vice 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.)

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''.

DEFINITIONS

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

SUBCHAPTER II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

PART A—INFORMATION AND ANALYSIS AND INFRASTRUCTURE PROTECTION; ACCESS TO INFORMATION

CODIFICATION

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 and Infrastructure Protection

(a) Intelligence and analysis and infrastructure protection

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

(b) Under Secretary for Intelligence and Analysis and Assistant Secretary for Infrastructure Protection

(1) Office of Intelligence and Analysis

The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intel-

ligence 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.

(3) Office of Infrastructure Protection

The Office of Infrastructure Protection shall be headed by an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

(c) Discharge of responsibilities

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

(d) Responsibilities of Secretary relating to intelligence and analysis and infrastructure protection

The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection 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, 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 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) To ensure that—

(A) any material received pursuant to this chapter is protected from unauthorized dis-

closure 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.

(12) 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.

(13) 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.

(14) 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.

(15) 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.

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

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

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

(19) 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.

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

(21) 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.

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

(23) 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.

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

(25) 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.

(26)(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;[1]

(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 and the Office of Infrastructure Protection 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 and the Office of Infrastructure Protection 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.)

REFERENCES IN TEXT

This chapter, referred to in subsec. (d)(11), 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)(11)(B), is act July 26, 1947, ch. 343, 61 Stat. 495, which was formerly classified principally to chapter 15

[1] See References in Text note below.

(§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.

Section 195f of this title, referred to in subsec. (d)(26)(B)(i), was in the original ''section 319'', meaning section 319 of Pub. L. 107–296, the Homeland Security Act of 2002, and has been translated as meaning the section 319 of the Act as added by section 1913(a)(3) of Pub. L. 114–328 and relating to EMP and GMD mitigation research and development, and not the section 319 of the Act as added by section 1906(a) of Pub. L. 114–328, to reflect the probable intent of Congress.

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

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. 404*o*),'' 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.

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 section 621 of this title.]

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. 824*o*–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.''

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) of the Intelligence Reform and Terrorist [Terrorism] Prevention Act of 2004 (6 U.S.C. 485(j)(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.''

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, 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.

(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, 2019, by Ex. Ord. No. 13811, Sept. 29, 2017, 82 F.R. 46363, set out as a note under section 14 of the Federal Advisory Committee Act in the Appendix to 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. 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 ele-

ments 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 6 U.S.C. 143 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 6 U.S.C. 133 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.]

EXECUTIVE ORDER NO. 13650

Ex. Ord. No. 13650, Aug. 1, 2013, 78 F.R. 48029, was transferred to a note set out under 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.

§ 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.)

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 Central

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 Central 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.)

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.

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] 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

[1] See References in Text note below.

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.)

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.

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.''

§ 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 Assistant Secretary for Infrastructure Protection, 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 Assistant Secretary for Infrastructure Protection, 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 environ-

ment 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.)

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.

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(i) 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.)

§ 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 Initia-

[1] So in original. A closing parenthesis probably should precede the comma.

tive 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) Office of Infrastructure Protection.

(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, sup-

ported, 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 Secu-

rity 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) 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.

(k) 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.)

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.''

§ 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.)

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 program manager

The program manager shall—

(1) monitor and assess the efficacy of the ITACG;

(2) not later than 180 days after August 3, 2007, and at least annually thereafter, submit to the Secretary, the Attorney General, the Director of National Intelligence, 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 progress of the ITACG; and

(3) in each report required by paragraph (2) submitted after October 7, 2010, include an assessment of whether the detailees under subsection (d)(5) have appropriate access to all relevant information, as required by subsection (g)(2)(C).

(d) 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 informa-

tion 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; and

(9) provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2).

(e) 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.

(f) 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.

(g) 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), 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(f)(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) 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) 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) complete appropriate privacy and civil liberties training.

(h) Inapplicability of the Federal Advisory Committee Act

The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the ITACG or any subsidiary groups thereof.

(i) 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.)

