Pars. (16), (17). Pub. L. 117–263, §7143(b)(4)(D), added pars. (16) and (17) and struck out former pars. (16) and (17) which defined security control and security vulnerability, respectively.

STATUTORY NOTES AND RELATED SUBSIDIARIES

SHORT TITLE

Pub. L. 114–113, div. N, §1(a), Dec. 18, 2015, 129 Stat. 2935, provided that: "This division [enacting this chapter and sections 149 and 151 of this title, amending sections 131, 148, 149, and 150 of this title, section 1029 of Title 18, Crimes and Criminal Procedure, and sections 3553 and 3554 of Title 44, Public Printing and Documents, enacting provisions set out as notes under this section and sections 101, 131, and 151 of this title and section 301 of Title 5, Government Organization and Employees] may be cited as the 'Cybersecurity Act of 2015'."

Pub. L. 114–113, div. N, title I, §101, Dec. 18, 2015, 129 Stat. 2936, provided that: "This title [enacting this subchapter] may be cited as the 'Cybersecurity Information Sharing Act of 2015'."

Pub. L. 114–113, div. N, title II, §221, Dec. 18, 2015, 129 Stat. 2963, provided that: "This subtitle [subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, enacting subchapter II of this chapter and sections 149 and 151 of this title, amending sections 148, 149, and 150 of this title and sections 3553 and 3554 of Title 44, Public Printing and Documents, and enacting provisions set out as a note under section 151 of this title] may be cited as the 'Federal Cybersecurity Enhancement Act of 2015'."

§1502. Sharing of information by the Federal Government

(a) In general

Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;

(2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;

(4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 632 of title 15).

(b) Development of procedures

(1) In general

The procedures developed under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified

information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, Federal entities and non-Federal entities that have received a cyber threat indicator or defensive measure from a Federal entity under this subchapter that is known or determined to be in error or in contravention of the requirements of this subchapter or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this subchapter.

(2) Consultation

In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 15801 of title 42), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) Submittal to Congress

Not later than 60 days after December 18, 2015, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

(Pub. L. 114–113, div. N, title I, §103, Dec. 18, 2015, 129 Stat. 2939.)

§1503. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats

(a) Authorization for monitoring

(1) In general

Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of

an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) Construction

Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this subchapter; or

(B) to limit otherwise lawful activity.

(b) Authorization for operation of defensive measures

(1) In general

Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) Construction

Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) Authorization for sharing or receiving cyber threat indicators or defensive measures

(1) In general

Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

(2) Lawful restriction

A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

(3) Construction

Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) Protection and use of information

(1) Security of information

A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) Removal of certain personal information

A non-Federal entity sharing a cyber threat indicator pursuant to this subchapter shall, prior to

such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

(3) Use of cyber threat indicators and defensive measures by non-Federal entities

(A) In general

Consistent with this subchapter, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by a non-Federal entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the non-Federal entity; or

(II) an information system of another non-Federal entity or a Federal entity upon the written consent of that other non-Federal entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by a non-Federal entity subject to—

(I) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) Construction

Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) Use of cyber threat indicators by State, tribal, or local government

(A) Law enforcement use

A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this subchapter may use such cyber threat indicator or defensive measure for the purposes described in section 1504(d)(5)(A) of this title.

(B) Exemption from disclosure

A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

(C) State, tribal, and local regulatory authority

(i) In general

Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this subchapter shall not be used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-Federal entity or any activity taken by a non-Federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats

A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) Antitrust exemption

(1) In general

Except as provided in section 1507(e) of this title, it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this subchapter.

(2) Applicability

Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) No right or benefit

The sharing of a cyber threat indicator or defensive measure with a non-Federal entity under this subchapter shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

(Pub. L. 114–113, div. N, title I, §104, Dec. 18, 2015, 129 Stat. 2940.)

§1504. Sharing of cyber threat indicators and defensive measures with the Federal Government

(a) Requirement for policies and procedures

(1) Interim policies and procedures

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) Final policies and procedures

Not later than 180 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly issue and make publicly available final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(3) Requirements concerning policies and procedures

Consistent with the guidelines required by subsection (b), the policies and procedures developed or issued under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 1503(c) of this title through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal

entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 1503 of this title in a manner other than the real-time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities; and

(C) ensure there are—

(i) audit capabilities; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this subchapter in an unauthorized manner.

(4) Guidelines for entities sharing cyber threat indicators with Federal Government

(A) In general

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall jointly develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this subchapter.

