finalizing, any Department policies, initiatives, or actions that will have a major impact on trade and customs revenue functions. Such notifications shall include a description of the proposed policies, initiatives, or actions and any comments or recommendations provided by the Commercial Operations Advisory Committee and other relevant groups regarding the proposed policies, initiatives, or actions.

**(B) Exception**

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

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

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

**(d) Notification of reorganization of customs revenue functions**

**(1) In general**

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

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

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

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

**(2) Analysis**

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

**(3) Report**

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

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

**Editorial Notes**

CODIFICATION

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

AMENDMENTS

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

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

**Statutory Notes and Related Subsidiaries**

DEFINITIONS

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

## SUBCHAPTER II—INFORMATION ANALYSIS

**Editorial Notes**

CODIFICATION

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

### PART A—INFORMATION AND ANALYSIS; ACCESS TO INFORMATION

**Editorial Notes**

CODIFICATION

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

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

**§ 121. Information and Analysis**

**(a) Intelligence and analysis**

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

**(b) Under Secretary for Intelligence and Analysis**

**(1) Office of Intelligence and Analysis**

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

**(2) Chief Intelligence Officer**

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

**(c) Discharge of responsibilities**

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

**(d) Responsibilities of Secretary relating to intelligence and analysis**

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

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

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

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

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

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

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

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

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

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

(5) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 485 of this title, including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

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

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

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

(9) To ensure that—

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

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

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

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

(12) To ensure, in conjunction with the chief information officer of the Department, that

[1] So in original. The comma probably should not appear.

any information databases and analytical tools developed or utilized by the Department—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**(e) Staff**

**(1) In general**

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

**(2) Private sector analysts**

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

**(3) Security clearances**

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

**(f) Detail of personnel**

**(1) In general**

In order to assist the Office of Intelligence and Analysis in discharging responsibilities

under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

**(2) Covered agencies**

The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

**(3) Cooperative agreements**

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

**(4) Basis**

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

**(g) Functions transferred**

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

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

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

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

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

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

(Pub. L. 107–296, title II, § 201, Nov. 25, 2002, 116 Stat. 2145; Pub. L. 110–53, title V, §§ 501(a)(2)(A), (b), 531(a), title X, § 1002(a), Aug. 3, 2007, 121 Stat. 309, 332, 374; Pub. L. 110–417, [div. A], title IX, § 931(b)(5), Oct. 14, 2008, 122 Stat. 4575; Pub. L. 111–84, div. A, title X, § 1073(c)(9), Oct. 28, 2009, 123 Stat. 2475; Pub. L. 111–258, § 5(b)(1), Oct. 7, 2010, 124 Stat. 2650; Pub. L. 114–328, div. A, title XIX, § 1913(a)(2), Dec. 23, 2016, 130 Stat. 2685; Pub. L. 115–278, § 2(g)(2)(C), Nov. 16, 2018, 132 Stat. 4177.)

**Editorial Notes**

REFERENCES IN TEXT

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

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

CODIFICATION

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

AMENDMENTS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(C) may be classified.''

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

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

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

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

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

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

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

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

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

Subsec. (d)(1). Pub. L. 110–53, §501(b)(1), inserted '', in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 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.

**Statutory Notes and Related Subsidiaries**

EFFECTIVE DATE OF 2009 AMENDMENT

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

REGULATIONS

Pub. L. 109–295, title V, §550, Oct. 4, 2006, 120 Stat. 1388, as amended by Pub. L. 110–161, div. E, title V, §534, Dec. 26, 2007, 121 Stat. 2075; Pub. L. 111–83, title V, §550,

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

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

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

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

''(a) DEFINITIONS.—In this section:

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

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

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

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

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

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

''(B) with respect to either the Overt Human Intelligence Collection Program or the Open Source Intelligence Collection Program, any collection targeting journalists in the performance of their journalistic functions; and

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

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

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

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

''(A) a United States citizen;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(D) Whether the responsibilities and requirements for such programs set forth in the relevant policy instructions, intelligence oversight guidelines, and other governing documents or standard operating procedures of the Office of Intelligence and Analysis, particularly as they relate to the obligation to safeguard the privacy, civil liberties, and civil rights of United States persons, are adequate, appropriate, and consistently adhered to by such personnel.

''(E) Whether such programs raise or have raised legal, ethical, or operational concerns, including

concerns relating to the actual or potential violation of any applicable policies or procedures for protecting the constitutional or statutory rights of United States persons.

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

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

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

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

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

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

''(4) REPORT.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(e) RULES OF CONSTRUCTION.—

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

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

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

''(B) the private sector; or

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

### DHS COMPONENT USAGE OF THE HOMELAND SECURITY INFORMATION NETWORK

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

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

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

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

''(b) TECHNICAL ENHANCEMENTS.—The Chief Information Officer, in consultation with the Chief Intelligence Officer, shall assess and implement, as appropriate, technical enhancements to HSIN to improve usability, including search functionality, data analysis, and collaboration capabilities.''

DEADLINE FOR INITIAL RECOMMENDED STRATEGY

Pub. L. 114–328, div. A, title XIX, § 1913(c), Dec. 23, 2016, 130 Stat. 2687, provided that: ''Not later than one year after the date of the enactment of this section [Dec. 23, 2016], the Secretary of Homeland Security shall submit the recommended strategy required under paragraph (26) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)), as added by this section.''

ENHANCED GRID SECURITY

Pub. L. 114–94, div. F, § 61003(c), Dec. 4, 2015, 129 Stat. 1778, provided that:

''(1) DEFINITIONS.—In this subsection:

''(A) CRITICAL ELECTRIC INFRASTRUCTURE; CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The terms 'critical electric infrastructure' and 'critical electric infrastructure information' have the meanings given those terms in section 215A of the Federal Power Act [16 U.S.C. 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.''

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

CYBERSECURITY COLLABORATION BETWEEN THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF HOMELAND SECURITY

Pub. L. 112–81, div. A, title X, § 1090, Dec. 31, 2011, 125 Stat. 1603, provided that:

''(a) INTERDEPARTMENTAL COLLABORATION.—

''(1) IN GENERAL.—The Secretary of Defense and the Secretary of Homeland Security shall provide personnel, equipment, and facilities in order to increase interdepartmental collaboration with respect to—

''(A) strategic planning for the cybersecurity of the United States;

''(B) mutual support for cybersecurity capabilities development; and

''(C) synchronization of current operational cybersecurity mission activities.

''(2) EFFICIENCIES.—The collaboration provided for under paragraph (1) shall be designed—

''(A) to improve the efficiency and effectiveness of requirements formulation and requests for products, services, and technical assistance for, and coordination and performance assessment of, cybersecurity missions executed across a variety of Department of Defense and Department of Homeland Security elements; and

''(B) to leverage the expertise of each individual Department and to avoid duplicating, replicating, or aggregating unnecessarily the diverse line organizations across technology developments, operations, and customer support that collectively execute the cybersecurity mission of each Department.

''(b) RESPONSIBILITIES.—

''(1) DEPARTMENT OF HOMELAND SECURITY.—The Secretary of Homeland Security shall identify and assign, in coordination with the Department of Defense, a Director of Cybersecurity Coordination within the Department of Homeland Security to undertake collaborative activities with the Department of Defense.

''(2) DEPARTMENT OF DEFENSE.—The Secretary of Defense shall identify and assign, in coordination with the Department of Homeland Security, one or more officials within the Department of Defense to coordinate, oversee, and execute collaborative activities and the provision of cybersecurity support to the Department of Homeland Security.''

CYBERSECURITY OVERSIGHT

Pub. L. 111–259, title III, § 336, Oct. 7, 2010, 124 Stat. 2689, which related to cybersecurity oversight and provided for notification of cybersecurity programs, program and information sharing reports, provisions for the detailing of personnel, and provisions for further planning to recruit, retain, and train a highly-qualified workforce to secure the networks of the intelligence community, terminated on Dec. 31, 2013.

TREATMENT OF INCUMBENT UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS

Pub. L. 110–53, title V, § 531(c), Aug. 3, 2007, 121 Stat. 335, provided that: ''The individual administratively performing the duties of the Under Secretary for Intelligence and Analysis as of the date of the enactment of this Act [Aug. 3, 2007] may continue to perform such duties after the date on which the President nominates an individual to serve as the Under Secretary pursuant to section 201 of the Homeland Security Act of 2002 [6 U.S.C. 121], as amended by this section, and until the individual so appointed assumes the duties of the position.''

REPORTS TO BE SUBMITTED TO CERTAIN COMMITTEES

Pub. L. 110–53, title XXIV, § 2403, Aug. 3, 2007, 121 Stat. 547, provided that: ''The Committee on Commerce, Science, and Transportation of the Senate shall receive the reports required by the following provisions of law in the same manner and to the same extent that the reports are to be received by the Committee on Homeland Security and Governmental Affairs of the Senate:

''(1) Section 1016(j)(1) [now 1016(i)(1)] of the Intelligence Reform and Terrorist [Terrorism] Prevention Act of 2004 (6 U.S.C. 485(j)(1) [now 6 U.S.C. 485(i)(1)]).

''(2) Section 511(d) of this Act [121 Stat. 323].

''(3) [Former] [s]ubsection (a)(3)(D) of section 2022 of the Homeland Security Act of 2002 [former 6 U.S.C. 612(a)(3)(D)], as added by section 101 of this Act.

''(4) Section 7215(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 123(d)).

''(5) Section 7209(b)(1)(C) of the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458] (8 U.S.C. 1185 note).

''(6) Section 804(c) of this Act [42 U.S.C. 2000ee–3(c)].

''(7) Section 901(b) of this Act [121 Stat. 370].

''(8) Section 1002(a) of this Act [amending this section].

''(9) Title III of this Act [enacting sections 579 and 580 of this title and amending sections 194 and 572 of this title].''

SECURITY MANAGEMENT SYSTEMS DEMONSTRATION PROJECT

Pub. L. 110–53, title XXIV, §2404, Aug. 3, 2007, 121 Stat. 548, provided that:

''(a) DEMONSTRATION PROJECT REQUIRED.—Not later than 120 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall—

''(1) establish a demonstration project to conduct demonstrations of security management systems that—

''(A) shall use a management system standards approach; and

''(B) may be integrated into quality, safety, environmental and other internationally adopted management systems; and

''(2) enter into one or more agreements with a private sector entity to conduct such demonstrations of security management systems.

''(b) SECURITY MANAGEMENT SYSTEM DEFINED.—In this section, the term 'security management system' means a set of guidelines that address the security assessment needs of critical infrastructure and key resources that are consistent with a set of generally accepted management standards ratified and adopted by a standards making body.''

**Executive Documents**

EX. ORD. NO. 13231. CRITICAL INFRASTRUCTURE PROTECTION IN THE INFORMATION AGE

Ex. Ord. No. 13231, Oct. 16, 2001, 66 F.R. 53063, as amended by Ex. Ord. No. 13284, §2, Jan. 23, 2003, 68 F.R. 4075; Ex. Ord. No. 13286, §7, Feb. 28, 2003, 68 F.R. 10620; Ex. Ord. No. 13385, §5, Sept. 29, 2005, 70 F.R. 57990; Ex. Ord. No. 13652, §6, Sept. 30, 2013, 78 F.R. 61818; Ex. Ord. No. 14048, §6, Sept. 30, 2021, 86 F.R. 55467, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

SECTION 1. *Policy*. The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

SEC. 2. *Continuing Authorities*. This order does not alter the existing authorities or roles of United States Government departments and agencies. Authorities set forth in 44 U.S.C. chapter 35, and other applicable law, provide senior officials with responsibility for the security of Federal Government information systems.

(a) Executive Branch Information Systems Security. The Director of the Office of Management and Budget (OMB) has the responsibility to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, except those noted in section 2(b) of this order. The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices within the purview of this section in an executive branch department or agency.

(b) National Security Information Systems. The Secretary of Defense and the Director of Central Intelligence (DCI) shall have responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.

(i) Policies, principles, standards, and guidelines developed under this subsection may require more stringent protection than those developed in accordance with section 2(a) of this order.

(ii) The Assistant to the President for National Security Affairs shall advise the President and the appropriate department or agency when there is a critical deficiency in the security practices of a department or agency within the purview of this section.

(iii) National Security Systems. The National Security Telecommunications and Information Systems Security Committee, as established by and consistent with NSD–42 and chaired by the Department of Defense, shall be designated as the ''Committee on National Security Systems.''

(c) Additional Responsibilities. The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

SEC. 3. *The National Infrastructure Advisory Council*. The National Infrastructure Advisory Council (NIAC), established on October 16, 2001, shall provide the President, through the Secretary of Homeland Security, with advice on the security and resilience of the critical infrastructure sectors and their functional systems, physical assets, and cyber networks.

(a) *Membership*. The NIAC shall be composed of not more than 30 members appointed by the President, taking appropriate account of the benefits of having members:

(i) from the private sector, including individuals with experience in banking and finance, transportation, energy, water, communications, health care services, food and agriculture, government facilities, emergency services organizations, institutions of higher education, environmental and climate resilience, and State, local, and tribal governments;

(ii) with senior executive leadership responsibilities for the availability and reliability, including security and resilience, of critical infrastructure sectors;

(iii) with expertise relevant to the functions of the NIAC; and

(iv) with experience equivalent to that of a chief executive of an organization.

