

partment who may be involved in the investigation of human trafficking offenses; and

(B) members of all task forces led by the Department that participate in the investigation of human trafficking offenses.

(2) Required instructions

The directive required to be issued under paragraph (1) shall include instructions on—

(A) the investigation of individuals who patronize or solicit human trafficking victims as being engaged in severe trafficking in persons and how such individuals should be investigated for their roles in severe trafficking in persons; and

(B) how victims of sex or labor trafficking often engage in criminal acts as a direct result of severe trafficking in persons and such individuals are victims of a crime and affirmative measures should be taken to avoid arresting, charging, or prosecuting such individuals for any offense that is the direct result of their victimization.

(b) Victim screening protocol

(1) In general

Not later than 180 days after December 21, 2018, the Secretary shall issue a screening protocol for use during all anti-trafficking law enforcement operations in which the Department is involved.

(2) Requirements

The protocol required to be issued under paragraph (1) shall—

(A) require the individual screening of all adults and children who are suspected of engaging in commercial sex acts, child labor that is a violation of law, or work in violation of labor standards to determine whether each individual screened is a victim of human trafficking;

(B) require affirmative measures to avoid arresting, charging, or prosecuting human trafficking victims for any offense that is the direct result of their victimization;

(C) be developed in consultation with relevant interagency partners and nongovernmental organizations that specialize in the prevention of human trafficking or in the identification and support of victims of human trafficking and survivors of human trafficking; and

(D) include—

(i) procedures and practices to ensure that the screening process minimizes trauma or revictimization of the person being screened; and

(ii) guidelines on assisting victims of human trafficking in identifying and receiving restorative services.

(c) Mandatory training

The training described in sections 642 and 644 of this title shall include training necessary to implement—

(1) the directive required under subsection (a); and

(2) the protocol required under subsection (b).

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

Editorial Notes

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.)

Editorial Notes

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

§ 650. Definitions

Except as otherwise specifically provided, in this subchapter:

(1) Agency

The term “Agency” means the Cybersecurity and Infrastructure Security Agency.

(2) 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.

(3) Cloud service provider

The term “cloud service provider” means an entity offering products or services related to cloud computing, as defined by the National

Institute of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto.

(4) 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.

(5) Cyber threat indicator

The term “cyber threat indicator” means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(6) Cybersecurity purpose

The term “cybersecurity purpose” means the purpose of protecting an information sys-

tem or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(7) Cybersecurity risk

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.

(8) Cybersecurity threat

(A) In general

Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) Exclusion

The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(9) Defensive measure

(A) In general

Except as provided in subparagraph (B), the term “defensive measure” means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) Exclusion

The term “defensive measure” does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity, as defined in section 1501 of this title, operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(10) Director

The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency.

(11) Homeland Security Enterprise

The term “Homeland Security Enterprise” means relevant governmental and nongovern-

mental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

(12) Incident

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.

(13) Information Sharing and Analysis Organization

The term “Information Sharing and Analysis Organization” means any formal or informal entity or collaboration created or employed 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 an interference, a compromise, or an 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).

(14) Information system

The term “information system”—

(A) has the meaning given the term in section 3502 of title 44; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(15) Intelligence community

The term “intelligence community” has the meaning given the term in section 3003(4) of title 50.

(16) Malicious cyber command and control

The term “malicious cyber command and control” means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(17) Malicious reconnaissance

The term “malicious reconnaissance”¹ a method for actively probing or passively moni-

toring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(18) Managed service provider

The term “managed service provider” means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

(19) Monitor

The term “monitor” means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(20) 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.

(21) National security system

The term “national security system” has the meaning given the term in section 11103 of title 40.

(22) Ransomware attack

The term “ransomware attack”—

(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(B) does not include any such event in which the demand for payment is—

(i) not genuine; or

(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

(23) Sector Risk Management Agency

The term “Sector Risk Management Agency” means a Federal department or agency,

¹ So in original. Probably should be followed by “means”.

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.

(24) Security control

The term “security control” means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(25) Security vulnerability

The term “security vulnerability” means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(26) Sharing

The term “sharing” (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

(27) SLTT entity

The term “SLTT entity” means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.