(B) Contents

The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this subchapter that would be unlikely to include information that—

(I) is not directly related to a cybersecurity threat; and

(II) is personal information of a specific individual or information that identifies a specific individual.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this subchapter.

(b) Privacy and civil liberties

(1) Interim guidelines

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with heads of the appropriate Federal entities and in consultation with officers designated under section 2000ee–1 of title 42, jointly develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this subchapter.

(2) Final guidelines

(A) In general

Not later than 180 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 2000ee–1 of title 42 and such private entities with industry expertise as the Attorney General and the Secretary consider relevant, jointly issue and make publicly available final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this subchapter.

(B) Periodic review

The Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every 2 years, jointly review the guidelines issued under subparagraph (A).

(3) Content

The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this subchapter;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this subchapter; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) consistent with this subchapter, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this subchapter, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government;

(E) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(F) protect the confidentiality of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this subchapter; and

(G) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) Capability and process within the Department of Homeland Security

(1) In general

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any non-Federal entity in real time cyber threat indicators and

defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this subchapter that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 1503 of this title, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) Certification and designation

(A) Certification of capability and process

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, submit to Congress a certification as to whether the capability and process required by paragraph (1) fully and effectively operates—

(i) as the process by which the Federal Government receives from any non-Federal entity a cyber threat indicator or defensive measure under this subchapter; and

(ii) in accordance with the interim policies, procedures, and guidelines developed under this subchapter.

(B) Designation

(i) In general

At any time after certification is submitted under subparagraph (A), the President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1) in addition to the capability and process developed under such paragraph by the Secretary of Homeland Security, if, not fewer than 30 days before making such designation, the President submits to Congress a certification and explanation that—

(I) such designation is necessary to ensure that full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this subchapter;

(II) the designated appropriate Federal entity will receive and share cyber threat indicators and defensive measures in accordance with the policies, procedures, and

guidelines developed under this subchapter, including subsection (a)(3)(A); and

(III) such designation is consistent with the mission of such appropriate Federal entity and improves the ability of the Federal Government to receive, share, and use cyber threat indicators and defensive measures as authorized under this subchapter.

(ii) Application to additional capability and process

If the President designates an appropriate Federal entity to develop and implement a capability and process under clause (i), the provisions of this subchapter that apply to the capability and process required by paragraph (1) shall also be construed to apply to the capability and process developed and implemented under clause (i).

(3) Public notice and access

The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any non-Federal entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security consistent with the policies and procedures issued under subsection (a).

(4) Other Federal entities

The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(d) Information shared with or provided to the Federal Government

(1) No waiver of privilege or protection

The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) Proprietary information

Consistent with section 1503(c)(2) of this title and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this subchapter shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity.

(3) Exemption from disclosure

A cyber threat indicator or defensive measure shared with the Federal Government under this subchapter shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) Ex parte communications

The provision of a cyber threat indicator or defensive measure to the Federal Government under this subchapter shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) Disclosure, retention, and use

(A) Authorized activities

Cyber threat indicators and defensive measures provided to the Federal Government under

this subchapter may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying—

(I) a cybersecurity threat, including the source of such cybersecurity threat; or

(II) a security vulnerability;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18 (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) Prohibited activities

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) Privacy and civil liberties

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual.

(D) Federal regulatory authority

(i) In general

Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) Exceptions

(I) Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information

systems, inform the development or implementation of regulations relating to such information systems.

(II) Procedures developed and implemented under this subchapter

Clause (i) shall not apply to procedures developed and implemented under this subchapter.

(Pub. L. 114–113, div. N, title I, §105, Dec. 18, 2015, 129 Stat. 2943.)

§1505. Protection from liability

(a) Monitoring of information systems

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 1503(a) of this title that is conducted in accordance with this subchapter.

(b) Sharing or receipt of cyber threat indicators

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c) of this title if—

(1) such sharing or receipt is conducted in accordance with this subchapter; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 1504(c)(1)(B) of this title and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 1504(a)(1) of this title and guidelines are submitted to Congress under section 1504(b)(1) of this title; or

(B) the date that is 60 days after December 18, 2015.

(c) Construction

Nothing in this subchapter shall be construed—

(1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(Pub. L. 114–113, div. N, title I, §106, Dec. 18, 2015, 129 Stat. 2950.)