Unless otherwise determined by the President, no full-time officer or employee of the executive branch shall be appointed to serve as a member of the NIAC. The President shall designate from among the members of the NIAC a Chair and a Vice Chair, who shall perform the functions of the Chair if the Chair is absent or disabled, or in the instance of a vacancy in the Chair, each for a term of up to two years.. [sic]

(b) *Functions of the NIAC*. The NIAC shall meet periodically to:

(i) enhance the partnership of the public and private sectors in securing and enhancing the security and resilience of critical infrastructure and their supporting functional systems, physical assets, and cyber networks, and provide reports on this issue to the President, through the Secretary of Homeland Security, as appropriate;

(ii) propose and develop ways to encourage private industry to perform periodic risk assessments and implement risk-reduction programs;

(iii) monitor the development and operations of critical infrastructure sector coordinating councils and their information-sharing mechanisms and provide recommendations to the President, through the Secretary of Homeland Security, on how these organizations can best foster improved cooperation among the sectors, the Department of Homeland Security, and other Federal Government entities;

(iv) report to the President through the Secretary of Homeland Security, who shall ensure appropriate coordination with the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs under the terms of this order; and

(v) advise sector-specific agencies with critical infrastructure responsibilities to include issues pertaining to sector and government coordinating councils and their information sharing mechanisms.

In implementing this order, the NIAC shall not advise or otherwise act on matters pertaining to National Security and Emergency Preparedness (NS/EP) Communications and, with respect to any matters to which the NIAC is authorized by this order to provide advice or otherwise act on that may depend on or affect NS/EP Communications, shall coordinate with the National Security and Telecommunications Advisory Committee established by Executive Order 12382 of September 13, 1982, as amended.

(c) Administration of the NIAC.

(i) The NIAC may hold hearings, conduct inquiries, and establish subcommittees, as appropriate.

(ii) Upon request of the Chair, and to the extent permitted by law, the heads of the executive departments and agencies shall provide the NIAC with information and advice relating to its functions.

(iii) Senior Federal Government officials may participate in the meetings of the NIAC, as appropriate.

(iv) Members shall serve without compensation for their work on the NIAC. However, members may be reimbursed for travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service (5 U.S.C. 5701–5707).

(v) To the extent permitted by law and subject to the availability of appropriations, the Department of Homeland Security shall provide the NIAC with administrative services, staff, and other support services, and such funds as may be necessary for the performance of the NIAC's functions.

SEC. 4. *Judicial Review*. This order does not create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

### EXTENSION OF TERM OF NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

Term of National Infrastructure Advisory Council extended until Sept. 30, 2025, by Ex. Ord. No. 14109, Sept. 29, 2023, 88 F.R. 68447, set out as a note under section 1013 of Title 5, Government Organization and Employees.

Previous extensions of term of National Infrastructure Advisory Council were contained in the following prior Executive Orders:

Ex. Ord. No. 14048, Sept. 30, 2021, 86 F.R. 55465, extended term until Sept. 30, 2023.

Ex. Ord. No. 13889, Sept. 27, 2019, 84 F.R. 52743, extended term until Sept. 30, 2021.

Ex. Ord. No. 13811, Sept. 29, 2017, 82 F.R. 46363, extended term until Sept. 30, 2019.

Ex. Ord. No. 13708, Sept. 30, 2015, 80 F.R. 60271, extended term until Sept. 30, 2017.

Ex. Ord. No. 13652, Sept. 30, 2013, 78 F.R. 61817, extended term until Sept. 30, 2015.

Ex. Ord. No. 13585, Sept. 30, 2011, 76 F.R. 62281, extended term until Sept. 30, 2013.

Ex. Ord. No. 13511, Sept. 29, 2009, 74 F.R. 50909, extended term until Sept. 30, 2011.

Ex. Ord. No. 13446, Sept. 28, 2007, 72 F.R. 56175, extended term until Sept. 30, 2009.

Ex. Ord. No. 13385, Sept. 29, 2005, 70 F.R. 57989, extended term until Sept. 30, 2007.

Ex. Ord. No. 13316, Sept. 17, 2003, 68 F.R. 55255, extended term until Sept. 30, 2005.

### EX. ORD. NO. 13284. AMENDMENT OF EXECUTIVE ORDERS, AND OTHER ACTIONS, IN CONNECTION WITH THE ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY

Ex. Ord. No. 13284, Jan. 23, 2003, 68 F.R. 4075, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Homeland Security Act of 2002 (Public Law 107–296) [see Tables for classification], and the National Security Act of 1947, as amended (50 U.S.C. 401 *et seq.*) [now 50 U.S.C. 3001 et seq.], and in order to reflect responsibilities vested in the Secretary of Homeland Security and take other actions in connection with the establishment of the Department of Homeland Security, it is hereby ordered as follows:

SECTION 1. [Amended Ex. Ord. No. 13234.]

SEC. 2. [Amended Ex. Ord. No. 13231, set out above.]

SEC. 3. Executive Order 13228 of October 8, 2001 (''Establishing the Office of Homeland Security and the Homeland Security Council'') [50 U.S.C. 3021 note], is amended by inserting ''the Secretary of Homeland Security,'' after ''the Secretary of Transportation,'' in section 5(b). Further, during the period from January 24, 2003, until March 1, 2003, the Secretary of Homeland Security shall have the responsibility for coordinating the domestic response efforts otherwise assigned to the Assistant to the President for Homeland Security pursuant to section 3(g) of Executive Order 13228.

SEC. 4. [Amended Ex. Ord. No. 13224, listed in a table under section 1701 of Title 50, War and National Defense.]

SEC. 5. [Amended Ex. Ord. No. 13151, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

SEC. 6. [Amended Ex. Ord. No. 13122, set out as a note under section 3121 of Title 42, The Public Health and Welfare.]

SEC. 7. [Amended Ex. Ord. No. 13048, set out as a note under section 501 of Title 31, Money and Finance.]

SEC. 8. [Amended Ex. Ord. No. 12992, set out as a note under section 1708 of Title 21, Food and Drugs.]

SEC. 9. [Amended Ex. Ord. No. 12881, set out as a note under section 6601 of Title 42, The Public Health and Welfare.]

SEC. 10. [Amended Ex. Ord. No. 12859, set out as a note preceding section 101 of Title 3, The President.]

SEC. 11. [Amended Ex. Ord. No. 12590, set out as a note under former section 1201 of Title 21, Food and Drugs.]

SEC. 12. [Amended Ex. Ord. No. 12260, set out as a note under section 2511 of Title 19, Customs Duties.]

SEC. 13. [Amended Ex. Ord. No. 11958, set out as a note under section 2751 of Title 22, Foreign Relations and Intercourse.]

SEC. 14. [Amended Ex. Ord. No. 11423, set out as a note under section 301 of Title 3, The President.]

SEC. 15. [Amended Ex. Ord. No. 10865, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 16. [Amended Ex. Ord. No. 13011, set out as a note under section 11101 of Title 40, Public Buildings, Property, and Works.]

SEC. 17. Those elements of the Department of Homeland Security that are supervised by the Department's Under Secretary for Information Analysis and Infrastructure Protection through the Department's Assistant Secretary for Information Analysis, with the exception of those functions that involve no analysis of foreign intelligence information, are designated as elements of the Intelligence Community under section 201(h) of the Homeland Security Act of 2002 [Pub. L. 107–296, amending 50 U.S.C. 3003] and section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a[(4)]) [now 50 U.S.C. 3003(4)].

SEC. 18. [Amended Ex. Ord. No. 12333, set out as a note under section 3001 of title 50, War and National Defense.]

SEC. 19. *Functions of Certain Officials in the Department of Homeland Security*.

The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a ''Senior Official of the Intelligence Community'' for purposes of Executive Order 12333 [50 U.S.C. 3001 note], and all other relevant authorities, and shall:

(a) recognize and give effect to all current clearances for access to classified information held by those who become employees of the Department of Homeland Security by operation of law pursuant to the Homeland Security Act of 2002 or by Presidential appointment;

(b) recognize and give effect to all current clearances for access to classified information held by those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities;

(c) make all clearance and access determinations pursuant to Executive Order 12968 of August 2, 1995 [50 U.S.C. 3161 note], or any successor Executive Order, as to employees of, and applicants for employment in, the Department of Homeland Security who do not then hold a current clearance for access to classified information; and

(d) ensure all clearance and access determinations for those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities are made in accordance with Executive Order 12829 of January 6, 1993 [50 U.S.C. 3161 note].

SEC. 20. Pursuant to the provisions of section 1.4 of [former] Executive Order 12958 of April 17, 1995 (''Classified National Security Information''), I hereby authorize the Secretary of Homeland Security to classify information originally as ''Top Secret.'' Any delegation of this authority shall be in accordance with section 1.4 of that order or any successor Executive Orders.

SEC. 21. This order shall become effective on January 24, 2003.

SEC. 22. This order does not create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH.

### EX. ORD. NO. 13636. IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Ex. Ord. No. 13636, Feb. 12, 2013, 78 F.R. 11739, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

SEC. 2. *Critical Infrastructure*. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

SEC. 3. *Policy Coordination*. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

SEC. 4. *Cybersecurity Information Sharing*. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the ''Secretary''), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with [former] 6 U.S.C. 143 [now 6 U.S.C. 655] and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure

owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

SEC. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with [former] 6 U.S.C. 133 [now 6 U.S.C. 673] by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

SEC. 6. *Consultative Process.* The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

SEC. 7. *Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.* (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the ''Director'') to lead the development of a framework to reduce cyber risks to critical infrastructure (the ''Cybersecurity Framework''). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the ''preliminary Framework''). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the ''final Framework'').

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

SEC. 8. *Voluntary Critical Infrastructure Cybersecurity Program.* (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the ''Program'').

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in

the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

SEC. 9. *Identification of Critical Infrastructure at Greatest Risk.* (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

SEC. 10. *Adoption of Framework.* (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

SEC. 11. *Definitions.* (a) ''Agency'' means any authority of the United States that is an ''agency'' under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) ''Critical Infrastructure Partnership Advisory Council'' means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) ''Fair Information Practice Principles'' means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) ''Independent regulatory agency'' has the meaning given the term in 44 U.S.C. 3502(5).

(e) ''Sector Coordinating Council'' means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) ''Sector-Specific Agency'' has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

SEC. 12. *General Provisions.* (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to

supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to the National Security Staff deemed to be a reference to the National Security Council Staff, see Ex. Ord. No. 13657, set out as a note under section 3021 of Title 50, War and National Defense.]

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

EXECUTIVE ORDER NO. 13650

Ex. Ord. No. 13650, Aug. 1, 2013, 78 F.R. 48029, was transferred to a note set out under section 621 of this title.

EX. ORD. NO. 13691. PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

Ex. Ord. No. 13691, Feb. 13, 2015, 80 F.R. 9349, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive–21 (PPD–21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–l [sic] (PPD–l [PPD–1]) of February 13, 2009 (Organization of the National Security Council System), or any successor.

SEC. 2. *Information Sharing and Analysis Organizations*. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the ''Act''), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

SEC. 3. *ISAO Standards Organization*. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

SEC. 4. *Critical Infrastructure Protection Program*. (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats

to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

SEC. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency's activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

SEC. 6. *National Industrial Security Program.* [Amended Ex. Ord. No. 12829, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 7. *Definitions.* (a) ''Critical infrastructure information'' has the meaning given the term in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) ''Critical infrastructure protection program'' has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.

(c) ''Cybersecurity risk'' has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) ''Fair Information Practice Principles'' means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) ''Incident'' has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) ''Information Sharing and Analysis Organization'' has the meaning given the term in section 212(5) of the Critical Infrastrucure Information Act of 2002.

(g) ''Sector-Specific Agency'' has the meaning given the term in PPD–21, or any successor.

SEC. 8. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

## § 121a. Homeland Security Intelligence Program

There is established within the Department of Homeland Security a Homeland Security Intelligence Program. The Homeland Security Intelligence Program constitutes the intelligence activities of the Office of Intelligence and Analysis of the Department that serve predominantly departmental missions.

(Pub. L. 112–277, title V, § 501, Jan. 14, 2013, 126 Stat. 2476.)

### Editorial Notes

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2013, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

## § 122. Access to information

### (a) In general

#### (1) Threat and vulnerability information

Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

#### (2) Other information

The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide.

### (b) Manner of access

Except as otherwise directed by the President, with respect to information to which the Secretary has access pursuant to this section—

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both; and

(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to paragraph (1), all agencies of the Federal Government shall promptly provide to the Secretary—

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed;

(C) all other information relating to significant and credible threats of terrorism against the United States, whether or not such information has been analyzed; and

(D) such other information or material as the President may direct.

**(c) Treatment under certain laws**

The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of National Intelligence, under any provision of the following:

(1) The USA PATRIOT Act of 2001 (Public Law 107–56).

(2) Section 2517(6) of title 18.

(3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

**(d) Access to intelligence and other information**

**(1) Access by elements of Federal Government**

Nothing in this subchapter shall preclude any element of the intelligence community (as that term is defined in section 3003(4) of title 50,[1] or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any intelligence or other information relating to terrorism.

**(2) Sharing of information**

The Secretary, in consultation with the Director of National Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

(Pub. L. 107–296, title II, § 202, Nov. 25, 2002, 116 Stat. 2149; Pub. L. 115–278, § 2(g)(2)(D), Nov. 16, 2018, 132 Stat. 4177.)

**Editorial Notes**

REFERENCES IN TEXT

The USA PATRIOT Act of 2001, referred to in subsec. (c)(1), is Pub. L. 107–56, Oct. 26, 2001, 115 Stat. 272, known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 or the USA PATRIOT Act. For complete classification of this Act to the Code, see Short Title of 2001 Amendment note set out under section 1 of Title 18, Crimes and Criminal Procedure, and Tables.

The Federal Rules of Criminal Procedure, referred to in subsec. (c)(3), are set out in the Appendix to Title 18, Crimes and Criminal Procedure.

