(Pub. L. 114–22, title IX, § 906, as added Pub. L. 115–392, § 5(a), Dec. 21, 2018, 132 Stat. 5252.)

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§ 645a. Human trafficking assessment

Not later than 1 year after December 21, 2018, and annually thereafter, the Executive Associate Director of Homeland Security Investigations shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives a report on human trafficking investigations undertaken by Homeland Security Investigations that includes—

(1) the number of confirmed human trafficking investigations by category, including labor trafficking, sex trafficking, and transnational and domestic human trafficking;

(2) the number of victims by category, including—

(A) whether the victim is a victim of sex trafficking or a victim of labor trafficking; and

(B) whether the victim is a minor or an adult; and

(3) an analysis of the data described in paragraphs (1) and (2) and other data available to Homeland Security Investigations that indicates any general human trafficking or investigatory trends.

(Pub. L. 115–393, title IV, § 403, Dec. 21, 2018, 132 Stat. 5275.)

CODIFICATION

Section was enacted as part of the Trafficking Victims Protection Act of 2017, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

§ 651. Definitions

In this part:

(1) Critical infrastructure information

The term ''critical infrastructure information'' has the meaning given the term in section 671 of this title.

(2) Cybersecurity risk

The term ''cybersecurity risk'' has the meaning given the term in section 659 of this title.

(3) Cybersecurity threat

The term ''cybersecurity threat'' has the meaning given the term in section 1501(5) of this title.

(4) National cybersecurity asset response activities

The term ''national cybersecurity asset response activities'' means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(5) Sector-Specific Agency

The term ''Sector-Specific Agency'' means a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

(6) Sharing

The term ''sharing'' has the meaning given the term in section 659 of this title.

(Pub. L. 107–296, title XXII, § 2201, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4168.)

CONSTRUCTION OF PUB. L. 115–278

Pub. L. 115–278, § 5, Nov. 16, 2018, 132 Stat. 4186, provided that: ''Nothing in this Act [see section 1 of Pub. L. 115–278, set out as a Short Title of 2018 Amendment note under section 101 of this title] or an amendment made by this Act may be construed as—

''(1) conferring new authorities to the Secretary of Homeland Security, including programmatic, regulatory, or enforcement authorities, outside of the authorities in existence on the day before the date of enactment of this Act [Nov. 16, 2018];

''(2) reducing or limiting the programmatic, regulatory, or enforcement authority vested in any other Federal agency by statute; or

''(3) affecting in any manner the authority, existing on the day before the date of enactment of this Act, of any other Federal agency or component of the Department of Homeland Security.''

§ 652. Cybersecurity and Infrastructure Security Agency

(a) Redesignation

(1) In general

The National Protection and Programs Directorate of the Department shall, on and after November 16, 2018, be known as the ''Cybersecurity and Infrastructure Security Agency'' (in this part referred to as the ''Agency'').

(2) References

Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record,

or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) Director

(1) In general

The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this part referred to as the ''Director''), who shall report to the Secretary.

(2) Reference

Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 113(a)(1)(H) of this title as in effect on the day before November 16, 2018, in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of Cybersecurity and Infrastructure Security of the Department.

(c) Responsibilities

The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44 and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(6) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this chapter;

(8) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

(9) carry out emergency communications responsibilities, in accordance with subchapter XIII;

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; and

(11) carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) Deputy Director

There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

(1) assist the Director in the management of the Agency; and

(2) report to the Director.

(e) Cybersecurity and infrastructure security authorities of the Secretary

(1) In general

The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

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

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

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 122 of this title, the timely and efficient access by

the Department to all information necessary to discharge the responsibilities under this subchapter, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

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

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

(J) To ensure that any material received pursuant to this chapter is protected from unauthorized disclosure and handled and used only for the performance of official duties.

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

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

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

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 121(g) of this title.

(P) To carry out the functions of the national cybersecurity and communications integration center under section 659 of this title.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under subchapter XVI and the secure handling of ammonium nitrate program established under part J of subchapter VIII, or any successor programs.

(2) Reallocation

The Secretary may reallocate within the Agency the functions specified in sections 653(b) and 654(b) of this title, consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) Staff

(A) In general

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

(B) Private sector analysts

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

(C) Security clearances

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

(4) Detail of personnel

(A) In general

In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be

detailed to the Agency for the performance of analytic functions and related duties.

(B) Agencies

The Federal agencies described in this subparagraph are—

(i) the Department of State;

(ii) the Central Intelligence Agency;

(iii) the Federal Bureau of Investigation;

(iv) the National Security Agency;

(v) the National Geospatial-Intelligence Agency;

(vi) the Defense Intelligence Agency;

(vii) Sector-Specific Agencies; and

(viii) any other agency of the Federal Government that the President considers appropriate.

(C) Interagency agreements

The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) Basis

The detail of personnel under this paragraph may be on a reimbursable or nonreimbursable basis.

(f) Composition

The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Assistant Director.

(2) The Infrastructure Security Division, headed by an Assistant Director.

(3) The Emergency Communications Division under subchapter XIII, headed by an Assistant Director.

