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.)

Editorial Notes

CODIFICATION

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

Statutory Notes and Related Subsidiaries

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) Definition

The term ''cybersecurity vulnerability'' has the meaning given the term ''security vulnerability'' in section 650 of this title.

(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 Executive 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;

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n), as appropriate; and

(C) sharing the analysis conducted under subparagraph (A) and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate, with Federal and non-Federal entities;

(6) upon request, providing operational and 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, which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions;

(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) share 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, mitigation protocols to counter cybersecurity vulnerabilities, as appropriate, 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;

(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;

(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices; and

(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as de-

fined in section 681 of this title) submitted by covered entities (as defined in section 681 of this title) and reports related to ransom payments (as defined in section 681 of this title) submitted by covered entities (as defined in section 681 of this title) in furtherance of the activities specified in sections 652(e), 653, and 681a of this title, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.

(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;

(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, including cybersecurity specialists;

(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, including an entity that collaborates with election officials, on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

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

(2) Incidents

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

(e) Principles

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

(1) to the extent practicable, that—

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

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

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

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

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

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) Information Sharing and Analysis Organizations; and

(III) other appropriate non-Federal partners;

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

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

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

(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;

(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) Cyber hunt and incident response teams

(1) In general

The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

(A) assistance to asset owners and operators in restoring services following a cyber incident;

(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

(C) mitigation strategies to prevent, deter, and protect against cybersecurity risks;

(D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate; and

(E) such other capabilities as the Secretary determines appropriate.

(2) Associated metrics

The Center shall—

(A) define the goals and desired outcomes for each cyber hunt and incident response team; and

(B) develop metrics—

(i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A); and

(ii) that—

(I) are quantifiable and actionable; and

(II) the Center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response teams.

(3) Cybersecurity specialists

After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team.

(g) No right or benefit

(1) In general

The provision of assistance or information to, and inclusion in the Center, or any team or activity of 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, or any team or activity of 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.

(h) 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.

(i) 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 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.

(j) 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.

(k) 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).

(*l*) 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.

(m) 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.

(n) 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.

(*o*) Protocols to counter certain cybersecurity vulnerabilities

The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.

(p) Subpoena authority

(1) Definition

In this subsection, the term ''covered device or system''—

(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

(B) does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices.

(2) Authority

(A) In general

If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe such security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under subsection (c)(12).

(B) Limit on information

A subpoena issued pursuant to subparagraph (A) may seek information—

(i) only in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18; and

(ii) for not more than 20 covered devices or systems.

(C) Liability protections for disclosing providers

The provisions of section 2703(e) of title 18, shall apply to any subpoena issued pursuant to subparagraph (A).

(3) Coordination

(A) In general

If the Director exercises the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to interagency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after January 1, 2021.

(B) Contents

The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

(i) issued to carry out a function described in subsection (c)(12); and

(ii) subject to the limitations specified in this subsection.

(4) Noncompliance

If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued pursuant to this subsection, the Director may request that the Attorney General seek enforcement of such subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) Notice

Not later than seven days after the date on which the Director receives information obtained through a subpoena issued pursuant to this subsection, the Director shall notify any entity identified by information obtained pur-

suant to such subpoena regarding such subpoena and the identified vulnerability.

(6) Authentication

(A) In general

Any subpoena issued pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) Invalid if not authenticated

Any subpoena issued pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

(7) Procedures

Not later than 90 days after January 1, 2021, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued pursuant to this subsection, which shall address the following:

(A) The protection of and restriction on dissemination of nonpublic information obtained through such a subpoena, including a requirement that the Agency not disseminate nonpublic information obtained through such a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in accordance with paragraph (4), and may share with a Federal agency the nonpublic information of the entity at risk if—

(i) the Agency identifies or is notified of a cybersecurity incident involving such entity, which relates to the vulnerability which led to the issuance of such subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow such department or agency to take a law enforcement or national security action, consistent with the interagency procedures under paragraph (3)(A), or actions related to mitigating or otherwise resolving such incident;

(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests, consistent with such interagency procedures; and

(iv) the entity consents, except that the entity's consent shall not be required if another Federal department or agency identifies the entity to the Agency in connection with a suspected cybersecurity incident.

(B) The restriction on the use of information obtained through such a subpoena for a cybersecurity purpose.

(C) The retention and destruction of nonpublic information obtained through such a subpoena, including—

(i) destruction of such information that the Director determines is unrelated to critical infrastructure immediately upon providing notice to the entity pursuant to paragraph (5); and

(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through such a subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent.

(D) The processes for providing notice to each party that is subject to such a subpoena and each entity identified by information obtained under such a subpoena.

(E) The processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued pursuant to this subsection.

(F) The information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—

(i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and

(ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.

(8) Limitation on procedures

The internal procedures established pursuant to paragraph (7) may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to this chapter.