This subchapter, referred to in subsec. (d)(1), was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 3003 of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c), (d)(2). Pub. L. 115–278 substituted ''Director of National Intelligence'' for ''Director of Central Intelligence''.

[1] So in original. There probably should be a closing parenthesis after ''50''.

## § 123. Terrorist travel program

**(a) Requirement to establish**

Not later than 90 days after August 3, 2007, the Secretary of Homeland Security, in consultation with the Director of the National Counterterrorism Center and consistent with the strategy developed under section 7201,[1] shall establish a program to oversee the implementation of the Secretary's responsibilities with respect to terrorist travel.

**(b) Head of the program**

The Secretary of Homeland Security shall designate an official of the Department of Homeland Security to be responsible for carrying out the program. Such official shall be—

(1) the Assistant Secretary for Policy of the Department of Homeland Security; or

(2) an official appointed by the Secretary who reports directly to the Secretary.

**(c) Duties**

The official designated under subsection (b) shall assist the Secretary of Homeland Security in improving the Department's ability to prevent terrorists from entering the United States or remaining in the United States undetected by—

(1) developing relevant strategies and policies;

(2) reviewing the effectiveness of existing programs and recommending improvements, if necessary;

(3) making recommendations on budget requests and on the allocation of funding and personnel;

(4) ensuring effective coordination, with respect to policies, programs, planning, operations, and dissemination of intelligence and information related to terrorist travel—

(A) among appropriate subdivisions of the Department of Homeland Security, as determined by the Secretary and including—

(i) United States Customs and Border Protection;

(ii) United States Immigration and Customs Enforcement;

(iii) United States Citizenship and Immigration Services;

[1] See References in Text note below.

(iv) the Transportation Security Administration; and

(v) the United States Coast Guard; and

(B) between the Department of Homeland Security and other appropriate Federal agencies; and

(5) serving as the Secretary's primary point of contact with the National Counterterrorism Center for implementing initiatives related to terrorist travel and ensuring that the recommendations of the Center related to terrorist travel are carried out by the Department.

**(d) Report**

Not later than 180 days after August 3, 2007, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this section.

(Pub. L. 108–458, title VII, §7215, Dec. 17, 2004, 118 Stat. 3832; Pub. L. 110–53, title VII, §722, Aug. 3, 2007, 121 Stat. 348.)

**Editorial Notes**

REFERENCES IN TEXT

Section 7201, referred to in subsec. (a), is section 7201 of Pub. L. 108–458, title VII, Dec. 17, 2004, 118 Stat. 3808, which enacted section 1776 of Title 8, Aliens and Nationality, and provisions set out as notes under section 1776 of Title 8 and sections 3024 and 3056 of Title 50, War and National Defense.

CODIFICATION

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the 9/11 Commission Implementation Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

AMENDMENTS

2007—Pub. L. 110–53 reenacted section catchline without change and amended text generally, substituting provisions relating to establishment of a program to oversee the implementation of the Secretary's responsibilities with respect to terrorist travel not later than 90 days after Aug. 3, 2007, and relating to the head of the program, such official's duties, and report on implementation for provisions relating to establishment of a program to oversee the implementation of the Department's responsibilities with respect to terrorist travel.

**Statutory Notes and Related Subsidiaries**

NATIONAL STRATEGY TO COMBAT TERRORIST TRAVEL

Pub. L. 114–328, div. A, title XIX, §1908, Dec. 23, 2016, 130 Stat. 2678, provided that:

''(a) SENSE OF CONGRESS.—It is the sense of Congress that it should be the policy of the United States to—

''(1) continue to regularly assess the evolving terrorist threat to the United States;

''(2) catalog existing Federal Government efforts to obstruct terrorist and foreign fighter travel into, out of, and within the United States, and overseas;

''(3) identify such efforts that may benefit from reform or consolidation, or require elimination;

''(4) identify potential security vulnerabilities in United States defenses against terrorist travel; and

''(5) prioritize resources to address any such security vulnerabilities in a risk-based manner.

''(b) NATIONAL STRATEGY AND UPDATES.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees a national strategy to combat terrorist travel. The strategy shall address efforts to intercept terrorists and foreign fighters and constrain the domestic and international travel of such persons. Consistent with the protection of classified information, the strategy shall be submitted in unclassified form, including, as appropriate, a classified annex.

''(2) UPDATED STRATEGIES.—Not later than 180 days after the date on which a new President is inaugurated, the President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an updated version of the strategy described in paragraph (1).

''(3) CONTENTS.—The strategy and updates required under this subsection shall—

''(A) include an accounting and description of all Federal Government programs, projects, and activities designed to constrain domestic and international travel by terrorists and foreign fighters;

''(B) identify specific security vulnerabilities within the United States and outside of the United States that may be exploited by terrorists and foreign fighters;

''(C) delineate goals for—

''(i) closing the security vulnerabilities identified under subparagraph (B); and

''(ii) enhancing the ability of the Federal Government to constrain domestic and international travel by terrorists and foreign fighters; and

''(D) describe the actions that will be taken to achieve the goals delineated under subparagraph (C) and the means needed to carry out such actions, including—

''(i) steps to reform, improve, and streamline existing Federal Government efforts to align with the current threat environment;

''(ii) new programs, projects, or activities that are requested, under development, or undergoing implementation;

''(iii) new authorities or changes in existing authorities needed from Congress;

''(iv) specific budget adjustments being requested to enhance United States security in a risk-based manner; and

''(v) the Federal departments and agencies responsible for the specific actions described in this subparagraph.

''(4) SUNSET.—The requirement to submit updated national strategies under this subsection shall terminate on the date that is seven years after the date of the enactment of this Act [Dec. 23, 2016].

''(c) DEVELOPMENT OF IMPLEMENTATION PLANS.—For each national strategy required under subsection (b), the President shall direct the heads of relevant Federal agencies to develop implementation plans for each such agency.

''(d) IMPLEMENTATION PLANS.—

''(1) IN GENERAL.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an implementation plan developed under subsection (c) with each national strategy required under subsection (b). Consistent with the protection of classified information, each such implementation plan shall be submitted in unclassified form, but may include a classified annex.

''(2) ANNUAL UPDATES.—The President shall submit to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the House of Representatives, and the appropriate congressional committees an annual updated implementation plan during the ten-year period beginning on the date of the enactment of this Act [Dec. 23, 2016].

''(e) DEFINITION.—In this section, the term 'appropriate congressional committees' means—

''(1) in the House of Representatives—

''(A) the Committee on Homeland Security;

''(B) the Committee on Armed Services;

''(C) the Permanent Select Committee on Intelligence;

''(D) the Committee on the Judiciary;

''(E) the Committee on Foreign Affairs;

''(F) the Committee on Appropriations; and

''(2) in the Senate—

''(A) the Committee on Homeland Security and Governmental Affairs;

''(B) the Committee on Armed Services;

''(C) the Select Committee on Intelligence;

''(D) the Committee on the Judiciary;

''(E) the Committee on Foreign Relations; and

''(F) the Committee on Appropriations.

''(f) SPECIAL RULE FOR CERTAIN RECEIPT.—The definition under subsection (e) shall be treated as including the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate for purposes of receipt of those portions of—

''(1) the national strategy (including updates thereto), and

''(2) the implementation plan (including updates thereto),

required under this section that relate to maritime travel into and out of the United States.''

### § 124. Homeland Security Advisory System

#### (a) Requirement

The Secretary shall administer the Homeland Security Advisory System in accordance with this section to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal, State, local, and tribal government authorities and to the people of the United States, as appropriate. The Secretary shall exercise primary responsibility for providing such advisories or warnings.

#### (b) Required elements

In administering the Homeland Security Advisory System, the Secretary shall—

(1) establish criteria for the issuance and revocation of such advisories or warnings;

(2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of such advisories or warnings;

(3) provide, in each such advisory or warning, specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable to enable individuals, government entities, emergency response providers, and the private sector to act appropriately;

(4) whenever possible, limit the scope of each such advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and

(5) not, in issuing any advisory or warning, use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

(Pub. L. 107–296, title II, § 203, as added Pub. L. 110–53, title V, § 501(a)(1), Aug. 3, 2007, 121 Stat. 306.)

### § 124a. Homeland security information sharing

#### (a) Information sharing

Consistent with section 485 of this title, the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50) except for any internal security protocols or personnel information of such intelligence components, or other administrative processes that are administered by any chief security officer of the Department.

#### (b) Information sharing and knowledge management officers

For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3003(5) of title 50).

#### (c) State, local, and private-sector sources of information

##### (1) Establishment of business processes

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall—

(A) establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

##### (2) Feedback

The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of information provided by any entity of State, local, or tribal government or the private sector that provides such information to the Department.

#### (d) Training and evaluation of employees

##### (1) Training

The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall provide to employees of the Department op-

portunities for training and education to develop an understanding of—

(A) the definitions of homeland security information and national intelligence (as defined in section 3003(5) of title 50); and

(B) how information available to such employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

**(2) Evaluations**

The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, as described in this subchapter, and participating in the information sharing environment established under section 485 of this title; and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

(Pub. L. 107–296, title II, §204, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 307; amended Pub. L. 115–278, §2(g)(2)(E), Nov. 16, 2018, 132 Stat. 4177.)

**Editorial Notes**

REFERENCES IN TEXT

This subchapter, referred to in subsec. (d)(2)(A), was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2018—Subsecs. (c)(1), (d)(1). Pub. L. 115–278 substituted ''Director of the Cybersecurity and Infrastructure Security Agency'' for ''Assistant Secretary for Infrastructure Protection'' in introductory provisions.

**Statutory Notes and Related Subsidiaries**

RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERVICE

Pub. L. 110–53, title V, §502(b), Aug. 3, 2007, 121 Stat. 311, provided that:

''(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall receive from the United States Secret Service homeland security information, terrorism information, weapons of mass destruction information (as these terms are defined in Section [sic] 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)), or national intelligence, as defined in Section [sic] 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)) [now 50 U.S.C. 3003(5)], as well as suspect information obtained in criminal investigations. The United States Secret Service shall cooperate with the Under Secretary for Intelligence and Analysis with respect to activities under sections 204 and 205 of the Homeland Security Act of 2002 [6 U.S.C. 124a, 124b].

''(2) SAVINGS CLAUSE.—Nothing in this Act [see Tables for classification] shall interfere with the operation of Section [sic] 3056(g) of Title 18, United States Code, or with the authority of the Secretary of Homeland Security or the Director of the United States Secret Service regarding the budget of the United States Secret Service.''

## §124b. Comprehensive information technology network architecture

**(a) Establishment**

The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 485 of this title, and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department.

**(b) Comprehensive information technology network architecture defined**

The term ''comprehensive information technology network architecture'' means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic management and information resources management goals of the Office of Intelligence and Analysis.

(Pub. L. 107–296, title II, §205, as added Pub. L. 110–53, title V, §501(a)(1), Aug. 3, 2007, 121 Stat. 308.)

## §124c. Coordination with information sharing environment

**(a) Guidance**

All activities to comply with sections 124, 124a, and 124b of this title shall be—

(1) consistent with any policies, guidelines, procedures, instructions, or standards established under section 485 of this title;

(2) implemented in coordination with, as appropriate, the program manager for the information sharing environment established under that section;

(3) consistent with any applicable guidance issued by the Director of National Intelligence; and

(4) consistent with any applicable guidance issued by the Secretary relating to the protection of law enforcement information or proprietary information.

**(b) Consultation**

In carrying out the duties and responsibilities under this part, the Under Secretary for Intelligence and Analysis shall take into account the views of the heads of the intelligence components of the Department.

(Pub. L. 107–296, title II, § 206, as added Pub. L. 110–53, title V, § 501(a)(1), Aug. 3, 2007, 121 Stat. 309.)

### § 124d. Intelligence components

Subject to the direction and control of the Secretary, and consistent with any applicable guidance issued by the Director of National Intelligence, the responsibilities of the head of each intelligence component of the Department are as follows:

(1) To ensure that the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence (as defined in section 3003(5) of title 50), are carried out effectively and efficiently in support of the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(2) To otherwise support and implement the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.

(4) To coordinate with the Under Secretary for Intelligence and Analysis in developing policies and requirements for the recruitment and selection of intelligence officials of the intelligence component.

(5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.

(6) To ensure that employees of the intelligence component have knowledge of, and comply with, the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that such employees comply with all applicable laws and regulations.

(7) To perform such other activities relating to such responsibilities as the Secretary may provide.

(Pub. L. 107–296, title II, § 207, as added Pub. L. 110–53, title V, § 503(a), Aug. 3, 2007, 121 Stat. 311.)

### § 124e. Training for employees of intelligence components

The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs that are related to the functions of the Department relating to the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50).

(Pub. L. 107–296, title II, § 208, as added Pub. L. 110–53, title V, § 503(a), Aug. 3, 2007, 121 Stat. 312.)

### § 124f. Intelligence training development for State and local government officials

#### (a) Curriculum

The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall—

(1) develop a curriculum for training State, local, and tribal government officials, including law enforcement officers, intelligence analysts, and other emergency response providers, in the intelligence cycle and Federal laws, practices, and regulations regarding the development, handling, and review of intelligence and other information; and

(2) ensure that the curriculum includes executive level training for senior level State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers.

#### (b) Training

To the extent possible, the Federal Law Enforcement Training Center and other existing Federal entities with the capacity and expertise to train State, local, and tribal government officials based on the curriculum developed under subsection (a) shall be used to carry out the training programs created under this section. If such entities do not have the capacity, resources, or capabilities to conduct such training, the Secretary may approve another entity to conduct such training.