(g) Co-location

(1) In general

To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) Coordination

When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) Privacy

(1) In general

There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) Responsibilities

The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5 (commonly known as the ''Privacy Act of 1974'');

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) Savings

Nothing in this subchapter may be construed as affecting in any manner the authority, existing on the day before November 16, 2018, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector-Specific Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114–94).

(Pub. L. 107–296, title XXII, § 2202, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4169.)

REFERENCES IN TEXT

The Cybersecurity Act of 2015, referred to in subsec. (c)(3), is div. N of Pub. L. 114–113, Dec. 18, 2015, 129 Stat. 2935. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

This chapter, referred to in subsecs. (c)(7) and (e)(1)(J), was in the original ''this Act'', meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

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

Pub. L. 115–278, § 2(b)(1), Nov. 16, 2018, 132 Stat. 4175, provided that: ''The individual serving as the Under Secretary appointed pursuant to section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H)) of the Department of Homeland Security on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Director of Cybersecurity and Infrastructure Security of the Department on and after such date.''

§ 653. Cybersecurity Division

(a) Establishment

(1) In general

There is established in the Agency a Cybersecurity Division.

(2) Assistant Director

The Cybersecurity Division shall be headed by an Assistant Director for Cybersecurity (in this section referred to as the ''Assistant Director''), who shall—

(A) be at the level of Assistant Secretary within the Department;

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) Reference

Any reference to the Assistant Secretary for Cybersecurity and Communications in any

law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Cybersecurity.

(b) Functions

The Assistant Director shall—

(1) direct the cybersecurity efforts of the Agency;

(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44 and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(3) fully participate in the mechanisms required under section 652(c)(7) of this title; and

(4) carry out such other duties and powers as prescribed by the Director.

(Pub. L. 107–296, title XXII, § 2203, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4174.)

REFERENCES IN TEXT

The Cybersecurity Act of 2015, referred to in subsec. (b)(2), is div. N of Pub. L. 114–113, Dec. 18, 2015, 129 Stat. 2835. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR FOR CYBERSECURITY

Pub. L. 115–278, § 2(b)(3), Nov. 16, 2018, 132 Stat. 4175, provided that: ''The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Cybersecurity on and after such date.''

§ 654. Infrastructure Security Division

(a) Establishment

(1) In general

There is established in the Agency an Infrastructure Security Division.

(2) Assistant Director

The Infrastructure Security Division shall be headed by an Assistant Director for Infrastructure Security (in this section referred to as the ''Assistant Director''), who shall—

(A) be at the level of Assistant Secretary within the Department;

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) Reference

Any reference to the Assistant Secretary for Infrastructure Protection in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Infrastructure Security.

(b) Functions

The Assistant Director shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under subchapter XVI and the secure handling of ammonium nitrate program established under part J of subchapter VIII, or any successor programs;

(3) fully participate in the mechanisms required under section 652(c)(7) of this title; and

(4) carry out such other duties and powers as prescribed by the Director.

(Pub. L. 107–296, title XXII, § 2204, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4174.)

ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION AUTHORIZED TO SERVE AS ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY

Pub. L. 115–278, § 2(b)(4), Nov. 16, 2018, 132 Stat. 4175, provided that: ''The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of enactment of this Act [Nov. 16, 2018] may continue to serve as the Assistant Director for Infrastructure Security on and after such date.''

§ 655. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 652 of this title, the Director of Cybersecurity and Infrastructure Security shall—

(1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems;

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems; and

(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44.

(Pub. L. 107–296, title XXII, § 2205, formerly title II, § 223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, § 531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, § 2(e)(3)(A), Dec. 18, 2014, 128 Stat. 3086; renumbered title XXII, § 2205, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(i), Nov. 16, 2018, 132 Stat. 4178, 4180.)

CODIFICATION

Section was formerly classified to section 143 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, § 2(g)(9)(A)(i)(I), substituted ''section 652 of this title'' for ''section 121 of this title'' and ''Director of Cybersecurity and Infrastructure Security'' for ''Under Secretary appointed under section 113(a)(1)(H) of this title'' in introductory provisions.

Par. (1)(B). Pub. L. 115–278, § 2(g)(9)(A)(i)(II), struck out ''and'' at end.

2014—Pub. L. 113–283, § 2(e)(3)(A)(i), (ii), inserted ''Federal and'' before ''non-Federal'' in section catchline

and substituted ''the Under Secretary appointed under section 113(a)(1)(H) of this title'' for ''the Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection'' in introductory provisions.

Par. (3). Pub. L. 113–283, § 2(e)(3)(A)(iii), (iv), added par. (3).

2007—Pub. L. 110–53 substituted ''Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection'' for ''Under Secretary for Information Analysis and Infrastructure Protection'' in introductory provisions.

§ 656. NET Guard

The Director of Cybersecurity and Infrastructure Security may establish a national technology guard, to be known as ''NET Guard'', comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

(Pub. L. 107–296, title XXII, § 2206, formerly title II, § 224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, § 531(b)(1)(B), Aug. 3, 2007, 121 Stat. 334; renumbered title XXII, § 2206, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(ii), Nov. 16, 2018, 132 Stat. 4178, 4180.)

CODIFICATION

Section was formerly classified to section 144 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, § 2(g)(9)(A)(ii), substituted ''Director of Cybersecurity and Infrastructure Security'' for ''Assistant Secretary for Infrastructure Protection''.