§1506. Oversight of government activities

(a) Report on implementation

(1) In general

Not later than 1 year after December 18, 2015, the heads of the appropriate Federal entities shall jointly submit to Congress a detailed report concerning the implementation of this subchapter.

(2) Contents

The report required by paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities, policies, procedures, and guidelines under this subchapter and shall include the following:

(A) An evaluation of the effectiveness of real-time information sharing through the capability

and process developed under section 1504(c) of this title, including any impediments to such real-time sharing.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 1504(c) of this title.

(D) A list of Federal entities that have received cyber threat indicators or defensive measures under this subchapter.

(b) Biennial report on compliance

(1) In general

Not later than 2 years after December 18, 2015 and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this subchapter during the most recent 2-year period.

(2) Contents

Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this subchapter, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this subchapter, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 1504(c) of this title.

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government [1] entity with the Federal government [1] in contravention of this subchapter, or was shared within the Federal Government in contravention of the guidelines required by this subchapter, including a description of any significant violation of this subchapter.

(iii) The number of times, according to the Attorney General, that information shared under this subchapter was used by a Federal entity to prosecute an offense listed in section 1504(d)(5)(A) of this title.

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 1504(b)(3)(E) of this title.

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this subchapter on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) Recommendations

Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this subchapter.

(c) Independent report on removal of personal information

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this subchapter. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this subchapter in addressing concerns relating to privacy and civil liberties.

(d) Form of reports

Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) Public availability of reports

The unclassified portions of the reports required under this section shall be made available to the public.

(Pub. L. 114–113, div. N, title I, §107, Dec. 18, 2015, 129 Stat. 2951.)

[1] *So in original. Probably should be capitalized.*

§1507. Construction and preemption

(a) Otherwise lawful disclosures

Nothing in this subchapter shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this subchapter; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter.

(b) Whistle blower protections

Nothing in this subchapter shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5 (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5 (governing disclosures to Congress), section 1034 of title 10 (governing disclosure to Congress by members of the military), section 3234 of title 50 (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) Protection of sources and methods

Nothing in this subchapter shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) Relationship to other laws

Nothing in this subchapter shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(e) Prohibited conduct

Nothing in this subchapter shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) Information sharing relationships

Nothing in this subchapter shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 1504(c) of this title.

(g) Preservation of contractual obligations and rights

Nothing in this subchapter shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

(h) Anti-tasking restriction

Nothing in this subchapter shall be construed to permit a Federal entity—

(1) to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity;

(2) to condition the sharing of cyber threat indicators with a non-Federal entity on such entity's provision of cyber threat indicators to a Federal entity or another non-Federal entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another non-Federal entity.

(i) No liability for non-participation

Nothing in this subchapter shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this subchapter.

(j) Use and retention of information

Nothing in this subchapter shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this subchapter for any use other than permitted in this subchapter.

(k) Federal preemption

(1) In general

This subchapter supersedes any statute or other provision of law of a State or political

subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this subchapter.

(2) State law enforcement

Nothing in this subchapter shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) Regulatory authority

Nothing in this subchapter shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized to be issued under this subchapter;

(2) to establish or limit any regulatory authority not specifically established or limited under this subchapter; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) Authority of Secretary of Defense to respond to malicious cyber activity carried out by foreign powers

Nothing in this subchapter shall be construed to limit the authority of the Secretary of Defense under section 394 of title 10.

(n) Criminal prosecution

Nothing in this subchapter shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this subchapter in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.

(Pub. L. 114–113, div. N, title I, §108, Dec. 18, 2015, 129 Stat. 2953; Pub. L. 115–232, div. A, title XVI, §1631(b), Aug. 13, 2018, 132 Stat. 2123.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (m). Pub. L. 115–232 substituted "section 394" for "section 130g".

§1508. Report on cybersecurity threats

(a) Report required

Not later than 180 days after December 18, 2015, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) Contents

The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual

property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) Form of report

The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) Intelligence community defined

In this section, the term "intelligence community" has the meaning given that term in section 3003 of title 50.

(Pub. L. 114–113, div. N, title I, §109, Dec. 18, 2015, 129 Stat. 2955.)

§1509. Exception to limitation on authority of Secretary of Defense to disseminate certain information

Notwithstanding subsection (c)(3) of section 393 of title 10, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this subchapter.

(Pub. L. 114–113, div. N, title I, §110, Dec. 18, 2015, 129 Stat. 2956.)