#### (c) Consultation

In carrying out the duties described in subsection (a), the Under Secretary for Intelligence and Analysis shall consult with the Director of the Federal Law Enforcement Training Center, the Attorney General, the Director of National Intelligence, the Administrator of the Federal Emergency Management Agency, and other appropriate parties, such as private industry, institutions of higher education, nonprofit institutions, and other intelligence agencies of the Federal Government.

(Pub. L. 107–296, title II, § 209, as added Pub. L. 110–53, title V, § 503(a), Aug. 3, 2007, 121 Stat. 312.)

### § 124g. Information sharing incentives

#### (a) Awards

In making cash awards under chapter 45 of title 5, the President or the head of an agency, in consultation with the program manager designated under section 485 of this title, may consider the success of an employee in appropriately sharing information within the scope of the information sharing environment established under that section, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3003(5) of title 50[1], in a manner consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of that

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

environment for the implementation and management of that environment.

**(b) Other incentives**

The head of each department or agency described in section 485(h) of this title, in consultation with the program manager designated under section 485 of this title, shall adopt best practices regarding effective ways to educate and motivate officers and employees of the Federal Government to participate fully in the information sharing environment, including—

(1) promotions and other nonmonetary awards; and

(2) publicizing information sharing accomplishments by individual employees and, where appropriate, the tangible end benefits that resulted.

(Pub. L. 107–296, title II, §210, as added Pub. L. 110–53, title V, §503(a), Aug. 3, 2007, 121 Stat. 313; amended Pub. L. 117–263, div. F, title LXVIII, §6811(c)(2), Dec. 23, 2022, 136 Stat. 3601.)

**Editorial Notes**

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–263 substituted ''section 485(h) of this title'' for ''section 485(i) of this title'' in introductory provisions.

### § 124h. Department of Homeland Security State, Local, and Regional Fusion Center Initiative

**(a) Establishment**

The Secretary, in consultation with the program manager of the information sharing environment established under section 485 of this title, the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

**(b) Department support and coordination**

Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

(7) provide management assistance to State, local, and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

(11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

(12) carry out such other duties as the Secretary determines are appropriate.

**(c) Personnel assignment**

**(1) In general**

The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.

**(2) Personnel sources**

Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

(A) Office of Intelligence and Analysis.

(B) Cybersecurity and Infrastructure Security Agency.

(C) Transportation Security Administration.

(D) United States Customs and Border Protection.

(E) United States Immigration and Customs Enforcement.

(F) United States Coast Guard.

(G) Other components of the Department, as determined by the Secretary.

**(3) Qualifying criteria**

**(A) In general**

The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.

**(B) Criteria**

Any criteria developed under subparagraph (A) may include—

(i) whether the fusion center, through its mission and governance structure, focuses

on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;

(ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;

(iii) whether the fusion center has—

(I) access to relevant law enforcement, emergency response, private sector, open source, and national security data; and

(II) the ability to share and analytically utilize that data for lawful purposes;

(iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and

(v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

**(4) Prerequisite**

**(A) Intelligence analysis, privacy, and civil liberties training**

Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and

(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);

(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 142 of this title and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42; and

(iii) such other training prescribed by the Under Secretary for Intelligence and Analysis.

**(B) Prior work experience in area**

In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—

(i) has been previously assigned in the geographic area; or

(ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.

**(5) Expedited security clearance processing**

The Under Secretary for Intelligence and Analysis—

(A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and

(B) may request that security clearance processing be expedited for each such officer or intelligence analyst and may use available funds for such purpose.

**(6) Further qualifications**

Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other qualifications the Under Secretary for Intelligence and Analysis may prescribe.

**(d) Responsibilities**

An officer or intelligence analyst assigned to a fusion center under this section shall—

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

(3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; and

(4) assist in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies.

**(e) Border intelligence priority**

**(1) In general**

The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

**(2) Border intelligence products**

When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to participating State, local, and regional fusion centers under this section shall have, as a primary responsi-

bility, the creation of border intelligence products that—

(A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

**(f) Database access**

In order to fulfill the objectives described under subsection (d), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

**(g) Consumer feedback**

**(1) In general**

The Secretary shall create a voluntary mechanism for any State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other information products referred to in subsection (d) to provide feedback to the Department on the quality and utility of such intelligence products.

**(2) Report**

Not later than one year after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

**(h) Rule of construction**

**(1) In general**

The authorities granted under this section shall supplement the authorities granted under section 121(d) of this title and nothing in this section shall be construed to abrogate the authorities granted under section 121(d) of this title.

**(2) Participation**

Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

**(i) Guidelines**

The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that any such fusion center shall—

(1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;

(2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;

(3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment;

(4) leverage the databases, systems, and networks available from public and private sector entities, in accordance with all applicable laws, to maximize information sharing;

(5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;

(6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private sector representatives at the fusion center;

(7) ensure appropriate security measures are in place for the facility, data, and personnel;

(8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;

(9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and

(10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

**(j) Fusion center information sharing strategy**

Not later than 1 year after March 2, 2020, and not less frequently than once every 5 years thereafter, the Secretary shall develop or update a strategy for Department engagement with fusion centers. Such strategy shall be developed and updated in consultation with the heads of intelligence components of the Department, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, officials of fusion centers, officers designated as Homeland Security Advisors, and the heads of other relevant agencies, as appropriate. Such strategy shall include the following:

(1) Specific goals and objectives for sharing information and engaging with fusion centers—

(A) through the direct deployment of personnel from intelligence components of the Department;

(B) through the use of Department unclassified and classified information sharing systems, including the Homeland Security Information Network and the Homeland Secure Data Network, or any successor systems; and

(C) through any additional means.

(2) The performance metrics to be used to measure success in achieving the goals and objectives referred to in paragraph (1).

(3) A 5-year plan for continued engagement with fusion centers.

**(k) Definitions**

In this section—

(1) the term ''fusion center'' means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity;

(2) the term ''information sharing environment'' means the information sharing environment established under section 485 of this title;

(3) the term ''intelligence analyst'' means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

(4) the term ''intelligence-led policing'' means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; and

(5) the term ''terrorism information'' has the meaning given that term in section 485 of this title.

**(*l*) Authorization of appropriations**

There is authorized to be appropriated $10,000,000 for each of fiscal years 2008 through 2012, to carry out this section, except for subsection (i), including for hiring officers and intelligence analysts to replace officers and intelligence analysts who are assigned to fusion centers under this section.

(Pub. L. 107–296, title II, § 210A, as added Pub. L. 110–53, title V, § 511(a), Aug. 3, 2007, 121 Stat. 317; amended Pub. L. 115–278, § 2(g)(2)(F), Nov. 16, 2018, 132 Stat. 4177; Pub. L. 116–116, § 2, Mar. 2, 2020, 134 Stat. 110.)

**Editorial Notes**

AMENDMENTS

2020—Subsecs. (j) to (*l*). Pub. L. 116–116 added subsec. (j) and redesignated former subsecs. (j) and (k) as (k) and (*l*), respectively.

2018—Subsec. (c)(2)(B). Pub. L. 115–278 substituted ''Cybersecurity and Infrastructure Security Agency'' for ''Office of Infrastructure Protection''.

**Statutory Notes and Related Subsidiaries**

OFFICE OF INTELLIGENCE AND ANALYSIS FIELD PERSONNEL SUPPORT TO FUSION CENTERS

Pub. L. 116–116, § 3, Mar. 2, 2020, 134 Stat. 111, provided that:

''(a) PERFORMANCE METRICS.—Not later than 180 days after the date of the enactment of this Act [Mar. 2, 2020], the Under Secretary for Intelligence and Analysis shall—

''(1) consider the effectiveness of existing processes to identify and prepare field personnel for deployment to support fusion centers and internal mechanisms to ensure oversight and accountability of such field personnel, including field personnel assigned to one center and field personnel assigned to multiple centers; and

''(2) publish and disseminate performance metrics, taking into account, as appropriate, regional and threat diversity, for—

''(A) field personnel from the Office of Intelligence and Analysis assigned to an individual fusion center;

''(B) field personnel from the Office of Intelligence and Analysis assigned to multiple fusion centers; and

''(C) Regional Directors of the Office of Intelligence and Analysis to ensure accountability for monitoring all field personnel under the supervision of such Regional Directors.

''(b) TRAINING.—In consultation with the Chief Information Officer, the Under Secretary for Intelligence and Analysis shall develop and implement a formalized training module for fusion center personnel regarding the classified Homeland Secure Data Network, or any successor system.

''(c) FUSION CENTER DEFINED.—In this section, the term 'fusion center' has the meaning given such term in section 210A(k) of the Homeland Security Act of 2002 [6 U.S.C. 124h(k)], as so redesignated by section 2 [amending this section].''

TRAINING FOR PREDEPLOYED OFFICERS AND ANALYSTS

Pub. L. 110–53, title V, § 511(b), Aug. 3, 2007, 121 Stat. 323, provided that: ''An officer or analyst assigned to a fusion center by the Secretary of Homeland Security before the date of the enactment of this Act [Aug. 3, 2007] shall undergo the training described in section 210A(c)(4)(A) of the Homeland Security Act of 2002 [6 U.S.C. 124h(c)(4)(A)], as added by subsection (a), by not later than 6 months after such date.''

## § 124h–1. Threat information sharing

**(a) Prioritization**

The Secretary of Homeland Security shall prioritize the assignment of officers and intelligence analysts under section 124h of this title from the Transportation Security Administration and, as appropriate, from the Office of Intelligence and Analysis of the Department of Homeland Security, to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset in order to enhance the security of such assets, including by improving timely sharing, in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, of information regarding threats of terrorism and other threats, including targeted violence.

**(b) Intelligence products**

Officers and intelligence analysts assigned to locations with participating State, local, and regional fusion centers under this section shall participate in the generation and dissemination

of transportation security intelligence products, with an emphasis on such products that relate to threats of terrorism and other threats, including targeted violence, to surface transportation assets that—

(1) assist State, local, and Tribal law enforcement agencies in deploying their resources, including personnel, most efficiently to help detect, prevent, investigate, apprehend, and respond to such threats;

(2) promote more consistent and timely sharing with and among jurisdictions of threat information; and

(3) enhance the Department of Homeland Security's situational awareness of such threats.

**(c) Clearances**

The Secretary of Homeland Security shall make available to appropriate owners and operators of surface transportation assets, and to any other person that the Secretary determines appropriate to foster greater sharing of classified information relating to threats of terrorism and other threats, including targeted violence, to surface transportation assets, the process of application for security clearances under Executive Order No. 13549 (75 Fed. Reg. 162;[1] relating to a classified national security information program) or any successor Executive order.

**(d) Report to Congress**

Not later than one year after December 27, 2021, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes a detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out this section.

**(e) GAO report**

Not later than two years after December 27, 2021, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a review of the implementation of this section, including an assessment of the measures used to ensure privacy rights, civil rights, and civil liberties protections, and any recommendations to improve this implementation, together with any recommendations to improve information sharing with State, local, Tribal, territorial, and private sector entities to prevent, identify, and respond to threats of terrorism and other threats, including targeted violence, to surface transportation assets.

**(f) Definitions**

In this section:

(1) The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

(A) a public transportation agency (as such term is defined in section 1131(5) of this title);

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49);

(C) an owner or operator of—

(i) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as such term is defined in section 1151(4) of this title); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(2) The term ''targeted violence'' means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(3) The term ''terrorism'' means the terms—

(A) domestic terrorism (as such term is defined in section 2331(5) of title 18, United States Code); and

(B) international terrorism (as such term is defined in section 2331(1) of title 18).

(Pub. L. 117–81, div. F, title LXIV, § 6418, Dec. 27, 2021, 135 Stat. 2415.)

**Editorial Notes**

REFERENCES IN TEXT

Executive Order No. 13549, referred to in subsec. (c), is Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, which is set out as a note under section 3161 of Title 50, War and National Defense.

CODIFICATION

Section was enacted as part of the National Defense Authorization Act for Fiscal Year 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

## § 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;

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

(ii) identify information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is of interest to State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers;

(iii) assist Department analysts in preparing and disseminating products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal law enforcement officers and intelligence analysts and designed to prepare for and thwart acts of terrorism; and

(iv) assist Department analysts in preparing products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal emergency response providers and assist in the dissemination of such products through appropriate Department channels.

**(2) Program name**

The program under this section shall be known as the ''Homeland Security Information Sharing Fellows Program''.

**(b) Eligibility**

**(1) In general**

In order to be eligible for selection as an Information Sharing Fellow under the program under this section, an individual shall—

(A) have homeland security-related responsibilities;

(B) be eligible for an appropriate security clearance;

(C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis;

(D) be an employee of an eligible entity; and

(E) have undergone appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer and the Officer for Civil Rights and Civil Liberties, in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42.

**(2) Eligible entities**

In this subsection, the term ''eligible entity'' means—

(A) a State, local, or regional fusion center;

(B) a State or local law enforcement or other government entity that serves a major metropolitan area, suburban area, or rural area, as determined by the Secretary;

(C) a State or local law enforcement or other government entity with port, border, or agricultural responsibilities, as determined by the Secretary;

(D) a tribal law enforcement or other authority; or

(E) such other entity as the Secretary determines is appropriate.

**(c) Optional participation**

No State, local, or tribal law enforcement or other government entity shall be required to participate in the Homeland Security Information Sharing Fellows Program.

**(d) Procedures for nomination and selection**

**(1) In general**

The Under Secretary for Intelligence and Analysis shall establish procedures to provide for the nomination and selection of individuals to participate in the Homeland Security Information Sharing Fellows Program.

**(2) Limitations**

The Under Secretary for Intelligence and Analysis shall—

(A) select law enforcement officers and intelligence analysts representing a broad cross-section of State, local, and tribal agencies; and

(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis.