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

§ 657. Cyber Security Enhancement Act of 2002

(a) Short title

This section may be cited as the ''Cyber Security Enhancement Act of 2002''.

(b) Amendment of sentencing guidelines relating to certain computer crimes

(1) Directive to the United States Sentencing Commission

Pursuant to its authority under section 994(p) of title 28 and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18.

(2) Requirements

In carrying out this subsection, the Sentencing Commission shall—

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18.

(c) Study and report on computer crimes

Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18.

(d) Emergency disclosure exception

(1) Omitted

(2) Reporting of disclosures

A government entity that receives a disclosure under section 2702(b) of title 18 shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after November 25, 2002.

(Pub. L. 107–296, title XXII, § 2207, formerly title II, § 225, Nov. 25, 2002, 116 Stat. 2156; renumbered title XXII, § 2207, Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

CODIFICATION

Section was formerly classified to section 145 of this title prior to renumbering by Pub. L. 115–278.

Section is comprised of section 2207 of Pub. L. 107–296. Subsecs. (d)(1) and (e) to (j) of section 2207 of Pub. L. 107–296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

§ 658. Cybersecurity recruitment and retention

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term ''appropriate committees of Congress'' means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) Collective bargaining agreement

The term ''collective bargaining agreement'' has the meaning given that term in section 7103(a)(8) of title 5.

(3) Excepted service

The term ''excepted service'' has the meaning given that term in section 2103 of title 5.

(4) Preference eligible

The term ''preference eligible'' has the meaning given that term in section 2108 of title 5.

(5) Qualified position

The term ''qualified position'' means a position, designated by the Secretary for the purpose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

(6) Senior Executive Service

The term ''Senior Executive Service'' has the meaning given that term in section 2101a of title 5.

(b) General authority

(1) Establish positions, appoint personnel, and fix rates of pay

(A) General authority

The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

(I) senior level positions designated under section 5376 of title 5; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

(B) Construction with other laws

The authority of the Secretary under this subsection applies without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

(2) Basic pay

(A) Authority to fix rates of basic pay

In accordance with this section, the Secretary shall fix the rates of basic pay for any qualified position established under paragraph (1) in relation to the rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

(B) Prevailing rate systems

The Secretary may, consistent with section 5341 of title 5, adopt such provisions of that title as provide for prevailing rate systems of basic pay and may apply those provisions to qualified positions for employees in or under which the Department may employ individuals described by section 5342(a)(2)(A) of that title.

(3) Additional compensation, incentives, and allowances

(A) Additional compensation based on title 5 authorities

The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5.

(B) Allowances in nonforeign areas

An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) Plan for execution of authorities

Not later than 120 days after December 18, 2014, the Secretary shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

(5) Collective bargaining agreements

Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

(6) Required regulations

The Secretary, in coordination with the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

(c) Annual report

Not later than 1 year after December 18, 2014, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office within the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

(d) Three-year probationary period

The probationary period for all employees hired under the authority established in this section shall be 3 years.

(e) Incumbents of existing competitive service positions

(1) In general

An individual serving in a position on December 18, 2014, that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

(2) Subsequent conversion

After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

(f) Study and report

Not later than 120 days after December 18, 2014, the National Protection and Programs Directorate shall submit a report regarding the availability of, and benefits (including cost savings and security) of using, cybersecurity personnel and facilities outside of the National Capital Region (as defined in section 2674 of title 10) to serve the Federal and national need to—

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

(Pub. L. 107–296, title XXII, § 2208, formerly title II, § 226, as added Pub. L. 113–277, § 3(a), Dec. 18, 2014, 128 Stat. 3005; renumbered title XXII, § 2208, Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

CODIFICATION

Section was formerly classified to section 147 of this title prior to renumbering by Pub. L. 115–278.

CHANGE OF NAME

Reference to National Protection and Programs Directorate of the Department of Homeland Security deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department, see section 652(a)(2) of this title, enacted Nov. 16, 2018.

§ 659. National cybersecurity and communications integration center

(a) Definitions

In this section—

(1) the term ''cybersecurity risk''—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

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

(3) the term ''incident'' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

(4) the term ''information sharing and analysis organization'' has the meaning given that term in section 671(5) of this title;

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

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

(b) Center

There is in the Department a national cybersecurity and communications integration

center (referred to in this section as the ''Center'') to carry out certain responsibilities of the Director. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity.

(c) Functions

The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.];

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and

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

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) sharing[1] cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department; and

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

(d) Composition

(1) In general

The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3003(4) of title 50;

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) information sharing and analysis organizations, including information sharing and analysis centers;

(iii) owners and operators of critical information systems; and

(iv) private entities;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector;

(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

(F) other appropriate representatives or entities, as determined by the Secretary.

(2) Incidents

In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) Principles

In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

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

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and;[2]

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

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015 [6 U.S.C. 1504].

(f) No right or benefit

(1) In general

The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Director.

(2) Certain assistance or information

The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(g) Automated information sharing

(1) In general

The Director, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.].