§1510. Effective period

(a) In general

Except as provided in subsection (b), this subchapter and the amendments made by this subchapter shall be effective during the period beginning on December 18, 2015 and ending on December 11, 2026.

(b) Exception

With respect to any action authorized by this subchapter or information obtained pursuant to an action authorized by this subchapter, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this subchapter shall continue in effect.

(Pub. L. 114–113, div. N, title I, §111, Dec. 18, 2015, 129 Stat. 2956; Pub. L. 119–75, div. I, §5008, Feb. 3, 2026, 140 Stat. 630; Pub. L. 119–103, div. B, §2011, Sept. 2, 2026, 140 Stat. 1001.)

EDITORIAL NOTES

REFERENCES IN TEXT

The amendments made by this subchapter, referred to in subsec. (a), was in the original "the amendments made by this title", meaning title I of div. N of Pub. L. 114–113, which is classified generally to this subchapter.

AMENDMENTS

2026—Subsec. (a). Pub. L. 119–103 substituted "December 11, 2026" for "September 30, 2026".
Pub. L. 119–75 substituted "September 30, 2026" for "September 30, 2025".

SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT

§1521. Definitions

In this subchapter:

(1) Agency

The term "agency" has the meaning given the term in section 3502 of title 44.

(2) Agency information system

The term "agency information system" has the meaning given the term in section 660 of this title.

(3) Appropriate congressional committees

The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(4) Cybersecurity risk; information system

The terms "cybersecurity risk" and "information system" have the meanings given those terms in section 650 of this title.

(5) Director

The term "Director" means the Director of the Office of Management and Budget.

(6) Intelligence community

The term "intelligence community" has the meaning given the term in section 3003(4) of title 50.

(7) National security system

The term "national security system" has the meaning given the term in section 11103 of title 40.

(8) Secretary

The term "Secretary" means the Secretary of Homeland Security.

(Pub. L. 114–113, div. N, title II, §222, Dec. 18, 2015, 129 Stat. 2963; Pub. L. 115–278, §2(h)(1)(D), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–263, div. G, title LXXI, §7143(d)(1)(A), Dec. 23, 2022, 136 Stat. 3663.)

EDITORIAL NOTES

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, which is classified principally to this subchapter. For complete classification of subtitle B to the Code, see Tables.

AMENDMENTS

2022—Par. (4). Pub. L. 117–263 substituted "section 650 of this title" for "section 659 of this title".

2018—Par. (2). Pub. L. 115–278, §2(h)(1)(D)(i), substituted "section 660 of this title" for "section 149 of this title, as added by section 223(a)(4) of this division".

Par. (4). Pub. L. 115–278, §2(h)(1)(D)(ii), substituted "section 659 of this title" for "section 148 of this title, as so redesignated by section 223(a)(3) of this division".

§1522. Advanced internal defenses

(a) Advanced network security tools

(1) In general

The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

(2) Development of plan

The Director shall develop and the Secretary shall implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) Prioritizing advanced security tools

The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) Improved metrics

The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44 to include measures of intrusion and incident detection and response times.

(d) Transparency and accountability

The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro-agencies.

(e) Omitted

(f) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, §224, Dec. 18, 2015, 129 Stat. 2967.)

EDITORIAL NOTES

CODIFICATION

Section is comprised of section 224 of title II of div. N of Pub. L. 114–113. Subsec. (e) of section 224 of title II of div. N of Pub. L. 114–113 amended section 3553 of Title 44, Public Printing and Documents.

§1523. Federal cybersecurity requirements

(a) Implementation of Federal cybersecurity standards

Consistent with section 3553 of title 44, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40 [1] for securing agency information systems.

(b) Cybersecurity requirements at agencies

(1) In general

Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section

11331 of title 40 and except as provided in paragraph (2), not later than 1 year after December 18, 2015, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 7464 of title 15, including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) Exception

The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) Construction

Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, §225, Dec. 18, 2015, 129 Stat. 2967.)

EDITORIAL NOTES

REFERENCES IN TEXT

The text of section 11331 of title 40, referred to in subsec. (a), was generally amended by Pub. L. 117–167, div. B, title II, §10246(f), Aug. 9, 2022, 136 Stat. 1492, so as to provide for the prescription by the Secretary of Commerce of standards and guidelines pertaining to Federal information systems.

[1] *See References in Text note below.*

§1524. Assessment; reports

(a) Definitions

In this section:

(1) Agency information

The term "agency information" has the meaning given the term in section 2213 of the Homeland Security Act of 2002 [6 U.S.C. 663].