(9) Review of procedures

Not later than 1 year after January 1, 2021, the Privacy Officer of the Agency shall—

(A) review the internal procedures established pursuant to paragraph (7) to ensure that—

(i) such procedures are consistent with fair information practices; and

(ii) the operations of the Agency comply with such procedures; and

(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review under subparagraph (A).

(10) Publication of information

Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall publish information on the website of the Agency regarding the subpoena process under this subsection, including information regarding the following:

(A) Such internal procedures.

(B) The purpose for subpoenas issued pursuant to this subsection.

(C) The subpoena process.

(D) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.

(E) Policies and procedures on retention and sharing of data obtained by subpoenas.

(F) Guidelines on how entities contacted by the Director may respond to notice of a subpoena.

(11) Annual reports

The Director shall annually 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 (which may include a classified annex but with the presumption of declassification) on the use of subpoenas issued pursuant to this subsection, which shall include the following:

(A) A discussion of the following:

(i) The effectiveness of the use of such subpoenas to mitigate critical infrastructure security vulnerabilities.

(ii) The critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection.

(iii) The number of subpoenas so issued during the preceding year.

(iv) To the extent practicable, the number of vulnerable covered devices or systems mitigated under this subsection by the Agency during the preceding year.

(v) The number of entities notified by the Director under this subsection, and their responses, during the preceding year.

(B) For each subpoena issued pursuant to this subsection, the following:

(i) Information relating to the source of the security vulnerability detected, identified, or received by the Director.

(ii) Information relating to the steps taken to identify the entity at risk prior to issuing the subpoena.

(iii) A description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

(12) Publication of the annual reports

The Director shall publish a version of the annual report required under paragraph (11) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv), and (v) of subparagraph (A) of such paragraph.

(13) Prohibition on use of information for unauthorized purposes

Any information obtained pursuant to a subpoena issued under this subsection may not be provided to any other Federal department or agency for any purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.

(q) Industrial control systems

The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

(5) conduct such other efforts and assistance as the Secretary determines appropriate.

(r) Coordination on cybersecurity for SLTT entities

(1)[1] Coordination

The Center shall, upon request and to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

(A) conduct exercises with SLTT entities;

(B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

(i) cyber threat indicators;

(ii) defensive measures;

(iii) cybersecurity risks;

(iv) vulnerabilities; and

(v) incident response and management;

(C) in order to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable—

(i) cyber threat indicators;

(ii) defensive measures;

(iii) information about cybersecurity risks; and

(iv) information about incidents;

(D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;

(E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—

(i) information about tools;

(ii) information about products;

(iii) resources;

(iv) policies;

(v) guidelines;

(vi) controls; and

(vii) other cybersecurity standards and best practices and procedures related to

[1] So in original. There is no par. (2).

information security, including, as appropriate, information produced by other Federal agencies;

(F) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;

(G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;

(H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and

(I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

(s) Report

Not later than 1 year after June 21, 2022, and every 2 years 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 services and capabilities that the Agency directly and indirectly provides to SLTT entities.

(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; Pub. L. 116–94, div. L, §102(a), Dec. 20, 2019, 133 Stat. 3089; Pub. L. 116–283, div. A, title XVII, §1716(a), Jan. 1, 2021, 134 Stat. 4094; Pub. L. 117–81, div. A, title XV, §§1541(a), 1542, 1548(c), Dec. 27, 2021, 135 Stat. 2054, 2056, 2063; Pub. L. 117–103, div. Y, §103(a)(1), Mar. 15, 2022, 136 Stat. 1038; Pub. L. 117–150, §2(2), June 21, 2022, 136 Stat. 1295; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(D), Dec. 23, 2022, 136 Stat. 3659.)

Editorial Notes

REFERENCES IN TEXT

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

This chapter, referred to in subsec. (p)(8), 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 below and Tables.

CODIFICATION

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

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, §7143(b)(2)(D)(i), added subsec. (a) and struck out former subsec. (a) which defined cybersecurity purpose, cybersecurity risk, cyber threat indicator, defensive measure, cybersecurity vulnerability, incident, information sharing and analysis organization, information system, security vulnerability, and sharing.

Subsec. (b). Pub. L. 117–263, §7143(b)(2)(D)(ii), inserted ''Executive'' before ''Assistant Director for Cybersecurity''.

Subsec. (c)(6). Pub. L. 117–150, §2(2)(A), inserted ''operational and'' before ''timely''.

Subsec. (c)(13). Pub. L. 117–103 added par. (13).

Subsec. (d)(1)(A)(iii). Pub. L. 117–263, §7143(b)(2)(D)(iii)(I), struck out '', as that term is defined under section 3003(4) of title 50'' after ''intelligence community''.

Subsec. (d)(1)(B)(ii). Pub. L. 117–263, §7143(b)(2)(D)(iii)(II), substituted ''Information Sharing and Analysis Organizations'' for ''information sharing and analysis organizations''.