(Pub. L. 107–296, title II, § 210B, as added Pub. L. 110–53, title V, § 512(a), Aug. 3, 2007, 121 Stat. 324.)

### § 124j. Rural Policing Institute

**(a) In general**

The Secretary shall establish a Rural Policing Institute, which shall be administered by the Federal Law Enforcement Training Center, to target training to law enforcement agencies and other emergency response providers located in rural areas. The Secretary, through the Rural Policing Institute, shall—

(1) evaluate the needs of law enforcement agencies and other emergency response providers in rural areas;

(2) develop expert training programs designed to address the needs of law enforcement agencies and other emergency response providers in rural areas as identified in the evaluation conducted under paragraph (1), including training programs about intelligence-led policing and protections for privacy, civil rights, and civil liberties;

(3) provide the training programs developed under paragraph (2) to law enforcement agencies and other emergency response providers in rural areas; and

(4) conduct outreach efforts to ensure that local and tribal governments in rural areas are aware of the training programs developed under paragraph (2) so they can avail themselves of such programs.

**(b) Curricula**

The training at the Rural Policing Institute established under subsection (a) shall—

(1) be configured in a manner so as not to duplicate or displace any law enforcement or emergency response program of the Federal Law Enforcement Training Center or a local or tribal government entity in existence on August 3, 2007; and

(2) to the maximum extent practicable, be delivered in a cost-effective manner at facilities of the Department, on closed military installations with adequate training facilities, or at facilities operated by the participants.

**(c) Definition**

In this section, the term ''rural'' means an area that is not located in a metropolitan statistical area, as defined by the Office of Management and Budget.

**(d) Authorization of appropriations**

There are authorized to be appropriated to carry out this section (including for contracts, staff, and equipment)—

(1) $10,000,000 for fiscal year 2008; and

(2) $5,000,000 for each of fiscal years 2009 through 2013.

(Pub. L. 107–296, title II, § 210C, as added Pub. L. 110–53, title V, § 513(a), Aug. 3, 2007, 121 Stat. 327.)

**Statutory Notes and Related Subsidiaries**

RURAL AREA

Pub. L. 112–74, div. D, title V, § 546, Dec. 23, 2011, 125 Stat. 977, provided that: ''For fiscal year 2012 and thereafter, for purposes of section 210C of the Homeland Security Act of 2002 (6 U.S.C. 124j), a rural area shall also include any area that is located in a metropolitan statistical area and a county, borough, parish, or area under the jurisdiction of an Indian tribe with a population of not more than 50,000.''

## § 124k. Interagency Threat Assessment and Coordination Group

**(a) In general**

To improve the sharing of information within the scope of the information sharing environment established under section 485 of this title with State, local, tribal, and private sector officials, the Director of National Intelligence, through the program manager for the information sharing environment, in coordination with the Secretary, shall coordinate and oversee the creation of an Interagency Threat Assessment and Coordination Group (referred to in this section as the ''ITACG'').

**(b) Composition of ITACG**

The ITACG shall consist of—

(1) an ITACG Advisory Council to set policy and develop processes for the integration, analysis, and dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(2) an ITACG Detail comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work in the National Counterterrorism Center with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, through appropriate channels identified by the ITACG Advisory Council.

**(c) Responsibilities of Secretary**

The Secretary, or the Secretary's designee, in coordination with the Director of the National Counterterrorism Center and the ITACG Advisory Council, shall—

(1) create policies and standards for the creation of information products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are suitable for dissemination to State, local, and tribal governments and the private sector;

(2) evaluate and develop processes for the timely dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal governments and the private sector;

(3) establish criteria and a methodology for indicating to State, local, and tribal governments and the private sector the reliability of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, disseminated to them;

(4) educate the intelligence community about the requirements of the State, local, and tribal homeland security, law enforcement, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(5) establish and maintain the ITACG Detail, which shall assign an appropriate number of State, local, and tribal homeland security and law enforcement officers and intelligence analysts to work in the National Counterterrorism Center who shall—

(A) educate and advise National Counterterrorism Center intelligence analysts about the requirements of the State, local, and tribal homeland security and law enforcement officers, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(B) assist National Counterterrorism Center intelligence analysts in integrating, analyzing, and otherwise preparing versions of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information that are unclassified or classified at the lowest possible level and suitable for dissemination to State, local, and tribal homeland security and law enforcement agencies in order to help deter and prevent terrorist attacks;

(C) implement, in coordination with National Counterterrorism Center intelligence analysts, the policies, processes, procedures,

standards, and guidelines developed by the ITACG Advisory Council;

(D) assist in the dissemination of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal jurisdictions only through appropriate channels identified by the ITACG Advisory Council;

(E) make recommendations, as appropriate, to the Secretary or the Secretary's designee, for the further dissemination of intelligence products that could likely inform or improve the security of a State, local, or tribal government, (including a State, local, or tribal law enforcement agency) or a private sector entity; and

(F) report directly to the senior intelligence official from the Department under paragraph (6);

(6) detail a senior intelligence official from the Department of Homeland Security to the National Counterterrorism Center, who shall—

(A) manage the day-to-day operations of the ITACG Detail;

(B) report directly to the Director of the National Counterterrorism Center or the Director's designee; and

(C) in coordination with the Director of the Federal Bureau of Investigation, and subject to the approval of the Director of the National Counterterrorism Center, select a deputy from the pool of available detailees from the Federal Bureau of Investigation in the National Counterterrorism Center;

(7) establish, within the ITACG Advisory Council, a mechanism to select law enforcement officers and intelligence analysts for placement in the National Counterterrorism Center consistent with paragraph (5), using criteria developed by the ITACG Advisory Council that shall encourage participation from a broadly representative group of State, local, and tribal homeland security and law enforcement agencies; and

(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies) and private sector entities.

**(d) Membership**

The Secretary, or the Secretary's designee, shall serve as the chair of the ITACG Advisory Council, which shall include—

(1) representatives of—

(A) the Department;

(B) the Federal Bureau of Investigation;

(C) the National Counterterrorism Center;

(D) the Department of Defense;

(E) the Department of Energy;

(F) the Department of State; and

(G) other Federal entities as appropriate;

(2) the program manager of the information sharing environment, designated under section 485(f) of this title, or the program manager's designee; and

(3) executive level law enforcement and intelligence officials from State, local, and tribal governments.

**(e) Criteria**

The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the program manager of the information sharing environment established under section 485 of this title, shall—

(1) establish procedures for selecting members of the ITACG Advisory Council and for the proper handling and safeguarding of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by those members; and

(2) ensure that at least 50 percent of the members of the ITACG Advisory Council are from State, local, and tribal governments.

**(f) Operations**

**(1) In general**

Beginning not later than 90 days after August 3, 2007, the ITACG Advisory Council shall meet regularly, but not less than quarterly, at the facilities of the National Counterterrorism Center of the Office of the Director of National Intelligence.

**(2) Management**

Pursuant to section 3056(f)(E)[1] of title 50, the Director of the National Counterterrorism Center, acting through the senior intelligence official from the Department of Homeland Security detailed pursuant to subsection (d)(6),[2] shall ensure that—

(A) the products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, prepared by the National Counterterrorism Center and the ITACG Detail for distribution to State, local, and tribal homeland security and law enforcement agencies reflect the requirements of such agencies and are produced consistently with the policies, processes, procedures, standards, and guidelines established by the ITACG Advisory Council;

(B) in consultation with the ITACG Advisory Council and consistent with sections 3024(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)[2] have appropriate access to all relevant information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction informa-

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

[2] See References in Text note below.

tion, available at the National Counterterrorism Center in order to accomplish the objectives under that paragraph;

(D) all detailees under subsection (d)(5)[2] have the appropriate security clearances and are trained in the procedures for handling, processing, storing, and disseminating classified products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(E) all detailees under subsection (d)(5)[2] complete appropriate privacy and civil liberties training.

**(g) Inapplicability of chapter 10 of title 5**

Chapter 10 of title 5 shall not apply to the ITACG or any subsidiary groups thereof.

**(h) Authorization of appropriations**

There are authorized to be appropriated such sums as may be necessary for each of fiscal years 2008 through 2012 to carry out this section, including to obtain security clearances for the State, local, and tribal participants in the ITACG.

(Pub. L. 107–296, title II, §210D, as added Pub. L. 110–53, title V, §521(a), Aug. 3, 2007, 121 Stat. 328; amended Pub. L. 111–258, §5(b)(2), (c), Oct. 7, 2010, 124 Stat. 2650, 2651; Pub. L. 116–92, div. E, title LXVII, §6726(b), Dec. 20, 2019, 133 Stat. 2236; Pub. L. 117–286, §4(a)(12), Dec. 27, 2022, 136 Stat. 4306.)

**Editorial Notes**

REFERENCES IN TEXT

Subsection (d)(5) and (6), referred to in subsec. (f)(2), was redesignated subsec. (c)(5) and (6), respectively, by Pub. L. 116–92, div. E, title LXVII, §6726(b)(2), Dec. 20, 2019, 133 Stat. 2236.

AMENDMENTS

2022—Subsec. (g). Pub. L. 117–286, which directed amendment of subsec. (h) by substituting ''chapter 10 of title 5'' for ''the Federal Advisory Committee Act'' in heading and ''Chapter 10 of title 5'' for ''The Federal Advisory Committee Act (5 U.S.C. App.)'' in text, was executed by making the substitutions in subsec. (g) to reflect the probable intent of Congress and the prior amendment by Pub. L. 116–92. See 2019 Amendment below.

2019—Subsec. (c). Pub. L. 116–92, §6726(b)(1), (2), redesignated subsec. (d) as (c) and struck out former subsec. (c) which related to responsibilities of program manager.

Subsec. (c)(9). Pub. L. 116–92, §6726(b)(3), struck out par. (9) which read as follows: ''provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2).''

Subsecs. (d) to (i). Pub. L. 116–92, §6726(b)(2), redesignated subsecs. (e) to (i) as (d) to (h), respectively.

2010—Subsec. (c). Pub. L. 111–258, §5(c)(1), struck out '', in consultation with the Information Sharing Council,'' after ''program manager'' in introductory provisions.

Subsec. (c)(3). Pub. L. 111–258, §5(c)(2)–(4), added par. (3).

Subsec. (d)(5)(E), (F). Pub. L. 111–258, §5(b)(2)(A), added subpar. (E) and redesignated former subpar. (E) as (F).

Subsec. (d)(8), (9). Pub. L. 111–258, §5(b)(2)(B)–(D), added pars. (8) and (9).

## § 124*l*. Transferred

**Editorial Notes**

CODIFICATION

Section, Pub. L. 107–296, title II, §210E, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372, which related to national asset database, was renumbered section 2214 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(G), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 664 of this title.

## § 124m. Classified Information Advisory Officer

**(a) Requirement to establish**

The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

**(b) Responsibilities**

The responsibilities of the Classified Information Advisory Officer shall be as follows:

(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies) and private sector entities—

(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

(C) on the means by which such personnel may apply for security clearances.

(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

**(c) Initial designation**

Not later than 90 days after October 7, 2010, the Secretary shall—

(1) designate the initial Classified Information Advisory Officer; and

(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a written notification of the designation.

(Pub. L. 107–296, title II, §210E, formerly §210F, as added Pub. L. 111–258, §4(a), Oct. 7, 2010, 124 Stat. 2649; renumbered §210E, Pub. L. 115–278, §2(g)(2)(J), Nov. 16, 2018, 132 Stat. 4178.)

**Editorial Notes**

PRIOR PROVISIONS

A prior section 210E of Pub. L. 107–296, title II, as added Pub. L. 110–53, title X, §1001(a), Aug. 3, 2007, 121 Stat. 372, was renumbered section 2214 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(G), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 664 of this title.

**Statutory Notes and Related Subsidiaries**

FINDINGS

Pub. L. 111–258, §2, Oct. 7, 2010, 124 Stat. 2648, provided that: ''Congress finds the following:

''(1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the '9/11 Commission') concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.

''(2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

''(3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.

''(4) Over-classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

''(5) Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification markings and the policies of the National Archives and Records Administration.''

### § 124m–1. Departmental coordination on counter threats

#### (a) Establishment

There is authorized in the Department, for a period of 2 years beginning after December 27, 2020, a Counter Threats Advisory Board (in this section referred to as the ''Board'') which shall—

(1) be composed of senior representatives of departmental operational components and headquarters elements; and

(2) coordinate departmental intelligence activities and policy and information related to the mission and functions of the Department that counter threats.

#### (b) Charter

There shall be a charter to govern the structure and mission of the Board, which shall—

(1) direct the Board to focus on the current threat environment and the importance of aligning departmental activities to counter threats under the guidance of the Secretary; and

(2) be reviewed and updated as appropriate.

#### (c) Members

##### (1) In general

The Board shall be composed of senior representatives of departmental operational components and headquarters elements.

##### (2) Chair

The Under Secretary for Intelligence and Analysis shall serve as the Chair of the Board.

##### (3) Members

The Secretary shall appoint additional members of the Board from among the following:

(A) The Transportation Security Administration.

(B) U.S. Customs and Border Protection.

(C) U.S. Immigration and Customs Enforcement.

(D) The Federal Emergency Management Agency.

(E) The Coast Guard.

(F) U.S. Citizenship and Immigration Services.

(G) The United States Secret Service.

(H) The Cybersecurity and Infrastructure Security Agency.

(I) The Office of Operations Coordination.

(J) The Office of the General Counsel.

(K) The Office of Intelligence and Analysis.

(L) The Office of Strategy, Policy, and Plans.

(M) The Science and Technology Directorate.

(N) The Office for State and Local Law Enforcement.