(28) Supply chain compromise

The term “supply chain compromise” means an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

(Pub. L. 107–296, title XXII, § 2200, as added Pub. L. 117–263, div. G, title LXXI, § 7143(b)(1), Dec. 23, 2022, 136 Stat. 3654.)

Statutory Notes and Related Subsidiaries

RULE OF CONSTRUCTION

Pub. L. 117–263, div. G, title LXXI, § 7143(f), Dec. 23, 2022, 136 Stat. 3664, provided that:

“(1) INTERPRETATION OF TECHNICAL CORRECTIONS.—Nothing in the amendments made by subsections (a) through (d) [enacting this section and amending sections 195f, 321l, 464, 571, 624, 651 to 652a, 655, 656, 659 to 663, 665, 665b, 665d, 665g, 665i, 671, 681, 1501, 1521, and 1524 of this title, sections 278g–3a and 648 of Title 15, Commerce and Trade, section 824s–1 of Title 16, Conservation, sections 300hh–10 and 18723 of Title 42, The Public Health and Welfare, section 70101 of Title 46, Shipping, and sections 3049a and 3371a of Title 50, War and National Defense] shall be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in section 3502 of title 44, United States Code) or officer or employee of the United States on or before the date of enactment of this Act [Dec. 23, 2022].

“(2) INTERPRETATION OF REFERENCES TO DEFINITIONS.—Any reference to a term defined in the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) on the day before the date of enactment of this Act that is defined in section 2200 of that Act [6 U.S.C. 650] pursuant to the

amendments made under this Act [Pub. L. 117–263, see Tables for classification] shall be deemed to be a reference to that term as defined in section 2200 of the Homeland Security Act of 2002, as added by this Act.”

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

§ 651. Definition

In this part, the term “Cybersecurity Advisory Committee” means the advisory committee established under section 665e(a) of this title.

(Pub. L. 107–296, title XXII, § 2201, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4168; amended Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(C), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–150, § 2(1), June 21, 2022, 136 Stat. 1295; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(B), Dec. 23, 2022, 136 Stat. 3659.)

Editorial Notes

AMENDMENTS

2022—Pub. L. 117–263 amended section generally. Prior to amendment, section defined critical infrastructure information, cybersecurity risk, cybersecurity threat, national cybersecurity asset response activities, Sector Risk Management Agency, sharing, and SLTT entity.

Par. (7). Pub. L. 117–150 added par. (7).

2021—Par. (5). Pub. L. 116–283 substituted “Sector Risk Management Agency” for “Sector-Specific Agency” in heading and “Sector Risk Management Agency” for “Sector-Specific Agency” in text.

Statutory Notes and Related Subsidiaries

RULE 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, and references to terms defined in the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) on the day before Dec. 23, 2022, that are defined in section 650 of this title are deemed to be references to those terms as defined in such section 650, see section 7143(f) of Pub. L. 117–263, set out as a note under section 650 of this title.

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.”

NATIONAL CYBER EXERCISES

Pub. L. 116–283, div. A, title XVII, § 1744, Jan. 1, 2021, 134 Stat. 4135, provided that:

“(a) REQUIREMENT.—Not later than December 31, 2023, the Secretary of Homeland Security, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall conduct an exercise, which may be a tabletop exercise, to

test the resilience, response, and recovery of the United States to a significant cyber incident impacting critical infrastructure. The Secretary shall convene similar exercises not fewer than three times, in consultation with such officials, until 2033.

“(b) PLANNING AND PREPARATION.—The exercises required under subsection (a) shall be prepared by—

“(1) appropriate personnel from—

“(A) the Department of Homeland Security;

“(B) the Department of Defense; and

“(C) the Department of Justice; and

“(2) appropriate elements of the intelligence community, identified by the Director of National Intelligence.

“(c) SUBMISSION TO CONGRESS.—For each fiscal year in which an exercise is planned, the Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall submit to the appropriate congressional committees a plan for the exercise not later than 180 days prior to the exercise. Each such plan shall include information regarding the goals of the exercise at issue, how the exercise is to be carried out, where and when the exercise will take place, how many individuals are expected to participate from each Federal agency specified in subsection (b), and the costs or other resources associated with the exercise.