(2) Annual report

The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(h) Voluntary information sharing procedures

(1) Procedures

(A) In general

The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) National security

The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) Voluntary information sharing relationships

A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) Standard agreement

For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) Negotiated agreement

At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Director, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) Existing agreements

An agreement between the Center and a non-Federal entity that is entered into before December 18, 2015, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements

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

of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) Direct reporting

The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) Reports on international cooperation

Not later than 180 days after December 18, 2015, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(k) Outreach

Not later than 60 days after December 18, 2015, the Secretary, acting through the Director, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(*l*) Cybersecurity outreach

(1) In general

The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(2) Definitions

For purposes of this subsection, the terms ''small business concern'' and ''small business development center'' have the meaning given such terms, respectively, under section 632 of title 15.

(m) Coordinated vulnerability disclosure

The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(Pub. L. 107–296, title XXII, §2209, formerly title II, §227, formerly §226, as added Pub. L. 113–282, §3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered §227 and amended Pub. L. 114–113, div. N, title II, §§203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963; Pub. L. 114–328, div. A, title XVIII, §1841(b), Dec. 23, 2016, 130 Stat. 2663; renumbered title XXII, §2209, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(iii), Nov. 16, 2018, 132 Stat. 4178, 4180.)

REFERENCES IN TEXT

Title I of the Cybersecurity Act of 2015, referred to in subsecs. (c)(1) and (g)(1), is title I of Pub. L. 114–113, div. N, Dec. 18, 2015, 129 Stat. 2936, also known as the Cybersecurity Information Sharing Act of 2015, which is classified generally to subchapter I of chapter 6 of this title. For complete classification of title I to the Code, see Short Title note set out under section 1501 of this title and Tables.

CODIFICATION

Section was formerly classified to section 148 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, §2(g)(9)(A)(iii)(I), substituted ''Director'' for ''Under Secretary appointed under section 113(a)(1)(H) of this title'' wherever appearing.

Subsec. (a)(4). Pub. L. 115–278, §2(g)(9)(A)(iii)(II), substituted ''section 671(5) of this title'' for ''section 131(5) of this title''.

Subsec. (b). Pub. L. 115–278, §2(g)(9)(A)(iii)(III), inserted at end ''The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity.''

Subsec. (c)(11). Pub. L. 115–278, §2(g)(9)(A)(iii)(IV), substituted ''Emergency Communications Division'' for ''Office of Emergency Communications''.

2016—Subsecs. (*l*), (m). Pub. L. 114–328 added subsec. (*l*) and redesignated former subsec. (*l*) as (m).

2015—Subsec. (a)(1) to (5). Pub. L. 114–113, §203(1)(A), (B), added pars. (1) to (3), redesignated former pars. (3) and (4) as (4) and (5), respectively, and struck out former pars. (1) and (2), which defined ''cybersecurity risk'' and ''incident'', respectively.

Subsec. (a)(6). Pub. L. 114–113, §203(1)(C)–(E), added par. (6).

Subsec. (c)(1). Pub. L. 114–113, §203(2)(A), inserted ''cyber threat indicators, defensive measures,'' before ''cybersecurity risks'' and '', including the implementation of title I of the Cybersecurity Act of 2015'' before semicolon at end.

Subsec. (c)(3). Pub. L. 114–113, §203(2)(B), substituted ''cyber threat indicators, defensive measures, cybersecurity risks,'' for ''cybersecurity risks''.

Subsec. (c)(5)(A). Pub. L. 114–113, §203(2)(C), substituted ''cyber threat indicators, defensive measures, cybersecurity risks,'' for ''cybersecurity risks''.

Subsec. (c)(6). Pub. L. 114–113, §203(2)(D), substituted ''cyber threat indicators, defensive measures, cybersecurity risks,'' for ''cybersecurity risks'' and struck out ''and'' at end.

Subsec. (c)(7)(C). Pub. L. 114–113, §203(2)(E), added subpar. (C).

Subsec. (c)(8) to (11). Pub. L. 114–113, §203(2)(F), added pars. (8) to (11).

Subsec. (d)(1)(B)(i). Pub. L. 114–113, §203(3)(A)(i), substituted '', local, and tribal'' for ''and local''.

Subsec. (d)(1)(B)(ii). Pub. L. 114–113, §203(3)(A)(ii), substituted '', including information sharing and analysis centers;'' for ''; and''.

Subsec. (d)(1)(B)(iv). Pub. L. 114–113, §203(3)(A)(iii), (iv), added cl. (iv).

Subsec. (d)(1)(E), (F). Pub. L. 114–113, §203(3)(B)–(D), added subpar. (E) and redesignated former subpar. (E) as (F).

Subsec. (e)(1)(A). Pub. L. 114–113, §203(4)(A)(i), inserted ''cyber threat indicators, defensive measures, and'' before ''information''.

Subsec. (e)(1)(B). Pub. L. 114–113, §203(4)(A)(ii), inserted ''cyber threat indicators, defensive measures, and'' before ''information related''.

Subsec. (e)(1)(F). Pub. L. 114–113, § 203(4)(A)(iii), substituted ''cyber threat indicators, defensive measures, cybersecurity risks,'' for ''cybersecurity risks'' and struck out ''and'' at end.