(O) The Privacy Office.

(P) The Office for Civil Rights and Civil Liberties.

(Q) Other departmental offices and programs as determined appropriate by the Secretary.

#### (d) Meetings

The Board shall—

(1) meet on a regular basis to discuss intelligence and coordinate ongoing threat mitigation efforts and departmental activities, including coordination with other Federal, State, local, tribal, territorial, and private sector partners; and

(2) make recommendations to the Secretary.

#### (e) Terrorism alerts

The Board shall advise the Secretary on the issuance of terrorism alerts under section 124 of this title.

#### (f) Prohibition on additional funds

No additional funds are authorized to carry out this section.

(Pub. L. 107–296, title II, § 210F, as added Pub. L. 116–260, div. U, title VI, § 602(a), Dec. 27, 2020, 134 Stat. 2294.)

#### Editorial Notes

PRIOR PROVISIONS

A prior section 210F of Pub. L. 107–296 was renumbered section 210E and is classified to section 124m of this title.

#### Statutory Notes and Related Subsidiaries

NOTICE REGARDING MECHANISMS TO COORDINATE THREATS

Pub. L. 116–260, div. U, title VI, § 602(d), Dec. 27, 2020, 134 Stat. 2295, provided that: ''The Secretary of Homeland Security shall provide written notification to and brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on any changes to or introductions of new mechanisms to coordinate threats across the Department of Homeland Security.''

### § 124n. Protection of certain facilities and assets from unmanned aircraft

#### (a) Authority

Notwithstanding section 46502 of title 49 or sections 32, 1030, 1367 and chapters 119 and 206 of

title 18, the Secretary and the Attorney General may, for their respective Departments, take, and may authorize personnel with assigned duties that include the security or protection of people, facilities, or assets, to take such actions as are described in subsection (b)(1) that are necessary to mitigate a credible threat (as defined by the Secretary or the Attorney General, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

**(b) Actions described**

**(1) In general**

The actions authorized in subsection (a) are the following:

(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

**(2) Required coordination**

The Secretary and the Attorney General shall develop for their respective Departments the actions described in paragraph (1) in coordination with the Secretary of Transportation.

**(3) Research, testing, training, and evaluation**

The Secretary and the Attorney General shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b)(1).

**(4) Coordination**

The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration when any action authorized by this section might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

**(c) Forfeiture**

Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary or the Attorney General is subject to forfeiture to the United States.

**(d) Regulations and guidance**

**(1) In general**

The Secretary, the Attorney General, and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary or the Attorney General to carry out this section.

**(2) Coordination**

**(A) Coordination with Department of Transportation**

The Secretary and the Attorney General shall coordinate the development of their respective guidance under paragraph (1) with the Secretary of Transportation.

**(B) Effect on aviation safety**

The Secretary and the Attorney General shall respectively coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, if such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

**(e) Privacy protection**

The regulations or guidance issued to carry out actions authorized under subsection (b) by each Secretary or the Attorney General, as the case may be, shall ensure that—

(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are intercepted or acquired only to the extent necessary to support an action described in subsection (b)(1);

(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary of Homeland Security or the Attorney General determine[1] that maintenance of such records is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, is required under Federal law, or for the purpose of any litigation;

(4) such communications are not disclosed outside the Department of Homeland Security or the Department of Justice unless the disclosure—

(A) is necessary to investigate or prosecute a violation of law;

(B) would support the Department of Defense, a Federal law enforcement agency, or

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

the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to an action described in subsection (b)(1);

(C) is between the Department of Homeland Security and the Department of Justice in the course of a security or protection operation of either agency or a joint operation of such agencies; or

(D) is otherwise required by law; and

(5) to the extent necessary, the Department of Homeland Security and the Department of Justice are authorized to share threat information, which shall not include communications referred to in subsection (b), with State, local, territorial, or tribal law enforcement agencies in the course of a security or protection operation.

**(f) Budget**

The Secretary and the Attorney General shall submit to Congress, as a part of the homeland security or justice budget materials for each fiscal year after fiscal year 2019, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of Homeland Security or the Department of Justice. The funding display shall be in unclassified form, but may contain a classified annex.

**(g) Semiannual briefings and notifications**

**(1) In general**

On a semiannual basis during the period beginning 6 months after October 5, 2018, and ending on the date specified in subsection (i), the Secretary and the Attorney General shall, respectively, provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section.

**(2) Requirement**

Each briefing required under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

**(3) Content**

Each briefing required under paragraph (1) shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances in which actions described in subsection (b)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

(C) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights or civil liberties;

(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1);

(E) a description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system were held for more than 180 days or shared outside of the Department of Justice or the Department of Homeland Security;

(F) how the Secretary, the Attorney General, and the Secretary of Transportation have informed the public as to the possible use of authorities under this section; [2]

(G) how the Secretary, the Attorney General, and the Secretary of Transportation have engaged with Federal, State, and local law enforcement agencies to implement and use such authorities.

**(4) Unclassified form**

Each briefing required under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

**(5) Notification**

Within 30 days of deploying any new technology to carry out the actions described in subsection (b)(1), the Secretary and the Attorney General shall, respectively, submit a notification to the appropriate congressional committees. Such notification shall include a description of options considered to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

**(h) Rule of construction**

Nothing in this section may be construed to—

(1) vest in the Secretary or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration;

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary or the Attorney General;

(3) vest in the Secretary of Homeland Security any authority of the Attorney General;

(4) vest in the Attorney General any authority of the Secretary of Homeland Security; or

(5) provide a new basis of liability for any State, local, territorial, or tribal law enforcement officers who participate in the protection of a mass gathering identified by the Secretary or Attorney General under subsection (k)(3)(C)(iii)(II), act within the scope of their authority, and do not exercise the authority granted to the Secretary and Attorney General by this section.

**(i) Termination**

The authority to carry out this section with respect to a covered facility or asset specified in subsection (k)(3) shall terminate on February 3, 2024.

---

[2] So in original. Probably should be followed by ''and''.

**(j) Scope of authority**

Nothing in this section shall be construed to provide the Secretary or the Attorney General with additional authorities beyond those described in subsections (a) and (k)(3)(C)(iii).

**(k) Definitions**

In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Homeland Security, the Committee on Transportation and Infrastructure, the Committee on Energy and Commerce, and the Committee on the Judiciary of the House of Representatives.

(2) The term ''budget'', with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) The term ''covered facility or asset'' means any facility or asset that—

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section (except that in the case of the missions described in subparagraph (C)(i)(II) and (C)(iii)(I), such missions shall be presumed to be for the protection of a facility or asset that is assessed to be high-risk and a potential target for unlawful unmanned aircraft activity);

(B) is located in the United States (including the territories and possessions, territorial seas or navigable waters of the United States); and

(C) directly relates to one or more—

(i) missions authorized to be performed by the Department of Homeland Security, consistent with governing statutes, regulations, and orders issued by the Secretary, pertaining to—

(I) security or protection functions of the U.S. Customs and Border Protection, including securing or protecting facilities, aircraft, and vessels, whether moored or underway;

(II) United States Secret Service protection operations pursuant to sections 3056(a) and 3056A(a) of title 18 and the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note); or

(III) protection of facilities pursuant to section 1315(a) of title 40;

(ii) missions authorized to be performed by the Department of Justice, consistent with governing statutes, regulations, and orders issued by the Attorney General, pertaining to—

(I) personal protection operations by—

(aa) the Federal Bureau of Investigation as specified in section 533 of title 28; and

(bb) the United States Marshals Service of Federal jurists, court officers, witnesses, and other threatened persons in the interests of justice, as specified in section 566(e)(1)(A) of title 28;

(II) protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons; or

(III) protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice, and the provision of security for Federal courts, as specified in section 566(a) of title 28;

(iii) missions authorized to be performed by the Department of Homeland Security or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and orders issued by the Secretary or the Attorney General, respectively, pertaining to—

(I) protection of a National Special Security Event and Special Event Assessment Rating event;

(II) the provision of support to State, local, territorial, or tribal law enforcement, upon request of the chief executive officer of the State or territory, to ensure protection of people and property at mass gatherings, that is limited to a specified timeframe and location, within available resources, and without delegating any authority under this section to State, local, territorial, or tribal law enforcement; or

(III) protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified timeframe and location; and[3]

(iv) missions authorized to be performed by the United States Coast Guard, including those described in clause (iii) as directed by the Secretary, and as further set forth in section 104[4] of title 14, and consistent with governing statutes, regulations, and orders issued by the Secretary of the Department in which the Coast Guard is operating.

(4) The terms ''electronic communication'', ''intercept'', ''oral communication'', and ''wire communication'' have the meaning[5] given those terms in section 2510 of title 18.

(5) The term ''homeland security or justice budget materials'', with respect to a fiscal year, means the materials submitted to Congress by the Secretary and the Attorney General in support of the budget for that fiscal year.

(6) For purposes of subsection (a), the term ''personnel'' means officers and employees of the Department of Homeland Security or the Department of Justice.

---

[3] So in original. Probably should be ''or''.

[4] See References in Text note below.

[5] So in original. Probably should be ''meanings''.

(7) The terms ''unmanned aircraft'' and ''unmanned aircraft system'' have the meanings given those terms in section 44801,[6] of title 49.

(8) For purposes of this section, the term ''risk-based assessment'' includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Secretary or the Attorney General, respectively, of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the use of any system or technology for carrying out the actions described in subsection (b)(1).

(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(C) Potential consequences of the impacts of any actions taken under subsection (b)(1) to the national airspace system and infrastructure if not mitigated.

(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and any potential for interference with wireless communications or for injury or damage to persons or property.

(F) The setting, character, timeframe, and national airspace system impacts of National Special Security Event and Special Event Assessment Rating events.

(G) Potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated.

**(*l*) Department of Homeland Security assessment**

**(1) Report**

Not later than 1 year after October 5, 2018, the Secretary shall conduct, in coordination with the Attorney General and the Secretary of Transportation, an assessment to the appropriate congressional committees, including—

(A) an evaluation of the threat from unmanned aircraft systems to United States critical infrastructure (as defined in this chapter) and to domestic large hub airports (as defined in section 40102 of title 49);

(B) an evaluation of current Federal and[7] State, local, territorial, or tribal law enforcement authorities to counter the threat identified in subparagraph (A), and recommendations, if any, for potential changes to existing authorities to allow State, local, territorial, and tribal law enforcement to assist Federal law enforcement to counter the threat where appropriate;

(C) an evaluation of the knowledge of, efficiency of, and effectiveness of current procedures and resources available to owners of critical infrastructure and domestic large hub airports when they believe a threat from unmanned aircraft systems is present and what additional actions, if any, the Department of Homeland Security or the Department of Transportation could implement under existing authorities to assist these entities to counter the threat identified in subparagraph (A);

(D) an assessment of what, if any, additional authorities are needed by each Department and law enforcement to counter the threat identified in subparagraph (A); and

(E) an assessment of what, if any, additional research and development the Department needs to counter the threat identified in subparagraph (A).

**(2) Unclassified form**

The report required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(Pub. L. 107–296, title II, § 210G, as added Pub. L. 115–254, div. H, § 1602(a), Oct. 5, 2018, 132 Stat. 3522; amended Pub. L. 118–15, div. B, title II, § 2221, Sept. 30, 2023, 137 Stat. 86; Pub. L. 118–22, div. B, title III, § 601, Nov. 17, 2023, 137 Stat. 123.)

**Editorial Notes**

REFERENCES IN TEXT

The Presidential Protection Assistance Act of 1976, referred to in subsec. (k)(3)(C)(i)(II), is Pub. L. 94–524, Oct. 17, 1976, 90 Stat. 2475, which enacted and amended provisions set out as notes under section 3056 of Title 18, Crimes and Criminal Procedure. For complete classification of this Act to the Code, see Tables.

Section 104 of title 14, referred to in subsec. (k)(3)(C)(iv), was redesignated section 528 of title 14 by Pub. L. 115–282, title I, § 105(b), Dec. 4, 2018, 132 Stat. 4200, and references to section 104 of title 14 deemed to refer to such redesignated section, see section 123(b)(1) of Pub. L. 115–282, set out as a References to Sections of Title 14 as Redesignated by Pub. L. 115–282 note preceding section 101 of Title 14, Coast Guard.

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

AMENDMENTS

2023—Subsec. (i). Pub. L. 118–22 substituted ''February 3, 2024'' for ''November 18, 2023''.

Pub. L. 118–15 substituted ''on November 18, 2023'' for ''on the date that is 4 years after October 5, 2018''.

[6] So in original. The comma probably should not appear.

[7] So in original. Probably should be ''Federal,''.

**Statutory Notes and Related Subsidiaries**

TERMINATION DATE

Pub. L. 117–328, div. F, title V, §547, Dec. 29, 2022, 136 Stat. 4758, provided that: ''Section 210G(i) of the Homeland Security Act of 2002 (6 U.S.C. 124n(i)) shall be applied by substituting 'September 30, 2023' for 'the date that is 4 years after the date of enactment of this section [Oct. 5, 2018]'.''

## § 125. Annual report on intelligence activities of the Department of Homeland Security

### (a) In general

For each fiscal year and along with the budget materials submitted in support of the budget of the Department of Homeland Security pursuant to section 1105(a) of title 31, the Under Secretary for Intelligence and Analysis of the Department shall submit to the congressional intelligence committees a report for such fiscal year on each intelligence activity of each intelligence component of the Department, as designated by the Under Secretary, that includes the following:

(1) The amount of funding requested for each such intelligence activity.

(2) The number of full-time employees funded to perform each such intelligence activity.