“(d) PARTICIPANTS.—

“(1) FEDERAL GOVERNMENT PARTICIPANTS.—Appropriate personnel from the following Federal agencies shall participate in each exercise required under subsection (a):

“(A) The Department of Homeland Security.

“(B) The Department of Defense, as identified by the Secretary of Defense.

“(C) Elements of the intelligence community, as identified by the Director of National Intelligence.

“(D) The Department of Justice, as identified by the Attorney General.

“(E) Sector-specific agencies, as determined by the Secretary of Homeland Security.

“(2) STATE AND LOCAL GOVERNMENTS.—The Secretary shall invite representatives from State, local, and Tribal governments to participate in each exercise required under subsection (a) if the Secretary determines such is appropriate.

“(3) PRIVATE ENTITIES.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary, in consultation with the senior representative of the sector-specific agencies participating in such exercise in accordance with paragraph (1)(E), shall invite the following individuals to participate:

“(A) Representatives from appropriate private entities.

“(B) Other individuals whom the Secretary determines will best assist the United States in preparing for, and defending against, a significant cyber incident impacting critical infrastructure.

“(4) INTERNATIONAL PARTNERS.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary may, in coordination with the Secretary of State, invite allies and partners of the United States to participate in such exercise.

“(e) OBSERVERS.—The Secretary may invite representatives from the executive and legislative branches of the Federal Government to observe an exercise required under subsection (a).

“(f) ELEMENTS.—Each exercise required under subsection (a) shall include the following elements:

“(1) Exercising the orchestration of cybersecurity response and the provision of cyber support to Federal, State, local, and Tribal governments and private entities, including the exercise of the command, control, and deconfliction of—

“(A) operational responses through interagency coordination processes and response groups; and

“(B) each Federal agency participating in such exercise in accordance with subsection (d)(1).

“(2) Testing of the information sharing needs and capabilities of exercise participants.

“(3) Testing of the relevant policy, guidance, and doctrine, including the National Cyber Incident Response Plan of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

“(4) Testing of the integration and interoperability between the entities participating in the exercise in accordance with subsection (d).

“(5) Exercising the integration and interoperability of the cybersecurity operation centers of the Federal Government, as appropriate, in coordination with appropriate cabinet level officials.

“(g) BRIEFING.—

“(1) IN GENERAL.—Not later than 180 days after the date on which each exercise required under subsection (a) is conducted, the Secretary shall provide to the appropriate congressional committees a briefing on the exercise.

“(2) CONTENTS.—Each briefing required under paragraph (1) shall include—

“(A) an assessment of the decision and response gaps observed in the exercise at issue;

“(B) proposed recommendations to improve the resilience, response, and recovery of the United States to a significant cyber attack against critical infrastructure; and

“(C) appropriate plans to address the recommendations proposed under subparagraph (B).

“(h) REPEAL.—[Repealed section 1648(b) of Pub. L. 114-92, 129 Stat. 1119.]

“(i) DEFINITIONS.—In this section:

“(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ means—

“(A) the Committee on Armed Services of the Senate;

“(B) the Committee on Armed Services of the House of Representatives;

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

“(D) the Committee on Homeland Security of the House of Representatives;

“(E) the Select Committee on Intelligence of the Senate;

“(F) the Permanent Select Committee on Intelligence of the House of Representatives;

“(G) the Committee on the Judiciary of the Senate;

“(H) the Committee on the Judiciary of the House of Representatives;

“(I) the Committee on Commerce, Science, and Transportation of the Senate;

“(J) the Committee on Science, Space, and Technology of the House of Representatives;

“(K) the Committee on Foreign Relations of the Senate; and

“(L) the Committee on Foreign Affairs of the House of Representatives.

“(2) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term ‘element of the intelligence community’ means an element specified or designated under section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

“(3) PRIVATE ENTITY.—The term ‘private entity’ has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

“(4) SECRETARY.—The term ‘Secretary’ means the Secretary of Homeland Security.

“(5) SECTOR-SPECIFIC AGENCY.—The term ‘sector-specific agency’ has the meaning given the term ‘Sector-Specific Agency’ in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651) [see 6 U.S.C. 650].

“(6) STATE.—The term ‘State’ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.”