Subsec. (e)(1)(G). Pub. L. 114–113, § 203(4)(A)(iv), substituted ''cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and'' for ''cybersecurity risks and incidents''.

Subsec. (e)(1)(H). Pub. L. 114–113, § 203(4)(A)(v), added subpar. (H).

Subsec. (e)(2). Pub. L. 114–113, § 203(4)(B), substituted ''cyber threat indicators, defensive measures, cybersecurity risks,'' for ''cybersecurity risks'' and inserted ''or disclosure'' after ''access''.

Subsec. (e)(3). Pub. L. 114–113, § 203(4)(C), inserted '', including by working with the Privacy Officer appointed under section 142 of this title to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015'' before period at end.

Subsecs. (g) to (*l*). Pub. L. 114–113, § 203(5), added subsecs. (g) to (*l*).

RULES OF CONSTRUCTION

Pub. L. 113–282, § 8, Dec. 18, 2014, 128 Stat. 3072, provided that:

''(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title] or the amendments made by this Act shall be construed to grant the Secretary [of Homeland Security] any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2014].

''(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

''(1) to request assistance from the Secretary; or

''(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.''

DEFINITIONS

Pub. L. 113–282, § 2, Dec. 18, 2014, 128 Stat. 3066, provided that: ''In this Act [see section 1 of Pub. L. 113–282, set out as a Short Title of 2014 Amendment note under section 101 of this title]—

''(1) the term 'Center' means the national cybersecurity and communications integration center under section 226 [renumbered 227 by section 223(a)(3) of Pub. L. 114–113 and renumbered 2209 by section 2(g)(2)(I) of Pub. L. 115–278] of the Homeland Security Act of 2002 [6 U.S.C. 659], as added by section 3;

''(2) the term 'critical infrastructure' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

''(3) the term 'cybersecurity risk' has the meaning given that term in section 226 [2209] of the Homeland Security Act of 2002, as added by section 3;

''(4) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5) [renumbered 2222(5) by section 2(g)(2)(H) of Pub. L. 115–278] of the Homeland Security Act of 2002 ([former] 6 U.S.C. 131(5)) [now 6 U.S.C. 671(5)];

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

''(6) the term 'Secretary' means the Secretary of Homeland Security.''

§ 660. Cybersecurity plans

(a) Definitions

In this section—

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

(2) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 659 of this title;

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

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

(b) Intrusion assessment plan

(1) Requirement

The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) Exception

The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) Cyber incident response plan

The Director of Cybersecurity and Infrastructure Security shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 671(5) of this title), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 659 of this title) to critical infrastructure.

(d) National Response Framework

The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(Pub. L. 107–296, title XXII, § 2210, formerly title II, § 228, as added and amended Pub. L. 114–113, div. N, title II, §§ 205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964; renumbered title XXII, § 2210, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(iv), Nov. 16, 2018, 132 Stat. 4178, 4181.)

CODIFICATION

Section was formerly classified to section 149 of this title prior to renumbering by Pub. L. 115–278.

Former section 149 of this title, which was transferred and redesignated as subsec. (c) of this section by Pub. L. 114–113, div. N, title II, § 223(a)(2), Dec. 18, 2015, 129 Stat. 2963, was based on Pub. L. 107–296, title II, § 227, as added by Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070.

AMENDMENTS

2018—Subsec. (a)(2). Pub. L. 115–278, §2(g)(9)(A)(iv)(I), substituted ''section 659 of this title'' for ''section 148 of this title''.

Subsec. (c). Pub. L. 115–278, §2(g)(9)(A)(iv), substituted ''Director of Cybersecurity and Infrastructure Security'' for ''Under Secretary appointed under section 113(a)(1)(H) of this title'', ''section 671(5) of this title'' for ''section 131(5) of this title'', and ''section 659 of this title'' for ''section 148 of this title''.

2015—Subsec. (c). Pub. L. 114–113, §223(a)(5), made technical amendment to reference in original act which appears in text as reference to section 148 of this title.

Pub. L. 114–113, §223(a)(2), transferred former section 149 of this title to subsec. (c) of this section. See Codification note above.

Subsec. (d). Pub. L. 114–113, §205, added subsec. (d).

RULE OF CONSTRUCTION

Pub. L. 113–282, §7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: ''Nothing in the amendment made by subsection (a) [enacting subsec. (c) of this section and section 150 of this title] or in subsection (b)(1) [formerly classified as a note under section 3543 of Title 44, Public Printing and Documents, see now section 2(d)(1) of Pub. L. 113–283, set out as a note under section 3553 of Title 44] shall be construed to alter any authority of a Federal agency or department.''

§ 661. Cybersecurity strategy

(a) In general

Not later than 90 days after December 23, 2016, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

(b) Contents

The strategy required under subsection (a) shall include the following:

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in section 659 of this title (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) Considerations

In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 347 of this title; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

(d) Implementation plan

Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) Congressional oversight

The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) Classified information

The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(g) Rule of construction

Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(h) Definition

In this section, the term ''Homeland Security Enterprise'' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

(Pub. L. 107–296, title XXII, §2211, formerly title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683; renumbered title XXII, §2211, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(v), Nov. 16, 2018, 132 Stat. 4178, 4181.)