(2) Cyber threat indicator; defensive measure

The terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 650 of this title.

(3) Intrusion assessments

The term "intrusion assessments" means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems.

(4) Intrusion assessment plan

The term "intrusion assessment plan" means the plan required under section 2210(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 660(b)(1)].

(5) Intrusion detection and prevention capabilities

The term "intrusion detection and prevention capabilities" means the capabilities required under section 2213(b) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)].

(b) Third-party assessment

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) Reports to Congress

(1) Intrusion detection and prevention capabilities

(A) Secretary of Homeland Security report

Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention

capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 2213(c)(5) of the Homeland Security Act of 2002 [6 U.S.C. 663(c)(5)], including the number of new technologies tested and the number of participating agencies.

(B) OMB report

Not later than 18 months after December 18, 2015, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(C) Chief information officer

Not earlier than 18 months after December 18, 2015, and not later than 2 years after December 18, 2015, the Federal Chief Information Officer shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities, including—

(i) the effectiveness of the system in detecting, disrupting, and preventing cyber-threat actors, including advanced persistent threats, from accessing agency information and agency information systems;

(ii) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed under subtitle D [1] of title II of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) are effective in securing Federal information systems;

(iii) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools and including the value of classified cyber threat indicators; and

(iv) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

(2) OMB report on development and implementation of intrusion assessment plan, advanced internal defenses, and Federal cybersecurity requirements

The Director shall—

(A) not later than 6 months after December 18, 2015, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after December 18, 2015, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) a description of the advanced network security tools included in the efforts to continuously diagnose and mitigate cybersecurity risks pursuant to section 1522(a)(1) of this title; and

(iv) a list by agency of compliance with the requirements of section 1523(b) of this title; and

(C) not later than 1 year after December 18, 2015, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 1522(a)(2) of this title; and

(ii) the improved metrics developed pursuant to section 1522(c) of this title.

(d) Form

Each report required under this section shall be submitted in unclassified form, but may include a classified annex.

(Pub. L. 114–113, div. N, title II, §226, Dec. 18, 2015, 129 Stat. 2969; Pub. L. 115–278, §2(h)(1)(F), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–263, div. G, title LXXI, §7143(d)(1)(B), Dec. 23, 2022, 136 Stat. 3663.)

EDITORIAL NOTES

REFERENCES IN TEXT

Subtitle D of title II of the Homeland Security Act of 2002, referred to in subsec. (c)(1)(C)(ii), is subtitle D (§§231–237) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2159, which enacted part D (§161 et seq.) of subchapter II of chapter 1 of this title and amended sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement. Subtitle D was redesignated subtitle C of title II of the Homeland Security Act of 2002 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and is classified principally to part C (§161 et seq.) of subchapter II of chapter 1 of this title. For complete classification of subtitle C to the Code, see Tables.

AMENDMENTS

2022—Subsec. (a)(2). Pub. L. 117–263 substituted "section 650 of this title" for "section 1501 of this title".

2018—Subsec. (a)(1). Pub. L. 115–278, §2(h)(1)(F)(i)(I), substituted "section 2213" for "section 230" and struck out before period at end ", as added by section 223(a)(6) of this division".

Subsec. (a)(4). Pub. L. 115–278, §2(h)(1)(F)(i)(II), substituted "section 2210(b)(1)" for "section 228(b)(1)" and struck out before period at end ", as added by section 223(a)(4) of this division".

Subsec. (a)(5). Pub. L. 115–278, §2(h)(1)(F)(i)(III), substituted "section 2213(b)" for "section 230(b)" and struck out before period at end ", as added by section 223(a)(6) of this division".

Subsec. (c)(1)(A)(vi). Pub. L. 115–278, §2(h)(1)(F)(ii), substituted "section 2213(c)(5)" for "section 230(c)(5)" and struck out ", as added by section 223(a)(6) of this division" after "Homeland Security Act of 2002".

[1] *See References in Text note below.*

§1525. Termination

(a) In general

The authority provided under section 663 of this title, and the reporting requirements under section 1524(c) of this title shall terminate on December 11, 2026.