Executive Documents

EX. ORD. NO. 13905. STRENGTHENING NATIONAL RESILIENCE THROUGH RESPONSIBLE USE OF POSITIONING, NAVIGATION, AND TIMING SERVICES

Ex. Ord. No. 13905, Feb. 12, 2020, 85 F.R. 9359, provided:

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

SECTION 1. Purpose. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure. Since the United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response. Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

SEC. 2. Definitions. As used in this order:

(a) “PNT services” means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(b) “Responsible use of PNT services” means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(c) “Critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters.

(d) “PNT profile” means a description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.

(e) “Sector-Specific Agency” (SSA) is the executive department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

SEC. 3. Policy. It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation’s awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.

To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

SEC. 4. Implementation. (a) Within 1 year of the date of this order [Feb. 12, 2020], the Secretary of Commerce, in coordination with the heads of SSAs and in consultation, as appropriate, with the private sector, shall develop and make available, to at least the appropriate agencies and private sector users, PNT profiles. The PNT profiles will enable the public and private sectors

to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Once made available, the PNT profiles shall be reviewed every 2 years and, as necessary, updated.

(b) The Secretary of Defense, Secretary of Transportation, and Secretary of Homeland Security shall refer to the PNT profiles created pursuant to subsection (a) of this section in updates to the Federal Radio-navigation Plan.

(c) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services. The results of the tests carried out under that plan shall be used to inform updates to the PNT profiles identified in subsection (a) of this section.

(d) Within 90 days of the PNT profiles being made available, the heads of SSAs and the heads of other executive departments and agencies (agencies), as appropriate, through the Secretary of Homeland Security, shall develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services. The heads of SSAs and the heads of other agencies, as appropriate, shall update the requirements as necessary.

(e) Within 180 days of the completion of any of the duties described in subsection (d) of this section, and consistent with applicable law and to the maximum extent practicable, the Federal Acquisition Regulatory Council, in consultation with the heads of SSAs and the heads of other agencies, as appropriate, shall incorporate the requirements developed under subsection (d) of this section into Federal contracts for products, systems, and services that integrate or use PNT services.

(f) Within 1 year of the PNT profiles being made available, and biennially thereafter, the heads of SSAs and the heads of other agencies, as appropriate, through the Secretary of Homeland Security, shall submit a report to the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy (OSTP) on the extent to which the PNT profiles have been adopted in their respective agencies’ acquisitions and, to the extent possible, the extent to which PNT profiles have been adopted by owners and operators of critical infrastructure.

(g) Within 180 days of the date of this order, the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services. Each pilot program shall be completed within 1 year of developing the plan, and the results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities.

(h) Within 1 year of the date of this order, the Director of OSTP shall coordinate the development of a national plan, which shall be informed by existing initiatives, for the R&D and pilot testing of additional, robust, and secure PNT services that are not dependent on global navigation satellite systems (GNSS). The plan shall also include approaches to integrate and use multiple PNT services to enhance the resilience of critical infrastructure.

Once the plan is published, the Director of OSTP shall coordinate updates to the plan every 4 years, or as appropriate.

(i) Within 180 days of the date of this order, the Secretary of Commerce shall make available a GNSS-independent source of Coordinated Universal Time, to support the needs of critical infrastructure owners and operators, for the public and private sectors to access.

SEC. 5. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

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

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

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

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

DONALD J. TRUMP.

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

§ 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”.

(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 the Director, who shall report to the Secretary.

(2) Qualifications

(A) In general

The Director shall be appointed from among individuals who have—

(i) extensive knowledge in at least two of the areas specified in subparagraph (B); and

(ii) not fewer than five years of demonstrated experience in efforts to foster coordination and collaboration between the Federal Government, the private sector, and other entities on issues related to cybersecurity, infrastructure security, or security risk management.

(B) Specified areas

The areas specified in this subparagraph are the following:

(i) Cybersecurity.

(ii) Infrastructure security.

(iii) Security risk management.

(3) 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 the Cybersecurity and Infrastructure Security Agency.

