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

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

Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

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

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

(9) To ensure that—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate—

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

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

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

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

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

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

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

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

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

(e) Staff

(1) In general

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

(2) Private sector analysts

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

(3) Security clearances

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

(f) Detail of personnel

(1) In general

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

(2) Covered agencies

The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

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

(3) Cooperative agreements

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

(4) Basis

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

(g) Functions transferred

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

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

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

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

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

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

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

Editorial Notes

REFERENCES IN TEXT

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

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

CODIFICATION

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

AMENDMENTS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(C) may be classified.''

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

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

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

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

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

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

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

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

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

Subsec. (d)(1). Pub. L. 110–53, § 501(b)(1), inserted '', in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 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 former section 621 of this title.]

Prohibition on Availability of Funds for Certain Activities and Assessment of the Overt Human Intelligence and Open Source Intelligence Collection Programs of the Office of Intelligence and Analysis of the Department of Homeland Security

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

''(a) Definitions.—In this section:

''(1) Appropriate congressional committees.—The term 'appropriate congressional committees' means the following:

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

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

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

''(2) Covered activity.—The term 'covered activity' means—

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

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

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

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

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

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

''(A) a United States citizen;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(4) REPORT.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

''(e) RULES OF CONSTRUCTION.—

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

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

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

''(B) the private sector; or

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

DHS COMPONENT USAGE OF THE HOMELAND SECURITY INFORMATION NETWORK

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

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

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

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

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

DEADLINE FOR INITIAL RECOMMENDED STRATEGY

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

ENHANCED GRID SECURITY

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

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

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

ligence (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 con-

fidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

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

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

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

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

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

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

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

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

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

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

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

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

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

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future

collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

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

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

BARACK OBAMA.

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

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

EXECUTIVE ORDER NO. 13650

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

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

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

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

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

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

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

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

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

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

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

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

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities respon-

sible 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 Intel-