(3) The number of full-time contractor employees (or the equivalent of full-time in the case of part-time contractor employees) funded to perform or in support of each such intelligence activity.

(4) A determination as to whether each such intelligence activity is predominantly in support of national intelligence or departmental missions.

(5) The total number of analysts of the Intelligence Enterprise of the Department that perform—

(A) strategic analysis; or

(B) operational analysis.

### (b) Feasibility and advisability report

Not later than 120 days after December 19, 2014, the Secretary of Homeland Security, acting through the Under Secretary for Intelligence and Analysis, shall submit to the congressional intelligence committees a report that—

(1) examines the feasibility and advisability of including the budget request for all intelligence activities of each intelligence component of the Department that predominantly support departmental missions, as designated by the Under Secretary for Intelligence and Analysis, in the Homeland Security Intelligence Program; and

(2) includes a plan to enhance the coordination of department-wide intelligence activities to achieve greater efficiencies in the performance of the Department of Homeland Security intelligence functions.

### (c) Intelligence component of the Department

In this section, the term ''intelligence component of the Department'' has the meaning given that term in section 101 of this title.

(Pub. L. 113–293, title III, §324, Dec. 19, 2014, 128 Stat. 4004.)

**Editorial Notes**

CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

**Statutory Notes and Related Subsidiaries**

BRIEFING ON DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ACTIVITIES

Pub. L. 117–263, div. F, title LXVIII, §6819, Dec. 23, 2022, 136 Stat. 3611, provided that:

''(a) DEFINITIONS.—In this section:

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

''(A) The congressional intelligence committees.

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

''(C) The Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

''(2) COMPONENT OF THE DEPARTMENT OF HOMELAND SECURITY.—The term 'component of the Department of Homeland Security' means the following components of the Department of Homeland Security:

''(A) The Cybersecurity and Infrastructure Security Agency Threat Management Division.

''(B) The Federal Emergency Management Agency Protection and National Preparedness, Office of Counterterrorism and Security Preparedness.

''(C) The Transportation Security Administration Office of Intelligence and Analysis.

''(D) The United States Citizenship and Immigration Services Fraud Detection and National Security Directorate, Field Operations Directorate, and Collateral Duty Intelligence.

''(E) The United States Customs and Border Protection Office of Intelligence.

''(F) The United States Immigration and Customs Enforcement Homeland Security Investigations, Office of Intelligence, and Special Agent in Charge Intelligence Program.

''(3) INTELLIGENCE ACTIVITY.—The term 'intelligence activity' shall be interpreted consistent with how such term is used in section 502 of the National Security Act of 1947 (50 U.S.C. 3092).

''(b) BRIEFING ON INTELLIGENCE ACTIVITIES.—Consistent with section 501 of the National Security Act of 1947 (50 U.S.C. 3091), not later than 30 days after the date of the enactment of this Act [Dec. 23, 2022], the Chief Intelligence Officer of the Department of Homeland Security shall provide the appropriate congressional committees a briefing on the intelligence activities of elements of the Department of Homeland Security that are not elements of the intelligence community. Such briefing shall include the following:

''(1) A comprehensive description of all intelligence activities conducted during the period beginning on January 1, 2018, and ending on the date of the briefing, by any component of the Department of Homeland Security that conducts intelligence activities.

''(2) With respect to each such intelligence activity, a description of the activity, including, at a minimum—

''(A) the nature of the activity;

''(B) the component undertaking the activity;

''(C) the legal authority for such activity; and

''(D) the source of funding for such activity.

''(3) A description and the quantity of any types of finished intelligence products, or intelligence information reports, produced or contributed to by a component of the Department of Homeland Security that conducts intelligence activities during the period specified in paragraph (1).

''(4) An identification of any external or internal guidelines, policies, processes, practices, or programs governing the collection, retention, analysis, or dissemination by such a component of information regarding United States citizens, lawful permanent residents of the United States, or individuals located within the United States.

''(c) FORM.—The briefing under subsection (b) may be provided in classified form.

''(d) ADDITIONAL BRIEFINGS.—Not later than 1 year after the date on which the Chief Intelligence Officer provides the briefing under subsection (b) and not less frequently than once each year thereafter, the Chief Intelligence Officer shall provide the appropriate congressional committees a briefing on any new intelligence activities commenced by any component of the Department of Homeland Security and any that have been terminated.''

[For definitions of ''congressional intelligence committees'' and ''intelligence community'' as used in section 6819 of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of Title 50, War and National Defense.]

DEFINITIONS

''Congressional intelligence committees'' means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives, see section 2 of Pub. L. 113–293, set out as a note under section 3003 of Title 50, War and National Defense.

### § 126. Department of Homeland Security data framework

**(a) In general**

**(1) Development**

The Secretary of Homeland Security shall develop a data framework to integrate existing Department of Homeland Security datasets and systems, as appropriate, for access by authorized personnel in a manner consistent with relevant legal authorities and privacy, civil rights, and civil liberties policies and protections.

**(2) Requirements**

In developing the framework required under paragraph (1), the Secretary of Homeland Security shall ensure, in accordance with all applicable statutory and regulatory requirements, the following information is included:

(A) All information acquired, held, or obtained by an office or component of the Department of Homeland Security that falls within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence.

(B) Any information or intelligence relevant to priority mission needs and capability requirements of the homeland security enterprise, as determined appropriate by the Secretary.

**(b) Data framework access**

**(1) In general**

The Secretary of Homeland Security shall ensure that the data framework required under this section is accessible to employees of the Department of Homeland Security who the Secretary determines—

(A) have an appropriate security clearance;

(B) are assigned to perform a function that requires access to information in such framework; and

(C) are trained in applicable standards for safeguarding and using such information.

**(2) Guidance**

The Secretary of Homeland Security shall—

(A) issue guidance for Department of Homeland Security employees authorized to access and contribute to the data framework pursuant to paragraph (1); and

(B) ensure that such guidance enforces a duty to share between offices and components of the Department when accessing or contributing to such framework for mission needs.

**(3) Efficiency**

The Secretary of Homeland Security shall promulgate data standards and instruct components of the Department of Homeland Security to make available information through the data framework required under this section in a machine-readable standard format, to the greatest extent practicable.

**(c) Exclusion of information**

The Secretary of Homeland Security may exclude information from the data framework required under this section if the Secretary determines inclusion of such information may—

(1) jeopardize the protection of sources, methods, or activities;

(2) compromise a criminal or national security investigation;

(3) be inconsistent with other Federal laws or regulations; or

(4) be duplicative or not serve an operational purpose if included in such framework.

**(d) Safeguards**

The Secretary of Homeland Security shall incorporate into the data framework required under this section systems capabilities for auditing and ensuring the security of information included in such framework. Such capabilities shall include the following:

(1) Mechanisms for identifying insider threats.

(2) Mechanisms for identifying security risks.

(3) Safeguards for privacy, civil rights, and civil liberties.

**(e) Deadline for implementation**

Not later than 2 years after December 19, 2018, the Secretary of Homeland Security shall ensure the data framework required under this section has the ability to include appropriate information in existence within the Department of Homeland Security to meet the critical mission operations of the Department of Homeland Security.

**(f) Notice to Congress**

**(1) Status updates**

The Secretary of Homeland Security shall submit to the appropriate congressional committees regular updates on the status of the data framework until the framework is fully operational.

**(2) Operational notification**

Not later than 60 days after the date on which the data framework required under this section is fully operational, the Secretary of Homeland Security shall provide notice to the appropriate congressional committees that the data framework is fully operational.

**(3) Value added**

The Secretary of Homeland Security shall annually brief Congress on component use of

the data framework required under this section to support operations that disrupt terrorist activities and incidents in the homeland.

**(g) Definitions**

In this section:

**(1) Appropriate congressional committee; homeland**

The terms ''appropriate congressional committee'' and ''homeland'' have the meaning given those terms in section 101 of this title.

**(2) Homeland security information**

The term ''homeland security information'' has the meaning given such term in section 482 of this title.

**(3) National intelligence**

The term ''national intelligence'' has the meaning given such term in section 3003(5) of title 50.

**(4) Terrorism information**

The term ''terrorism information'' has the meaning given such term in section 485 of this title.

(Pub. L. 115–331, §2, Dec. 19, 2018, 132 Stat. 4484.)

**Editorial Notes**

CODIFICATION

Section was enacted as part of the Department of Homeland Security Data Framework Act of 2018, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

PART B—INFORMATION SECURITY

**Editorial Notes**

CODIFICATION

Subtitle C of title II of Pub. L. 107–296, which was classified to part C of this subchapter, was redesignated subtitle B of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

PRIOR PROVISIONS

A prior subtitle B of title II of Pub. L. 107–296, which was classified to this part, was redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to part B (§671 et seq.) of subchapter XVIII of this chapter.

## §§ 131 to 134. Transferred

**Editorial Notes**

CODIFICATION

Section 131, Pub. L. 107–296, title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961, which related to definitions, was renumbered section 2222 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 671 of this title.

Section 132, Pub. L. 107–296, title II, §213, Nov. 25, 2002, 116 Stat. 2152, which related to designation of critical infrastructure protection program, was renumbered section 2223 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 672 of this title.

Section 133, Pub. L. 107–296, title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 112–199, title I, §111, Nov. 27, 2012, 126 Stat. 1472, which related to protection of voluntarily shared critical infrastructure information, was renumbered section 2224 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 673 of this title.

Section 134, Pub. L. 107–296, title II, §215, Nov. 25, 2002, 116 Stat. 2155, which prohibited the construction of former part B as creating a private right of action for enforcement of any provision of this chapter, was renumbered section 2225 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 674 of this title.

## §141. Procedures for sharing information

The Secretary shall establish procedures on the use of information shared under this subchapter that—

(1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of such information;

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(Pub. L. 107–296, title II, §221, Nov. 25, 2002, 116 Stat. 2155.)

**Editorial Notes**

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

## §142. Privacy officer

**(a) Appointment and responsibilities**

The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. 552a];

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal in-

formation collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974 [5 U.S.C. 552a], internal controls, and other matters.

**(b) Authority to investigate**

**(1) In general**

The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

**(2) Enforcement of subpoenas**

Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

**(3) Effect of oaths**

Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

**(c) Supervision and coordination**

**(1) In general**

The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.

**(2) Coordination with the Inspector General**

**(A) In general**

Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

**(B) Coordination**

**(i) Referral**

Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

**(ii) Determinations and notifications by the Inspector General**

**(I) In general**

Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

**(II) Investigation not initiated**

If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this subclause shall be made not later than 3 days after the end of that 90-day period.

**(iii) Investigation by senior official**

The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

**(iv) Privacy training**

Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

**(d) Notification to Congress on removal**

If the Secretary removes the senior official appointed under subsection (a) or transfers that

senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

**(e) Reports by senior official to Congress**

The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

(Pub. L. 107–296, title II, §222, Nov. 25, 2002, 116 Stat. 2155; Pub. L. 108–458, title VIII, §8305, Dec. 17, 2004, 118 Stat. 3868; Pub. L. 110–53, title VIII, §802, Aug. 3, 2007, 121 Stat. 358.)

**Editorial Notes**

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsec. (a)(2), (6), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

AMENDMENTS

2007—Pub. L. 110–53 designated existing provisions as subsec. (a), inserted heading, and added subsecs. (b) to (e).

2004—Pub. L. 108–458, §8305(1), inserted '', who shall report directly to the Secretary,'' after ''in the Department'' in introductory provisions.

Pars. (5), (6). Pub. L. 108–458, §8305(2)–(4), added par. (5) and redesignated former par. (5) as (6).

## §§ 143 to 145. Transferred

**Editorial Notes**

CODIFICATION

Section 143, Pub. L. 107–296, title II, §223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, §2(e)(3)(A), Dec. 18, 2014, 128 Stat. 3086, which related to enhancement of Federal and non-Federal cybersecurity, was renumbered section 2205 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 655 of this title.

Section 144, Pub. L. 107–296, title II, §224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334, which related to NET Guard, was renumbered section 2206 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 656 of this title.

Section 145, Pub. L. 107–296, title II, §225, Nov. 25, 2002, 116 Stat. 2156, which related to Cyber Security Enhancement Act of 2002, was renumbered section 2207 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 657 of this title.

## §146. Cybersecurity workforce assessment and strategy

**(a) Workforce assessment**

**(1) In general**

Not later than 180 days after December 18, 2014, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.

**(2) Contents**

The assessment required under paragraph (1) shall include, at a minimum—

(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;

(B) information on where cybersecurity workforce positions are located within the Department;

(C) information on which cybersecurity workforce positions are—

(i) performed by—

(I) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about such employees;

(II) independent contractors; and

(III) individuals employed by other Federal agencies, including the National Security Agency; or

(ii) vacant; and

(D) information on—

(i) the percentage of individuals within each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(ii) in cases in which such essential training was not received, what challenges, if any, were encountered with respect to the provision of such essential training.

**(b) Workforce strategy**

**(1) In general**

The Secretary shall—

(A) not later than 1 year after December 18, 2014, develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).

**(2) Contents**

The comprehensive workforce strategy developed under paragraph (1) shall include a description of—

(A) a multi-phased recruitment plan, including with respect to experienced profes-

sionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

(B) a 5-year implementation plan;

(C) a 10-year projection of the cybersecurity workforce needs of the Department;

(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and

(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill any such gap.

**(c) Updates**

The Secretary submit[1] to the appropriate congressional committees annual updates on—

(1) the cybersecurity workforce assessment required under subsection (a); and

(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required to be developed under subsection (b).

(Pub. L. 113–246, § 3, Dec. 18, 2014, 128 Stat. 2880.)