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (h), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which is set out in the Appendix to Title 5, Government Organization and Employees.

AMENDMENTS

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).

§ 124*l*. 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

[1] So in original. Probably should be section ‘‘3056(f)(1)(E)’’.

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-specific 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) Inspector General study

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.

(f) 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 II, § 210E, as added Pub. L. 110–53, title X, § 1001(a), Aug. 3, 2007, 121 Stat. 372.)

DEADLINES FOR IMPLEMENTATION AND NOTIFICATION OF CONGRESS

Pub. L. 110–53, title X, § 1001(b), Aug. 3, 2007, 121 Stat. 374, provided that: ''Not later than 180 days after the

date of the enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall submit the first report required under section 210E(d) of the Homeland Security Act of 2002 [6 U.S.C. 124*l*(d)], as added by subsection (a).''

§ 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, § 210F, as added Pub. L. 111–258, § 4(a), Oct. 7, 2010, 124 Stat. 2649.)

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.''

§ 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.)

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.

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.

PART B—CRITICAL INFRASTRUCTURE INFORMATION

§ 131. 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'' 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.

(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) 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 a[1] interference, compromise, or a[2] 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).

(6) 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.

(7) 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 78*l*(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

[1] So in original. Probably should be ''an''.

[2] So in original. The word ''a'' probably should not appear.

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(8) Cybersecurity risk; incident

The terms ''cybersecurity risk'' and ''incident'' have the meanings given those terms in section 148 of this title.

(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.)

AMENDMENTS

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).

SHORT TITLE

For short title of this part as the ''Critical Infrastructure Information Act of 2002'', see section 211 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, 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 227 of the Homeland Security Act of 2002 [6 U.S.C. 148], as so redesignated by section 223(a)(3) of this division.

''(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.''

§ 132. 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 II, § 213, Nov. 25, 2002, 116 Stat. 2152.)

§ 133. 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 govern-

[1] So in original. The period probably should be a semicolon.

ment 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 the Federal Advisory Committee Act.

(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 132 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 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.)

REFERENCES IN TEXT

The Critical Infrastructure Information Act of 2002, referred to in subsec. (a)(2)(A), is subtitle B (§ 211 et seq.) of title II 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.

The Federal Advisory Committee Act, referred to in subsec. (b), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, as amended, which is set out in the Appendix to Title 5, Government Organization and Employees.

AMENDMENTS

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''.

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.

§ 134. 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 II, § 215, Nov. 25, 2002, 116 Stat. 2155.)

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.

PART C—INFORMATION SECURITY

§ 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.)

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, an-

swers, 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.)

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, as amended, 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. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 121 of this title, the Under Secretary appointed under section 113(a)(1)(H) of this title 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; and

(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 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.)

AMENDMENTS

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.

§ 144. NET Guard

The Assistant Secretary for Infrastructure Protection 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 II, § 224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, § 531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334.)

AMENDMENTS

2007—Pub. L. 110–53 substituted "Assistant Secretary for Infrastructure Protection" for "Under Secretary for Information Analysis and Infrastructure Protection".

§ 145. 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 II, § 225, Nov. 25, 2002, 116 Stat. 2156.)

CODIFICATION

Section is comprised of section 225 of Pub. L. 107–296. Subsecs. (d)(1) and (e) to (j) of section 225 of Pub. L. 107–296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

§ 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.)

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.

HOMELAND SECURITY CYBERSECURITY WORKFORCE ASSESSMENT

Pub. L. 113–277, § 4, Dec. 18, 2014, 128 Stat. 3008, provided that:

[1] So in original.

''(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.''

§ 147. 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 II, § 226, as added Pub. L. 113–277, § 3(a), Dec. 18, 2014, 128 Stat. 3005.)

§ 148. National cybersecurity and communications integration center

(a) Definitions

In this section—

(1) 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;

(2) the terms ''cyber threat indicator'' and ''defensive measure'' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 [6 U.S.C. 1501];

(3) 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;

(4) the term ''information sharing and analysis organization'' has the meaning given that term in section 131(5) of this title;

(5) the term ''information system'' has the meaning given that term in section 3502(8) of title 44; and

(6) the term ''sharing'' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(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 Under Secretary appointed under section 113(a)(1)(H) of this title.