CODIFICATION

Section was formerly classified to section 149a of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Subsec. (b)(2)(A). Pub. L. 115–278, §2(g)(9)(A)(v), substituted ''section 659 of this title'' for ''the section 148 of this title''.

§ 662. Clearances

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162;[1] relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and

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

analysis organizations (as defined in section 671(5) of this title), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

(Pub. L. 107–296, title XXII, § 2212, formerly title II, § 229, formerly § 228, as added Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered § 229, Pub. L. 114–113, div. N, title II, § 223(a)(1), Dec. 18, 2015, 129 Stat. 2963; renumbered title XXII, § 2212, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(vi), Nov. 16, 2018, 132 Stat. 4178, 4181.)

REFERENCES IN TEXT

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

CODIFICATION

Section was formerly classified to section 150 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Pub. L. 115–278, § 2(g)(9)(A)(vi), substituted ''section 671(5) of this title'' for ''section 131(5) of this title''.

§ 663. Federal intrusion detection and prevention system

(a) Definitions

In this section—

(1) the term ''agency'' has the meaning given the term in section 3502 of title 44;

(2) the term ''agency information'' means information collected or maintained by or on behalf of an agency;

(3) the term ''agency information system'' has the meaning given the term in section 660 of this title; and

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 659 of this title.

(b) Requirement

(1) In general

Not later than 1 year after December 18, 2015, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) Regular improvement

The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) Activities

In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) Principles

In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) Private entities

(1) Conditions

A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the

information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) Limitation on liability

No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) Rule of construction

Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) Privacy Officer review

Not later than 1 year after December 18, 2015, the Privacy Officer appointed under section 142 of this title, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(Pub. L. 107–296, title XXII, §2213, formerly title II, §230, as added Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964; renumbered title XXII, §2213, and amended Pub. L. 115–278, §2(g)(2)(I), (9)(A)(vii), Nov. 16, 2018, 132 Stat. 4178, 4181.)

REFERENCES IN TEXT

Section 208(b) of the E-Government Act of 2002, referred to in subsec. (c)(6), is section 208(b) of title II of Pub. L. 107–347, which is set out in a note under section 3501 of Title 44, Public Printing and Documents.

CODIFICATION

Section was formerly classified to section 151 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Subsec. (a)(3). Pub. L. 115–278, §2(g)(9)(A)(vii)(I), substituted ''section 660 of this title'' for ''section 149 of this title''.

Subsec. (a)(4). Pub. L. 115–278, §2(g)(9)(A)(vii)(II), substituted ''section 659 of this title'' for ''section 148 of this title''.

DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES

Pub. L. 115–390, title I, §101, Dec. 21, 2018, 132 Stat. 5173, provided that:

''(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

''(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

''(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

''(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

''(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

''(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

''(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

''(c) CONSULTATION.—

''(1) IN GENERAL.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

''(A) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) are protected from prosecution under section 1030 of title 18, United States Code, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

''(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

''(C) Non-governmental security researchers.

''(2) NONAPPLICABILITY OF FACA.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to any consultation under this section.

''(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

''(e) SUBMISSION TO CONGRESS.—

''(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act [Dec. 21, 2018], the Secretary of Homeland Security shall submit to the appropriate congressional committees a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

''(2) REPORT AND BRIEFING.—

''(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to the appropriate congressional committees a report on such policy and the remediation process required under subsection (b).

''(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to the appropriate congressional committees a briefing on the policy required under subsection (a) and the process required under subsection (b).

''(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (a) and the process required under subsection (b) for the period covered by the report or briefing, as the case may be:

''(i) The number of unique security vulnerabilities reported.

''(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

''(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

''(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

''(f) DEFINITIONS.—In this section:

''(1) The term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

''(2) The term 'information system' has the meaning given that term by section 3502 of title 44, United States Code.

''(3) The term 'appropriate information system' means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

''(4) The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate.''

DEPARTMENT OF HOMELAND SECURITY BUG BOUNTY PILOT PROGRAM

Pub. L. 115–390, title I, §102, Dec. 21, 2018, 132 Stat. 5175, provided that:

''(a) DEFINITIONS.—In this section:

''(1) The term 'appropriate congressional committees' means—

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

''(B) the Select Committee on Intelligence of the Senate;

''(C) the Committee on Homeland Security of the House of Representatives; and

''(D) Permanent Select Committee on Intelligence of the House of Representatives.

''(2) The term 'bug bounty program' means a program under which—

''(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

''(B) eligible individuals, organizations, and companies receive compensation in exchange for such reports.

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

''(4) The term 'eligible individual, organization, or company' means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

''(5) The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(6) The term 'pilot program' means the bug bounty pilot program required to be established under subsection (b)(1).

''(7) The term 'Secretary' means the Secretary of Homeland Security.

''(b) BUG BOUNTY PILOT PROGRAM.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act [Dec. 21, 2018], the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

''(2) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

''(A) designate appropriate information systems to be included in the pilot program;

''(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

''(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

''(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

''(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

''(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

''(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

''(3) CONTRACT AUTHORITY.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award 1 or more competitive contracts to an entity, as necessary, to manage the pilot program.