(b) Rule of construction

Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 663(d)(2) [1] of this title, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

(Pub. L. 114–113, div. N, title II, §227, Dec. 18, 2015, 129 Stat. 2971; Pub. L. 115–278, §2(h)(1)(G), Nov. 16, 2018, 132 Stat. 4182; Pub. L. 117–328, div. O, title I, §101, Dec. 29, 2022, 136 Stat. 5226; Pub. L. 118–47, div. G, title I, §106, Mar. 23, 2024, 138 Stat. 857; Pub. L. 118–83, div. B, title I, §103, Sept. 26, 2024, 138 Stat. 1534; Pub. L. 118–158, div. E, §5104, Dec. 21, 2024, 138 Stat. 1771;

Pub. L. 119–4, div. C, §3104, Mar. 15, 2025, 139 Stat. 46; Pub. L. 119–75, div. I, §5007, Feb. 3, 2026, 140 Stat. 630; Pub. L. 119–103, div. B, §2012, Sept. 2, 2026, 140 Stat. 1002.)

EDITORIAL NOTES

AMENDMENTS

2026—Subsec. (a). Pub. L. 119–103 substituted "December 11, 2026" for "September 30, 2026".
Pub. L. 119–75 substituted "September 30, 2026" for "September 30, 2025".
2025—Subsec. (a). Pub. L. 119–4 substituted "September 30, 2025" for "March 14, 2025".
2024—Subsec. (a). Pub. L. 118–158 substituted "March 14, 2025" for "December 20, 2024".
Pub. L. 118–83 substituted "December 20, 2024" for "September 30, 2024".
Pub. L. 118–47 substituted "September 30, 2024" for "September 30, 2023".
2022—Subsec. (a). Pub. L. 117–328 substituted "September 30, 2023" for "the date that is 7 years after December 18, 2015".
2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(G)(i), substituted "section 663 of this title" for "section 151 of this title, as added by section 223(a)(6) of this division,".
Subsec. (b). Pub. L. 115–278, §2(h)(1)(G)(ii), substituted "section 663(d)(2) of this title" for "section 151(d)(2) of this title, as added by section 223(a)(6) of this division,".

[1] *So in original. Probably should be "663(c)(2)".*

§1526. Inventory of cryptographic systems; migration to post-quantum cryptography

(a) Inventory

(1) Establishment

Not later than 180 days after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall issue guidance on the migration of information technology to post-quantum cryptography, which shall include at a minimum—

(A) a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers, prioritized using the criteria described in subparagraph (B);

(B) criteria to allow agencies to prioritize their inventory efforts; and

(C) a description of the information required to be reported pursuant to subsection (b).

(2) Additional content in guidance

In the guidance established by paragraph (1), the Director of OMB shall include, in addition to the requirements described in that paragraph—

(A) a description of information technology to be prioritized for migration to post-quantum cryptography; and

(B) a process for evaluating progress on migrating information technology to post-quantum cryptography, which shall be automated to the greatest extent practicable.

(3) Periodic updates

The Director of OMB shall update the guidance required under paragraph (1) as the Director of OMB determines necessary, in coordination with the National Cyber Director and in consultation with the Director of CISA.

(b) Agency reports

Not later than 1 year after December 21, 2022, and on an ongoing basis thereafter, the head of each agency shall provide to the Director of OMB, the Director of CISA, and the National Cyber Director—

(1) the inventory described in subsection (a)(1); and
(2) any other information required to be reported under subsection (a)(1)(C).

(c) Migration and assessment

Not later than 1 year after the date on which the Director of NIST has issued post-quantum cryptography standards, the Director of OMB shall issue guidance requiring each agency to—

(1) prioritize information technology described under subsection (a)(2)(A) for migration to post-quantum cryptography; and

(2) develop a plan to migrate information technology of the agency to post-quantum cryptography consistent with the prioritization under paragraph (1).

(d) Interoperability

The Director of OMB shall ensure that the prioritizations made under subsection (c)(1) are assessed and coordinated to ensure interoperability.

(e) Office of Management and Budget reports

(1) Report on post-quantum cryptography

Not later than 15 months after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report on the following:

(A) A strategy to address the risk posed by the vulnerabilities of information technology of agencies to weakened encryption due to the potential and possible capability of a quantum computer to breach that encryption.

(B) An estimate of the amount of funding needed by agencies to secure the information technology described in subsection (a)(1)(A) from the risk posed by an adversary of the United States using a quantum computer to breach the encryption of the information technology.

(C) A description of Federal civilian executive branch coordination efforts led by the National Institute of Standards and Technology, including timelines, to develop standards for post-quantum cryptography, including any Federal Information Processing Standards developed under chapter 35 of title 44, as well as standards developed through voluntary, consensus standards bodies such as the International Organization for Standardization.