(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; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

(6) upon request, providing 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;

(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) sharing[1] 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, 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; and

(11) in coordination with the Office of Emergency Communications 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.

(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, as that term is defined under section 3003(4) of title 50;

(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;

(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 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; and;[2]

(H) the Center designates an agency contact for non-Federal entities;

(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) No right or benefit

(1) In general

The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 113(a)(1)(H) of this title.

(2) Certain assistance or information

The provision of certain assistance or information to, or inclusion in the Center of, one

[1] So in original. Probably should be ''share''.

[2] So in original. The semicolon probably should not appear.

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.

(g) Automated information sharing

(1) In general

The Under Secretary appointed under section 113(a)(1)(H) of this title, 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 Under Secretary appointed under section 113(a)(1)(H) of this title 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.

(h) 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 Under Secretary appointed under section 113(a)(1)(H) of this title, 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 Under Secretary appointed under section 113(a)(1)(H) of this title, 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 Under Secretary appointed under section 113(a)(1)(H) of this title, 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.

(i) 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.

(j) 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).

(k) Outreach

Not later than 60 days after December 18, 2015, the Secretary, acting through the Under Secretary appointed under section 113(a)(1)(H) of this title, 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.

(*l*) 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.

(m) 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.

(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.)

REFERENCES IN TEXT

Title I of the Cybersecurity Act of 2015, referred to in subsecs. (c)(1) and (g)(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.

PRIOR PROVISIONS

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, which is now classified to section 149(c) of this title.

AMENDMENTS

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*).

RULES OF CONSTRUCTION

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] of the Homeland Security Act of 2002 [6 U.S.C. 148], 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 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) of the Homeland Security Act of 2002 (6 U.S.C. 131(5));

''(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.''

§ 149. Cybersecurity plans

(a) Definitions

In this section—

(1) the term ''agency information system'' means an information system used or operated by an agency or by another entity on behalf of an agency;

(2) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 148 of this title;

(3) the term ''intelligence community'' has the meaning given the term in section 3003(4) of title 50; and

(4) the term ''national security system'' has the meaning given the term in section 11103 of title 40.

(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 Under Secretary appointed under section 113(a)(1)(H) of this title shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 148 of this title) to critical infrastructure.

(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.

(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.)

CODIFICATION

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.

PRIOR PROVISIONS

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and is classified to section 150 of this title.

AMENDMENTS

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).

RULE OF CONSTRUCTION

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.''

§ 149a. 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 the[1] section 148 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

[1] So in original.

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.

(h) Definition

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.

(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.)

§ 150. 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 (as defined in section 131(5) of this title), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(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.)

REFERENCES IN TEXT

Executive Order 13549, referred to in text, is set out as a note under section 3161 of Title 50, War and National Defense.

[1] So in original. Probably should be ''51609;''.

§ 151. 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;

(3) the term ''agency information system'' has the meaning given the term in section 149 of this title; and

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 148 of this title.

(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 II, § 230, as added Pub. L. 114–113, div. N, title II, § 223(a)(6), Dec. 18, 2015, 129 Stat. 2964.)

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.

AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, § 223(b), Dec. 18, 2015, 129 Stat. 2966, 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 230(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(1)], as added by subsection (a), 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 230(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(2)], as added by subsection (a), 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 230(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 151(b)(1)], as added by subsection (a), at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.''

PART D—OFFICE OF SCIENCE AND TECHNOLOGY

§ 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.)

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 the Federal Advisory Committee Act (5 U.S.C. App.)) 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.)

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (b)(2), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, as amended, which is set out in the Appendix to Title 5, Government Organization and Employees.

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

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.)

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.)

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,,[1] 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 Assistant Secretary for Infrastructure Protection, 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,,[1] 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 re-

[1] So in original.