''(c) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

''(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

''(A) registered;

''(B) were determined eligible;

''(C) submitted security vulnerabilities; and

''(D) received compensation;

''(2) the number and severity of vulnerabilities reported as part of the pilot program;

''(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

''(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

''(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

''(6) the types of compensation provided under the pilot program; and

''(7) the lessons learned from the pilot program.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Department $250,000 for fiscal year 2019 to carry out this section.''

AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, §223(b), Dec. 18, 2015, 129 Stat. 2966, as amended by Pub. L. 115–278, §2(h)(1)(E), Nov. 16, 2018, 132 Stat. 4182, provided that:

''(1) IN GENERAL.—Except as provided in paragraph (2)—

''(A) not later than 1 year after the date of enactment of this Act [Dec. 18, 2015] or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], whichever is later, the head of

each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

''(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 2213(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(2)], the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

''(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

''(3) DEFINITION.—Notwithstanding section 222 [6 U.S.C. 1521], in this subsection, the term 'agency information system' means an information system owned or operated by an agency.

''(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.''

§ 664. National asset database

(a) Establishment

(1) National asset database

The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) Prioritized critical infrastructure list

In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) Use of database

The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) Maintenance of database

(1) In general

The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) Organization of information in database

The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7; and

(B) by the State and county of their location.

(3) Private sector integration

The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) Retention of classification

The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a sector-specific agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) Reports

(1) Report required

Not later than 180 days after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) Contents of report

Each such report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on such list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on such list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on such list or in such database.

(E) If appropriate, the extent to which such database and such list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any other information the Secretary deems relevant.

(3) Classified information

The report shall be submitted in unclassified form but may contain a classified annex.

(e) National Infrastructure Protection Consortium

The Secretary may establish a consortium to be known as the ''National Infrastructure Protection Consortium''. The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

(Pub. L. 107–296, title XXII, § 2214, formerly title II, § 210E, as added Pub. L. 110–53, title X, § 1001(a), Aug. 3, 2007, 121 Stat. 372; renumbered title XXII, § 2214, and amended Pub. L. 115–278, § 2(g)(2)(G), (9)(A)(viii), Nov. 16, 2018, 132 Stat. 4178, 4181.)

CODIFICATION

Section was formerly classified to section 124*l* of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Subsecs. (e), (f). Pub. L. 115–278, § 2(g)(9)(A)(viii), redesignated subsec. (f) as (e) and struck out former subsec. (e). Prior to amendment, text of subsec. (e) read as follows: ''By not later than two years after August 3, 2007, the Inspector General of the Department shall conduct a study of the implementation of this section.''

PART B—CRITICAL INFRASTRUCTURE INFORMATION

CODIFICATION

Subtitle B of title XXII of Pub. L. 107–296, comprising this part, was originally added as subtitle B of title II of Pub. L. 107–296, and was classified to part B (§ 131 et seq.) of subchapter II of this chapter. Subtitle B of title II of Pub. L. 107–296 was subsequently redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

§ 671. Definitions

In this part:

(1) Agency

The term ''agency'' has the meaning given it in section 551 of title 5.

(2) Covered Federal agency

The term ''covered Federal agency'' means the Department of Homeland Security.

(3) Critical infrastructure information

The term ''critical infrastructure information'' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) Critical infrastructure protection program

The term ''critical infrastructure protection program'' means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) Information Sharing and Analysis Organization

The term ''Information Sharing and Analysis Organization'' means any formal or informal entity or collaboration created or em-

ployed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a[1] interference, compromise, or a[2] incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) Protected system

The term ''protected system''—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) Voluntary

(A) In general

The term ''voluntary'', in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) Exclusions

The term ''voluntary''—

(i) in the case of any action brought under the securities laws as is defined in section 78c(a)(47) of title 15—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 78*l*(i) of title 15; and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

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

(8) Cybersecurity risk; incident

The terms ''cybersecurity risk'' and ''incident'' have the meanings given those terms in section 659 of this title.

(Pub. L. 107–296, title XXII, §2222, formerly title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961; renumbered title XXII, §2222, and amended Pub. L. 115–278, §2(g)(2)(H), (9)(B)(i), Nov. 16, 2018, 132 Stat. 4178, 4181.)

CODIFICATION

Section was formerly classified to section 131 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Par. (8). Pub. L. 115–278, §2(g)(9)(B)(i), substituted ''section 659 of this title'' for ''section 148 of this title''.

2015—Par. (5)(A). Pub. L. 114–113, §204(1)(A), inserted '', including information related to cybersecurity risks and incidents,'' after ''critical infrastructure information'' and '', including cybersecurity risks and incidents,'' after ''related to critical infrastructure''.

Par. (5)(B). Pub. L. 114–113, §204(1)(B), inserted '', including cybersecurity risks and incidents,'' after ''critical infrastructure information'' and '', including cybersecurity risks and incidents,'' after ''related to critical infrastructure''.

Par. (5)(C). Pub. L. 114–113, §204(1)(C), inserted '', including cybersecurity risks and incidents,'' after ''critical infrastructure information''.

Par. (8). Pub. L. 114–113, §204(2), added par. (8).

SHORT TITLE

For short title of this part as the ''Critical Infrastructure Information Act of 2002'', see section 2221 of Pub. L. 107–296, set out as a note under section 101 of this title.