(2) Report on migration to post-quantum cryptography in information technology

Not later than 1 year after the date on which the Director of OMB issues guidance under subsection (c)(2), and thereafter until the date that is 5 years after the date on which post-quantum cryptographic standards are issued, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, with the report submitted pursuant to section 3553(c) of title 44, a report on the progress of agencies in adopting post-quantum cryptography standards.

(Pub. L. 117–260, §4, Dec. 21, 2022, 136 Stat. 2390.)

EDITORIAL NOTES

CODIFICATION

Section was enacted as part of the Quantum Computing Cybersecurity Preparedness Act, and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress,

Jan. 9, 2023. Committee on Oversight and Accountability of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 5, One Hundred Nineteenth Congress, Jan. 3, 2025.

FINDINGS; SENSE OF CONGRESS

Pub. L. 117–260, §2, Dec. 21, 2022, 136 Stat. 2389, provided that:

"(a) FINDINGS.—Congress finds the following:

"(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

"(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

"(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

"(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

"(b) SENSE OF CONGRESS.—It is the sense of Congress that—

"(1) a strategy for the migration of information technology of the Federal Government to post-quantum cryptography is needed; and

"(2) the governmentwide and industrywide approach to post-quantum cryptography should prioritize developing applications, hardware intellectual property, and software that can be easily updated to support cryptographic agility."

EXEMPTION OF NATIONAL SECURITY SYSTEMS

Pub. L. 117–260, §5, Dec. 21, 2022, 136 Stat. 2392, provided that: "This Act [see Short Title of 2022 Amendment note set out under section 1500 of this title] shall not apply to any national security system."

DEFINITIONS

Pub. L. 117–260, §3, Dec. 21, 2022, 136 Stat. 2389, provided that: "In this Act [see Short Title of 2022 Amendment note set out under section 1500 of this title]:

"(1) AGENCY .—The term 'agency'—

"(A) means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

"(B) does not include—

"(i) the Government Accountability Office; or

"(ii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions.

"(2) CLASSICAL COMPUTER.—The term 'classical computer' means a device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed and encodes information in binary bits that can either be 0s or 1s.

"(3) DIRECTOR OF CISA.—The term 'Director of CISA' means the Director of the Cybersecurity and Infrastructure Security Agency.

"(4) DIRECTOR OF NIST.—The term 'Director of NIST' means the Director of the National Institute of Standards and Technology.

"(5) DIRECTOR OF OMB.—The term 'Director of OMB' means the Director of the Office of Management and Budget.

"(6) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 3502 of title 44, United States Code.

"(7) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44, United States Code.

"(8) POST-QUANTUM CRYPTOGRAPHY.—The term 'post-quantum cryptography' means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a quantum computer or classical computer.

"(9) QUANTUM COMPUTER.—The term 'quantum computer' means a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations."

SUBCHAPTER III—OTHER CYBER MATTERS

§1531. Apprehension and prosecution of international cyber criminals

(a) International cyber criminal defined

In this section, the term "international cyber criminal" means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a "Red Notice") has been circulated by Interpol.

(b) Consultations for noncooperation

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) Annual report

(1) In general

The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) Form

The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) Appropriate congressional committees

For purposes of this subsection, the term "appropriate congressional committees" means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(Pub. L. 114–113, div. N, title IV, §403, Dec. 18, 2015, 129 Stat. 2979.)

§1532. Enhancement of emergency services

(a) Collection of data

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, acting through the center established under section 659 of this title, in coordination with appropriate Federal entities and the Assistant Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 101 of this title) within the State.

(b) Analysis of data

Not later than 1 year after December 18, 2015, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Assistant Director for Emergency Communications, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) Best practices

(1) In general

Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 272(e) of title 15.

(2) Report

The Director of the National Institute of Standards and Technology shall submit to Congress a report on the result of the activities of the Director under paragraph (1), including any methods developed by the Director under such paragraph, and shall make such report publicly available on the website of the National Institute of Standards and Technology.

(d) Rule of construction

Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require a non-Federal entity (as defined in section 1501 of this title) to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the result of the activities carried out under subsection (c), including any methods developed under such subsection.

(Pub. L. 114–113, div. N, title IV, §404, Dec. 18, 2015, 129 Stat. 2980; Pub. L. 115–278, §2(h)(1)(H), Nov. 16, 2018, 132 Stat. 4183.)