**Editorial Notes**

CODIFICATION

Section was enacted as part of the Cybersecurity Workforce Assessment Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

**Statutory Notes and Related Subsidiaries**

HOMELAND SECURITY CYBERSECURITY WORKFORCE ASSESSMENT

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

''(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Workforce Assessment Act'.

''(b) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Committee on Homeland Security of the House of Representatives; and

''(C) the Committee on House Administration of the House of Representatives.

''(2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPECIALTY AREA.—The terms 'Cybersecurity Work Category', 'Data Element Code', and 'Specialty Area' have the meanings given such terms in the Office of Personnel Management's Guide to Data Standards.

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

''(4) DIRECTOR.—The term 'Director' means the Director of the Office of Personnel Management.

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

''(c) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.—

''(1) IN GENERAL.—The Secretary shall—

''(A) identify all cybersecurity workforce positions within the Department;

''(B) determine the primary Cybersecurity Work Category and Specialty Area of such positions; and

''(C) assign the corresponding Data Element Code, as set forth in the Office of Personnel Management's Guide to Data Standards which is aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report, in accordance with paragraph (2).

''(2) EMPLOYMENT CODES.—

''(A) PROCEDURES.—Not later than 90 days after the date of the enactment of this Act [Dec. 18, 2014], the Secretary shall establish procedures—

''(i) to identify open positions that include cybersecurity functions (as defined in the OPM Guide to Data Standards); and

''(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

''(B) CODE ASSIGNMENTS.—Not later than 9 months after the date of the enactment of this Act, the Secretary shall assign the appropriate employment code to—

''(i) each employee within the Department who carries out cybersecurity functions; and

''(ii) each open position within the Department that have been identified as having cybersecurity functions.

''(3) PROGRESS REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director shall submit a progress report on the implementation of this subsection to the appropriate congressional committees.

''(d) IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL NEED.—

''(1) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to subsection (c)(2)(B), and annually through 2021, the Secretary, in consultation with the Director, shall—

''(A) identify Cybersecurity Work Categories and Specialty Areas of critical need in the Department's cybersecurity workforce; and

''(B) submit a report to the Director that—

''(i) describes the Cybersecurity Work Categories and Specialty Areas identified under subparagraph (A); and

''(ii) substantiates the critical need designations.

''(2) GUIDANCE.—The Director shall provide the Secretary with timely guidance for identifying Cybersecurity Work Categories and Specialty Areas of critical need, including—

''(A) current Cybersecurity Work Categories and Specialty Areas with acute skill shortages; and

''(B) Cybersecurity Work Categories and Specialty Areas with emerging skill shortages.

''(3) CYBERSECURITY CRITICAL NEEDS REPORT.—Not later than 18 months after the date of the enactment of this Act, the Secretary, in consultation with the Director, shall—

''(A) identify Specialty Areas of critical need for cybersecurity workforce across the Department; and

''(B) submit a progress report on the implementation of this subsection to the appropriate congressional committees.

''(e) GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.—The Comptroller General of the United States shall—

''(1) analyze and monitor the implementation of subsections (c) and (d); and

''(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.''

DEFINITIONS

Pub. L. 113–246, § 2, Dec. 18, 2014, 128 Stat. 2880, provided that: ''In this Act [enacting this section and provisions set out as a note under section 101 of this title]—

''(1) the term 'Cybersecurity Category' means a position's or incumbent's primary work function involving cybersecurity, which is further defined by Specialty Area;

''(2) the term 'Department' means the Department of Homeland Security;

[1] So in original.

''(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 to 151. Transferred

### Editorial Notes

CODIFICATION

Section 147, Pub. L. 107–296, title II, §226, as added Pub. L. 113–277, §3(a), Dec. 18, 2014, 128 Stat. 3005, which related to cybersecurity recruitment and retention, was renumbered section 2208 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 658 of this title.

Section 148, Pub. L. 107–296, title II, §227, formerly §226, as added Pub. L. 113–282, §3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered §227 and amended Pub. L. 114–113, div. N, title II, §§203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963; Pub. L. 114–328, div. A, title XVIII, §1841(b), Dec. 23, 2016, 130 Stat. 2663, which related to national cybersecurity and communications integration center, was renumbered section 2209 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 659 of this title.

A prior section 227 of Pub. L. 107–296, as added by Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070, was classified to section 149 of this title prior to redesignation by Pub. L. 114–113 as section 228(c) of Pub. L. 107–296, and was classified to section 149(c) of this title prior to further redesignation by Pub. L. 115–278 as section 2210(c) of Pub. L. 107–296, which is classified to section 660(c) of this title.

Section 149, Pub. L. 107–296, title II, §228, as added and amended Pub. L. 114–113, div. N, title II, §§205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964, which related to cybersecurity plans, was renumbered section 2210 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 660 of this title.

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and was classified to section 150 of this title prior to renumbering as section 2212, which is classified to section 662 of this title.

Section 149a, Pub. L. 107–296, title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683, which related to cybersecurity strategy, was renumbered section 2211 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 661 of this title.

Section 150, Pub. L. 107–296, title II, §229, formerly §228, as added Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered §229, Pub. L. 114–113, div. N, title II, §223(a)(1), Dec. 18, 2015, 129 Stat. 2963, which related to clearances, was renumbered section 2212 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 662 of this title.

Section 151, Pub. L. 107–296, title II, §230, as added Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which related to Federal intrusion detection and prevention system, was renumbered section 2213 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 663 of this title.

# PART C—OFFICE OF SCIENCE AND TECHNOLOGY

### Editorial Notes

CODIFICATION

Subtitle D of title II of Pub. L. 107–296, which was classified to part D of this subchapter, was redesignated subtitle C of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

PRIOR PROVISIONS

A prior subtitle C of title II of Pub. L. 107–296, which was classified to this part, was redesignated subtitle B of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to part B (§141 et seq.) of this subchapter.

## § 161. Establishment of Office; Director

### (a) Establishment

#### (1) In general

There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this subchapter referred to as the ''Office'').

#### (2) Authority

The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be established within the National Institute of Justice.

### (b) Director

The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

(Pub. L. 107–296, title II, §231, Nov. 25, 2002, 116 Stat. 2159.)

### Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in subsec. (a)(1), was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

## § 162. Mission of Office; duties

### (a) Mission

The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

### (b) Duties

In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of chapter 10 of title 5) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of

1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113). The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.

(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.

(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.

(12) To support research fellowships in support of its mission.

(13) To serve as a clearinghouse for information on law enforcement technologies.

(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.

(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.

(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

**(c) Competition required**

Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis.

**(d) Information from Federal agencies**

Federal agencies shall, upon request from the Office and in accordance with Federal law, provide the Office with any data, reports, or other information requested, unless compliance with such request is otherwise prohibited by law.

**(e) Publications**

Decisions concerning publications issued by the Office shall rest solely with the Director of the Office.

**(f) Transfer of funds**

The Office may transfer funds to other Federal agencies or provide funding to non-Federal entities through grants, cooperative agreements, or contracts to carry out its duties under this section: *Provided*, That any such transfer or provision of funding shall be carried out in accordance with section 605 of Public Law 107–77.

**(g) Annual report**

The Director of the Office shall include with the budget justification materials submitted to Congress in support of the Department of Justice budget for each fiscal year (as submitted with the budget of the President under section 1105(a) of title 31) a report on the activities of the Office. Each such report shall include the following:

(1) For the period of 5 fiscal years beginning with the fiscal year for which the budget is submitted—

(A) the Director's assessment of the needs of Federal, State, and local law enforcement agencies for assistance with respect to law enforcement technology and other matters consistent with the mission of the Office; and

(B) a strategic plan for meeting such needs of such law enforcement agencies.

(2) For the fiscal year preceding the fiscal year for which such budget is submitted, a description of the activities carried out by the Office and an evaluation of the extent to which those activities successfully meet the needs assessed under paragraph (1)(A) in previous reports.

(Pub. L. 107–296, title II, § 232, Nov. 25, 2002, 116 Stat. 2159; Pub. L. 108–7, div. L, § 103(1), Feb. 20, 2003, 117 Stat. 529; Pub. L. 117–286, § 4(a)(13), Dec. 27, 2022, 136 Stat. 4306.)

**Editorial Notes**

REFERENCES IN TEXT

The National Technology Transfer and Advancement Act of 1995, referred to in subsec. (b)(3), (4), is Pub. L. 104–113, Mar. 7, 1996, 110 Stat. 775, as amended. For complete classification of this Act to the Code, see Short Title of 1996 Amendment note set out under section 3701 of Title 15, Commerce and Trade, and Tables.

Section 605 of Public Law 107–77, referred to in subsec. (f), is section 605 of Pub. L. 107–77, title VI, Nov. 28, 2001, 115 Stat. 798, which is not classified to the Code.

AMENDMENTS

2022—Subsec. (b)(2). Pub. L. 117–286 substituted ''chapter 10 of title 5)'' for ''the Federal Advisory Committee Act (5 U.S.C. App.))''.

2003—Subsec. (f). Pub. L. 108–7 inserted before period at end '': *Provided*, That any such transfer or provision of funding shall be carried out in accordance with section 605 of Public Law 107–77''.

### § 163. Definition of law enforcement technology

For the purposes of this subchapter, the term ''law enforcement technology'' includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

(Pub. L. 107–296, title II, § 233, Nov. 25, 2002, 116 Stat. 2161.)

**Editorial Notes**

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

### § 164. Abolishment of Office of Science and Technology of National Institute of Justice; transfer of functions

#### (a) Authority to transfer functions

The Attorney General may transfer to the Office any other program or activity of the Department of Justice that the Attorney General, in consultation with the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, determines to be consistent with the mission of the Office.

#### (b) Transfer of personnel and assets

With respect to any function, power, or duty, or any program or activity, that is established in the Office, those employees and assets of the element of the Department of Justice from which the transfer is made that the Attorney General determines are needed to perform that function, power, or duty, or for that program or activity, as the case may be, shall be transferred to the Office: *Provided*, That any such transfer shall be carried out in accordance with section 605 of Public Law 107–77.

#### (c) Report on implementation

Not later than 1 year after November 25, 2002, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the implementation of this subchapter. The report shall—

(1) provide an accounting of the amounts and sources of funding available to the Office to carry out its mission under existing authorizations and appropriations, and set forth the future funding needs of the Office; and

(2) include such other information and recommendations as the Attorney General considers appropriate.

(Pub. L. 107–296, title II, § 234, Nov. 25, 2002, 116 Stat. 2161; Pub. L. 108–7, div. L, § 103(2), Feb. 20, 2003, 117 Stat. 529.)

**Editorial Notes**

REFERENCES IN TEXT

Section 605 of Public Law 107–77, referred to in subsec. (b), is section 605 of Pub. L. 107–77, title VI, Nov. 28, 2001, 115 Stat. 798, which is not classified to the Code.

This subchapter, referred to in subsec. (c), was in the original ''this title'', meaning title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 401a of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judiciary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2003—Subsec. (b). Pub. L. 108–7 inserted before period at end '': *Provided*, That any such transfer shall be carried out in accordance with section 605 of Public Law 107–77''.

### § 165. National Law Enforcement and Corrections Technology Centers

#### (a) In general

The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as ''Centers'') and, to the extent necessary, establish new centers through a merit-based, competitive process.

#### (b) Purpose of Centers

The purpose of the Centers shall be to—

(1) support research and development of law enforcement technology;

(2) support the transfer and implementation of technology;

(3) assist in the development and dissemination of guidelines and technological standards; and

(4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

#### (c) Annual meeting

Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

**(d) Report**

Not later than 12 months after November 25, 2002, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

(Pub. L. 107–296, title II, § 235, Nov. 25, 2002, 116 Stat. 2162.)

SUBCHAPTER III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

### § 181. Under Secretary for Science and Technology

There shall be in the Department a Directorate of Science and Technology headed by an Under Secretary for Science and Technology.

(Pub. L. 107–296, title III, § 301, Nov. 25, 2002, 116 Stat. 2163.)

### § 182. Responsibilities and authorities of the Under Secretary for Science and Technology

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1) advising the Secretary regarding research and development efforts and priorities in support of the Department's missions;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the Director of the Cybersecurity and Infrastructure Security Agency, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 8401 of title 7;

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as ''select agents'' in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 262a of title 42;

(10) supporting United States leadership in science and technology;

(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;

(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; and

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

(Pub. L. 107–296, title III, § 302, Nov. 25, 2002, 116 Stat. 2163; Pub. L. 109–347, title V, § 501(b)(2), Oct. 13, 2006, 120 Stat. 1935; Pub. L. 110–53, title V, § 531(b)(1)(C), Aug. 3, 2007, 121 Stat. 334; Pub. L. 115–278, § 2(g)(3)(A), Nov. 16, 2018, 132 Stat. 4178.)

**Editorial Notes**

AMENDMENTS

2018—Par. (2). Pub. L. 115–278, § 2(g)(3)(A)(i), substituted ''biological,'' for ''biological,,''.

Par. (3). Pub. L. 115–278, § 2(g)(3)(A)(ii), substituted ''Director of the Cybersecurity and Infrastructure Security Agency'' for ''Assistant Secretary for Infrastructure Protection''.

Par. (5)(A). Pub. L. 115–278, § 2(g)(3)(A)(i), substituted ''biological,'' for ''biological,,''.

2007—Par. (3). Pub. L. 110–53 substituted ''Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection'' for ''Under Secretary for Information Analysis and Infrastructure Protection''.

2006—Pars. (2), (5)(A). Pub. L. 109–347 struck out ''radiological, nuclear'' after ''biological,''.

### § 183. Functions transferred

In accordance with subchapter XII, there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of the following entities:

(1) The following programs and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto (but not including programs and activities relating to the strategic nuclear defense posture of the United States):