PROHIBITION ON NEW REGULATORY AUTHORITY

Pub. L. 114–113, div. N, title II, §210, Dec. 18, 2015, 129 Stat. 2962, provided that: ''Nothing in this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title] or the amendments made by this subtitle may be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of enactment of this Act [Dec. 18, 2015].''

DEFINITIONS

Pub. L. 114–113, div. N, title II, §202, Dec. 18, 2015, 129 Stat. 2956, as amended by Pub. L. 115–278, §2(h)(1)(A), Nov. 16, 2018, 132 Stat. 4181, provided that: ''In this subtitle [subtitle A (§§201–211) of title II of div. N of Pub. L. 114–113, see Short Title of 2015 Amendment note set out under section 101 of this title]:

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

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

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

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

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

''(2) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given those terms in section 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659].

''(3) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms 'cyber threat indicator' and 'defensive measure' have the meanings given those terms in section 102 [6 U.S.C. 1501].

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

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

§ 672. Designation of critical infrastructure protection program

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

(Pub. L. 107–296, title XXII, § 2223, formerly title II, § 213, Nov. 25, 2002, 116 Stat. 2152; renumbered title XXII, § 2223, Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

CODIFICATION

Section was formerly classified to section 132 of this title prior to renumbering by Pub. L. 115–278.

§ 673. Protection of voluntarily shared critical infrastructure information

(a) Protection

(1) In general

Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5 (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this part, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.[1]

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) Express statement

For purposes of paragraph (1), the term ''express statement'', with respect to information or records, means—

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: ''This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.''; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) Limitation

No communication of critical infrastructure information to a covered Federal agency made pursuant to this part shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act.

(c) Independently obtained information

Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law. For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5.

(d) Treatment of voluntary submittal of information

The voluntary submittal to the Government of information or records that are protected from

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

disclosure by this part shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) Procedures

(1) In general

The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after November 25, 2002.

(2) Elements

The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this part;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) Penalties

Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this part coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) Authority to issue warnings

The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) Authority to delegate

The President may delegate authority to a critical infrastructure protection program, designated under section 672 of this title, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 4558 of title 50.

(Pub. L. 107–296, title XXII, §2224, formerly title II, §214, Nov. 25, 2002, 116 Stat. 2152; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 112–199, title I, §111, Nov. 27, 2012, 126 Stat. 1472; renumbered title XXII, §2224, and amended Pub. L. 115–278, §2(g)(2)(H), (9)(B)(ii), Nov. 16, 2018, 132 Stat. 4178, 4181.)

REFERENCES IN TEXT

The Critical Infrastructure Information Act of 2002, referred to in subsec. (a)(2)(A), is subtitle B (§2221 et seq.) of title XXII of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2150, which is classified generally to this part. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

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

CODIFICATION

Section was formerly classified to section 133 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2018—Subsec. (h). Pub. L. 115–278, §2(g)(9)(B)(ii), substituted ''section 672 of this title'' for ''section 132 of this title''.

2012—Subsec. (c). Pub. L. 112–199 inserted at end ''For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5.''

2004—Subsec. (a)(1)(D)(ii)(II). Pub. L. 108–271 substituted ''Government Accountability Office'' for ''General Accounting Office''.

EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–199 effective 30 days after Nov. 27, 2012, see section 202 of Pub. L. 112–199, set out as a note under section 1204 of Title 5, Government Organization and Employees.

§ 674. No private right of action

Nothing in this part may be construed to create a private right of action for enforcement of any provision of this chapter.

(Pub. L. 107–296, title XXII, §2225, formerly title II, §215, Nov. 25, 2002, 116 Stat. 2155; renumbered title XXII, §2225, Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002,

which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

CODIFICATION

Section was formerly classified to section 134 of this title prior to renumbering by Pub. L. 115–278.

CHAPTER 2—NATIONAL EMERGENCY MANAGEMENT

§ 701. Definitions

In this title—[1]

(1) the term ''Administrator'' means the Administrator of the Agency;

(2) the term ''Agency'' means the Federal Emergency Management Agency;

(3) the term ''appropriate committees of Congress'' means—

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

(B) those committees of the House of Representatives that the Speaker of the House of Representatives determines appropriate;

(4) the term ''catastrophic incident'' means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area;

(5) the term ''Department'' means the Department of Homeland Security;

(6) the terms ''emergency'' and ''major disaster'' have the meanings given the terms in section 5122 of title 42;

(7) the term ''emergency management'' means the governmental function that coordinates and integrates all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters;

(8) the term ''emergency response provider'' has the meaning given the term in section 101 of this title;

(9) the term ''Federal coordinating officer'' means a Federal coordinating officer as described in section 5143 of title 42;

(10) the term ''individual with a disability'' has the meaning given the term in section 12102 of title 42;

(11) the terms ''local government'' and ''State'' have the meaning given the terms in section 101 of this title;

(12) the term ''National Incident Management System'' means a system to enable effective, efficient, and collaborative incident management;

(13) the term ''National Response Plan'' means the National Response Plan or any successor plan prepared under section 314(a)(6) of this title;

(14) the term ''Secretary'' means the Secretary of Homeland Security;

[1] See References in Text note below.