EDITORIAL NOTES

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(H), substituted "section 659 of this title" for "section 148 of this title, as redesignated by section 223(a)(3) of this division," and "Assistant Director for Emergency Communications" for "Director for Emergency Communications".

Subsec. (b). Pub. L. 115–278, §2(h)(1)(H)(ii), substituted "Assistant Director for Emergency Communications" for "Director for Emergency Communications".

STATUTORY NOTES AND RELATED SUBSIDIARIES

CHANGE OF NAME

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

§1533. Improving cybersecurity in the health care industry

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term "appropriate congressional committees" means—

(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) Business associate

The term "business associate" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

(3) Covered entity

The term "covered entity" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

(4) Cybersecurity threat; cyber threat indicator; defensive measure; Federal entity; non-Federal entity; private entity

The terms "cybersecurity threat", "cyber threat indicator", "defensive measure", "Federal entity", "non-Federal entity", and "private entity" have the meanings given such terms in section 1501 of this title.

(5) Health care clearinghouse; health care provider; health plan

The terms "health care clearinghouse", "health care provider", and "health plan" have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

(6) Health care industry stakeholder

The term "health care industry stakeholder" means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) advocate for patients or consumers;

(C) pharmacist;

(D) developer or vendor of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

(7) Secretary

The term "Secretary" means the Secretary of Health and Human Services.

(b) Report

(1) In general

Not later than 1 year after December 18, 2015, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and

Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.

(2) Contents of report

With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report under paragraph (1) shall include—

(A) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(B) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(c) Health care industry cybersecurity task force

(1) In general

Not later than 90 days after December 18, 2015, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing subchapter I of this chapter, so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) Termination

The task force established under this subsection shall terminate on the date that is 1 year after the date on which such task force is established.

(3) Dissemination

Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(d) Aligning health care industry security approaches

(1) In general

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 272(c)(15) of title 15;

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note); and

(iii) the provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111–5), and the amendments made by such Act; and

(D) are updated on a regular basis and applicable to a range of health care organizations.

(2) Limitation

Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase, on compliance with this subsection.

(3) No liability for nonparticipation

Nothing in this section shall be construed to subject a health care industry stakeholder to liability for choosing not to engage in the voluntary activities authorized or guidelines developed under this subsection.

(e) Incorporating ongoing activities

In carrying out the activities under this section, the Secretary may incorporate activities that are ongoing as of the day before December 18, 2015 and that are consistent with the objectives of this section.

(f) Rule of construction

Nothing in this section shall be construed to limit the antitrust exemption under section 1503(e) of this title or the protection from liability under section 1505 of this title.

(Pub. L. 114–113, div. N, title IV, §405, Dec. 18, 2015, 129 Stat. 2981.)

EDITORIAL NOTES

REFERENCES IN TEXT

Section 264(c) of the Health Insurance Portability and Accountability Act of 1996, referred to subsec. (d)(1)(C)(ii), is section 264(c) of Pub. L. 104–191, which is set out as a note under section 1320d–2 of Title 42, The Public Health and Welfare.

The Health Information Technology for Economic and Clinical Health Act, referred to in subsec. (d)(1)(C)(iii), is title XIII of div. A and title IV of div. B of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 226, 467, also known as the HITECH Act. For complete classification of this Act to the Code, see Short Title of 2009 Amendment note set out under section 201 of Title 42, The Public Health and Welfare, and Tables.

§1534. Cybercrime

Subject to the availability of appropriations, and in accordance with the comparable level of the General Schedule, the Attorney General and the Secretary of Homeland Security shall provide incentive pay, in an amount that is not more than 25 percent of the basic pay of the individual, to an

individual appointed to a position in the Department of Justice (including the Federal Bureau of Investigation) or the Department of Homeland Security (including positions in Homeland Security Investigations), respectively, requiring significant cyber skills, including to aid in—

(1) the protection of trafficking victims;

(2) the prevention of trafficking in persons; or

(3) the prosecution of technology-facilitated crimes against children by buyers or traffickers in persons.

(Pub. L. 117–347, title IV, §401, Jan. 5, 2023, 136 Stat. 6207.)

EDITORIAL NOTES

REFERENCES IN TEXT

The General Schedule, referred to in text, is set out under section 5332 of Title 5, Government Organization and Employees.

CODIFICATION

Section was enacted as part of the Abolish Trafficking Reauthorization Act of 2022, and not as part of the Cybersecurity Act of 2015 which comprises this chapter.