(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)), including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;

(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;

(11) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security;

(12) appoint a Cybersecurity State Coordinator in each State, as described in section 665c of this title;

(13) carry out the duties and authorities relating to the .gov internet domain, as described in section 665 of this title; and

(14) 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 the Cybersecurity and Infrastructure Security Agency 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 De-

partment, 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.

(R) To encourage and build cybersecurity awareness and competency across the United States and to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department, including by—

- (i) overseeing elementary and secondary cybersecurity education and awareness related programs at the Agency;
- (ii) leading efforts to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department;
- (iii) encouraging and building cybersecurity awareness and competency across the United States; and
- (iv) carrying out cybersecurity related workforce development activities, including through—

(I) increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and

(II) building awareness of and competency in cybersecurity across the civilian Federal Government workforce.

(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 non-reimbursable basis.

(f) Composition

The Agency shall be composed of the following divisions:

- (1) The Cybersecurity Division, headed by an Executive Assistant Director.
- (2) The Infrastructure Security Division, headed by an Executive Assistant Director.
- (3) The Emergency Communications Division under subchapter XIII, headed by an Executive Assistant Director.

(g) Co-location

(1) In general

To the maximum extent practicable, the Director shall examine the establishment of cen-

tral 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 Risk Management 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; amended Pub. L. 116-260, div. U, title IX, § 904(b)(1)(A), Dec. 27, 2020, 134 Stat. 2298; Pub. L. 116-283, div. A, title XVII, §§ 1717(a)(1)(A), 1719(a), (b), div. H, title XC, §§ 9001(a), 9002(c)(2)(D), Jan. 1, 2021, 134 Stat. 4099, 4105, 4766, 4773; Pub. L. 117-81, div. A, title XV, §§ 1547(b)(1)(A)(i), (B), 1549(a), Dec. 27, 2021, 135 Stat. 2060, 2061, 2063; Pub. L. 117-263, div. G, title LXXI, § 7143(a)(1), (b)(2)(C), (c)(5), Dec. 23, 2022, 136 Stat. 3654, 3659, 3663.)

Editorial Notes

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.

AMENDMENTS

2022—Pub. L. 117-263, § 7143(a)(1), made amendment identical to that made by Pub. L. 117-81, § 1547(b)(1)(B). See 2021 Amendment note below.

Subsec. (a)(1). Pub. L. 117-263, § 7143(b)(2)(C)(i), which directed striking out “(in this part referred to as the Agency)”, was executed by striking out “(in this part referred to as the ‘Agency’)” before period at end, to reflect the probable intent of Congress.

Subsec. (b)(1). Pub. L. 117-263, § 7143(b)(2)(C)(ii), substituted “the Director” for “a Director of Cybersecurity and Infrastructure Security (in this part referred to as the ‘Director’)”.

Subsec. (b)(3). Pub. L. 117-263, § 7143(c)(5)(A), substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Director of Cybersecurity and Infrastructure Security of the Department”.

Subsec. (d). Pub. L. 117-263, § 7143(c)(5)(B), substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Director of Cybersecurity and Infrastructure Security” in introductory provisions.

Subsec. (f). Pub. L. 117-263, § 7143(b)(2)(C)(iii), inserted “Executive” before “Assistant Director” in pars. (1) to (3).

2021—Pub. L. 117-81, § 1547(b)(1)(B), made technical amendment to directory language of Pub. L. 116-260, § 904(b)(1). See 2020 Amendment notes below.

Subsec. (b)(2), (3). Pub. L. 116-283, § 9001(a), added par. (2) and redesignated former par. (2) as (3).

Subsec. (c)(3). Pub. L. 117-81, § 1549(a), substituted “, including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;” for semicolon at end.

Subsec. (c)(10). Pub. L. 116-283, §§ 1717(a)(1)(A)(i), 1719(b)(1), which directed identical amendments of par. (10) by striking out “and” at end, could not be executed because the word “and” did not appear at end after amendment by Pub. L. 116-260, § 904(b)(1)(A)(i). See 2020 Amendment note below.

Subsec. (c)(11). Pub. L. 117-81, § 1547(b)(1)(A)(i)(I), struck out “and” after the semicolon.

Pub. L. 116-283, § 1719(b)(3), added par. (11) relating to providing education, training, and capacity development to Federal and non-Federal entities. Former par. (11), relating to appointment of a Cybersecurity State Coordinator, redesignated (12).

