(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.