Subsec. (d)(1)(E). Pub. L. 117–150, §2(2)(B), inserted '', including an entity that collaborates with election officials,'' after ''governments''.

Subsec. (e)(1)(E)(ii)(II). Pub. L. 117–263, §7143(b)(2)(D)(iv), substituted ''Information Sharing and Analysis Organizations'' for ''information sharing and analysis organizations''.

Subsec. (p). Pub. L. 117–263, §7143(b)(2)(D)(v), redesignated subsec. (p) relating to coordination on cybersecurity for SLTT entities as (r).

Pub. L. 117–150, §2(2)(C), added subsec. (p) relating to coordination on cybersecurity for SLTT entities.

Subsec. (q). Pub. L. 117–263, §7143(b)(2)(D)(vi), redesignated subsec. (q) relating to report as (s).

Pub. L. 117–150, §2(2)(C), added subsec. (q) relating to report.

Subsec. (r). Pub. L. 117–263, §7143(b)(2)(D)(v), redesignated subsec. (p) relating to coordination on cybersecurity for SLTT entities as (r).

Subsec. (s). Pub. L. 117–263, §7143(b)(2)(D)(vi), redesignated subsec. (q) relating to report as (s).

2021—Subsec. (a). Pub. L. 117–81, §1542(1), added par. (4) and redesignated former pars. (4) to (8) (as previously added or redesignated by Pub. L. 116–283) as (5) to (9), respectively.

Pub. L. 116–283, §1716(a)(1), added pars. (1) and (7) and redesignated former pars. (1) to (5) as (2) to (6), respectively, and former par. (6) as (8).

Subsec. (c)(5)(B), (C). Pub. L. 117–81, §1542(2)(A), added subpar. (B), redesignated former subpar. (B) as (C), and inserted in subpar. (C) as redesignated ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate,'' before ''with Federal''.

Subsec. (c)(6). Pub. L. 117–81, §1548(c), inserted '', which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions'' after ''mitigation, and remediation''.

Subsec. (c)(7)(C). Pub. L. 117–81, §1542(2)(B), substituted ''share'' for ''sharing''.

Subsec. (c)(9). Pub. L. 117–81, §1542(2)(C), inserted ''mitigation protocols to counter cybersecurity vulnerabilities, as appropriate,'' after ''measures,''.

Subsec. (c)(12). Pub. L. 116–283, §1716(a)(2), added par. (12).

Subsec. (e)(1)(I). Pub. L. 117–81, §1541(a)(1), added subpar. (I).

Subsec. (*o*). Pub. L. 117–81, §1542(4), added subsec. (*o*). Former subsec. (*o*) redesignated (p) relating to subpoena authority.

Pub. L. 116–283, §1716(a)(3), added subsec. (*o*).

Subsec. (p). Pub. L. 117–81, §1542(3), redesignated subsec. (*o*) as (p) relating to subpoena authority.

Subsec. (q). Pub. L. 117–81, §1541(a)(2), added subsec. (q) relating to industrial control systems.

2019—Subsec. (d)(1)(B)(iv). Pub. L. 116–94, §102(a)(1), inserted '', including cybersecurity specialists'' after ''entities''.

Subsec. (f). Pub. L. 116–94, §102(a)(3), added subsec. (f). Former subsec. (f) redesignated (g).

Subsec. (g). Pub. L. 116–94, §102(a)(2), redesignated subsec. (f) as (g). Former subsec. (g) redesignated (h).

Subsec. (g)(1), (2). Pub. L. 116–94, §102(a)(4), inserted '', or any team or activity of the Center,'' after ''Center''.

Subsecs. (h) to (n). Pub. L. 116–94, §102(a)(2), redesignated subsecs. (g) to (m) as (h) to (n), respectively.

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*).

Statutory Notes and Related Subsidiaries

RULES OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

Pub. L. 116–283, div. A, title XVII, §1716(b), Jan. 1, 2021, 134 Stat. 4098, provided that:

''(1) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this section or the amendments made by this section [amending this section] may be construed to grant the Secretary of Homeland Security, or the head of any another Federal agency or department, 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 the enactment of this Act [Jan. 1, 2021].

''(2) PRIVATE ENTITIES.—Nothing in this section or the amendments made by this section [amending this section] may be construed to require any private entity to—

''(A) request assistance from the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; or

''(B) implement any measure or recommendation suggested by the Director.''

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); see 6 U.S.C. 650(13)];

''(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, the term ''agency information system'' means an information system used or operated by an agency or by another entity on behalf of an agency.

(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 the Cybersecurity and Infrastructure Security Agency shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

(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.

(e) Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments

(1) In general

(A) Requirement

Not later than one year after December 27, 2021, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(B) Recommendations and requirements

The strategy required under subparagraph (A) shall provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents.

(2) Contents

The strategy required under paragraph (1) shall—

(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

(i) incident exercises, information sharing and incident notification procedures;

(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40;

(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and terri-