Pub. L. 116-283, § 1717(a)(1)(A)(iii), added par. (11) relating to appointment of a Cybersecurity State Coordinator. Former par. (11), relating to the .gov internet domain, redesignated (12).

Subsec. (c)(12). Pub. L. 117-81, § 1547(b)(1)(A)(i)(II), struck out “and” at end and made technical amendment to reference in original Act which appears in text as reference to section 665c of this title.

Pub. L. 116-283, § 1719(b)(2), redesignated par. (11) relating to appointment of a Cybersecurity State Coordinator as (12).

Pub. L. 116-283, § 1717(a)(1)(A)(ii), redesignated par. (11) relating to the .gov internet domain as (12).

Subsec. (c)(13). Pub. L. 117-81, § 1547(b)(1)(A)(i)(III), redesignated par. (12) relating to the .gov internet domain as (13).

Subsec. (c)(14). Pub. L. 117-81, § 1547(b)(1)(A)(i)(IV), redesignated par. (12) relating to carrying out such other duties and powers as (14).

Subsec. (e)(1)(R). Pub. L. 116-283, § 1719(a), added subpar. (R).

Subsec. (i). Pub. L. 116-283, § 9002(c)(2)(D), substituted “Sector Risk Management Agency” for “Sector-Specific Agency”.

2020—Subsec. (c)(10). Pub. L. 116-260, §904(b)(1)(A)(i), as amended by Pub. L. 117-81, §1547(b)(1)(B), struck out “and” at end.

Subsec. (c)(11), (12). Pub. L. 116-260, §904(b)(1)(A)(ii), (iii), as amended by Pub. L. 117-81, §1547(b)(1)(B), added par. (11) relating to the .gov internet domain and redesignated former par. (11) relating to carrying out such other duties and powers as (12).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2022 AMENDMENT

Pub. L. 117-263, div. G, title LXXI, §7143(a)(2), Dec. 23, 2022, 136 Stat. 3654, provided that: “The amendment made by paragraph (1) [amending this section and section 665 of this title] shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116-260).”

CONSTRUCTION OF 2022 AMENDMENT

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.

CONSTRUCTION OF 2021 AMENDMENT

Amendment by section 1717(a)(1)(A) of Pub. L. 116-283 not to be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents, see section 1717(a)(4) of Pub. L. 116-283, set out as a note under section 665c of this title.

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM

Pub. L. 117-122, May 12, 2022, 136 Stat. 1193, provided that:

“SECTION 1. SHORT TITLE.

“This Act may be cited as the ‘National Cybersecurity Preparedness Consortium Act of 2021’.

“SEC. 2. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

“(a) IN GENERAL.—The Secretary may work with one or more consortia to support efforts to address cybersecurity risks and incidents.

“(b) ASSISTANCE TO DHS.—The Secretary may work with one or more consortia to carry out the Secretary’s responsibility pursuant to section 2202(e)(1)(P) of the Homeland Security Act of 2002 (6 U.S.C. 652(e)(1)(P)) to—

“(1) provide training and education to State, Tribal, and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, in accordance with applicable law;

“(2) develop and update a curriculum utilizing existing training and educational programs and models in accordance with section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), for State, Tribal, and local first responders and officials, related to cybersecurity risks and incidents;

“(3) provide technical assistance services, training, and educational programs to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of acts of terrorism, in accordance with such section 2209;

“(4) conduct cross-sector cybersecurity training, education, and simulation exercises for entities, including State and local governments and Tribal organizations, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, in accordance with section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c));

“(5) help States, Tribal organizations, and communities develop cybersecurity information sharing programs, in accordance with section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), for the dissemination of homeland security information related to cybersecurity risks and incidents;

“(6) help incorporate cybersecurity risk and incident prevention and response into existing State, Tribal, and local emergency plans, including continuity of operations plans; and

“(7) assist State governments and Tribal organizations in developing cybersecurity plans.

“(c) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this Act, the Secretary shall take into consideration the following:

“(1) Prior experience conducting cybersecurity training, education, and exercises for State and local entities.

“(2) Geographic diversity of the members of any such consortium so as to maximize coverage of the different regions of the United States.

“(3) The participation in such consortium of one or more historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges that participate in the National Centers of Excellence in Cybersecurity program, as carried out by the Department of Homeland Security.

“(d) METRICS.—If the Secretary works with a consortium under subsection (a), the Secretary shall measure the effectiveness of the activities undertaken by the consortium under this Act.

“(e) OUTREACH.—The Secretary shall conduct outreach to universities and colleges, including, in particular, outreach to historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges, regarding opportunities to support efforts to address cybersecurity risks and incidents, by working with the Secretary under subsection (a).

“(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize a consortium to control or direct any law enforcement agency in the exercise of the duties of the law enforcement agency.

“(g) DEFINITIONS.—In this section—

“(1) the term ‘community college’ has the meaning given the term ‘junior or community college’ in section 312 of the Higher Education Act of 1965 (20 U.S.C. 1058);

“(2) the term ‘consortium’ means a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training and education in support of homeland security;

“(3) the terms ‘cybersecurity risk’ and ‘incident’ have the meanings given those terms in section 2209(a) of the Homeland Security Act of 2002 (6 U.S.C. 659(a)) [see 6 U.S.C. 650(7), (12)];

“(4) the term ‘Department’ means the Department of Homeland Security;

“(5) the term ‘Hispanic-serving institution’ has the meaning given the term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a);

“(6) the term ‘historically Black college and university’ has the meaning given the term ‘part B institution’ in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061);

“(7) the term ‘minority-serving institution’ means an institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a));

“(8) the term ‘Secretary’ means the Secretary of Homeland Security;

“(9) The term ‘State’ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States;

“(10) the term ‘Tribal Colleges and Universities’ has the meaning given the term in section 316 of the Higher Education Act of 1965 (20 U.S.C. 1059c); and

“(11) the term ‘Tribal organization’ has the meaning given the term in section 4(e) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).”

RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM

Pub. L. 117–103, div. Y, §105, Mar. 15, 2022, 136 Stat. 1055, provided that:

“(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act [Mar. 15, 2022], the Director [of the Cybersecurity and Infrastructure Security Agency] shall establish a ransomware vulnerability warning pilot program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

“(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

“(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

“(2) utilize existing authorities to identify information systems that contain the security vulnerabilities identified in paragraph (1).

“(c) ENTITY NOTIFICATION.—

“(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

“(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures under that section.

“(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

“(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

“(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

“(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

“(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.”

[For definitions of terms used in section 105 of div. Y of Pub. L. 117–103, set out above, see section 681 of this title, as made applicable by section 102(1) of div. Y of Pub. L. 117–103, which is set out as a note under section 665j of this title, and see section 650 of this title, as made applicable by section 7143(f)(2) of div. G of Pub. L. 117–263, which is set out as a note under section 650 of this title.]

PILOT PROGRAM ON PUBLIC-PRIVATE PARTNERSHIPS WITH INTERNET ECOSYSTEM COMPANIES TO DETECT AND DISRUPT ADVERSARY CYBER OPERATIONS

Pub. L. 117–81, div. A, title XV, §1550, Dec. 27, 2021, 135 Stat. 2064, provided that:

“(a) PILOT REQUIRED.—Not later than one year after the date of the enactment of this Act [Dec. 27, 2021], the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and in coordination with the Secretary of Defense and the National Cyber Director, shall commence a pilot program to assess the feasibility and advisability of entering into public-private partnerships with internet ecosystem companies to facilitate, within the bounds of applicable provisions of law and such companies’ terms of service, policies, procedures, contracts, and other agreements, actions by such companies to discover and disrupt use by malicious cyber actors of the platforms, systems, services, and infrastructure of such companies.

“(b) PUBLIC-PRIVATE PARTNERSHIPS.—

“(1) IN GENERAL.—In carrying out the pilot program under subsection (a), the Secretary shall seek to enter into one or more public-private partnerships with internet ecosystem companies.

“(2) VOLUNTARY PARTICIPATION.—

“(A) IN GENERAL.—Participation by an internet ecosystem company in a public-private partnership under the pilot program, including in any activity described in subsection (c), shall be voluntary.

“(B) PROHIBITION.—No funds appropriated by any Act may be used to direct, pressure, coerce, or otherwise require that any internet ecosystem company take any action on their platforms, systems, services, or infrastructure as part of the pilot program.

“(c) AUTHORIZED ACTIVITIES.—In carrying out the pilot program under subsection (a), the Secretary may—

“(1) provide assistance to a participating internet ecosystem company to develop effective know-your-customer processes and requirements;

“(2) provide information, analytics, and technical assistance to improve the ability of participating companies to detect and prevent illicit or suspicious procurement, payment, and account creation on their own platforms, systems, services, or infrastructure;

“(3) develop and socialize best practices for the collection, retention, and sharing of data by participating internet ecosystem companies to support discovery of malicious cyber activity, investigations, and attribution on the platforms, systems, services, or infrastructure of such companies;

“(4) provide to participating internet ecosystem companies actionable, timely, and relevant information, such as information about ongoing operations and infrastructure, threats, tactics, and procedures, and indicators of compromise, to enable such companies to detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of such companies;

“(5) provide recommendations for (but not design, develop, install, operate, or maintain) operational workflows, assessment and compliance practices, and training that participating internet ecosystem companies can implement to reliably detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of such companies;

“(6) provide recommendations for accelerating, to the greatest extent practicable, the automation of existing or implemented operational workflows to operate at line-rate in order to enable real-time mitigation without the need for manual review or action;

“(7) provide recommendations for (but not design, develop, install, operate, or maintain) technical capabilities to enable participating internet ecosystem companies to collect and analyze data on malicious activities occurring on the platforms, systems, services, or infrastructure of such companies to detect and disrupt operations of malicious cyber actors; and

“(8) provide recommendations regarding relevant mitigations for suspected or discovered malicious cyber activity and thresholds for action.

“(d) COMPETITION CONCERNS.—Consistent with section 1905 of title 18, United States Code, the Secretary shall

ensure that any trade secret or proprietary information of a participating internet ecosystem company made known to the Federal Government pursuant to a public-private partnership under the pilot program remains private and protected unless explicitly authorized by such company.

“(e) IMPARTIALITY.—In carrying out the pilot program under subsection (a), the Secretary may not take any action that is intended primarily to advance the particular business interests of an internet ecosystem company but is authorized to take actions that advance the interests of the United States, notwithstanding differential impact or benefit to a given company’s or given companies’ business interests.

“(f) RESPONSIBILITIES.—

“(1) SECRETARY OF HOMELAND SECURITY.—The Secretary shall exercise primary responsibility for the pilot program under subsection (a), including organizing and directing authorized activities with participating Federal Government organizations and internet ecosystem companies to achieve the objectives of the pilot program.

“(2) NATIONAL CYBER DIRECTOR.—The National Cyber Director shall support prioritization and cross-agency coordination for the pilot program, including ensuring appropriate participation by participating agencies and the identification and prioritization of key private sector entities and initiatives for the pilot program.

“(3) SECRETARY OF DEFENSE.—The Secretary of Defense shall provide support and resources to the pilot program, including the provision of technical and operational expertise drawn from appropriate and relevant officials and components of the Department of Defense, including the National Security Agency, United States Cyber Command, the Chief Information Officer, the Office of the Secretary of Defense, military department Principal Cyber Advisors, and the Defense Advanced Research Projects Agency.

“(g) PARTICIPATION OF OTHER FEDERAL GOVERNMENT COMPONENTS.—The Secretary may invite to participate in the pilot program required under subsection (a) the heads of such departments or agencies as the Secretary considers appropriate.

“(h) INTEGRATION WITH OTHER EFFORTS.—The Secretary shall ensure that the pilot program required under subsection (a) makes use of, builds upon, and, as appropriate, integrates with and does not duplicate other efforts of the Department of Homeland Security and the Department of Defense relating to cybersecurity, including the following:

“(1) The Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

“(2) The Cybersecurity Collaboration Center and Enduring Security Framework of the National Security Agency.

“(i) RULES OF CONSTRUCTION.—

“(1) LIMITATION ON GOVERNMENT ACCESS TO DATA.—Nothing in this section authorizes sharing of information, including information relating to customers of internet ecosystem companies or private individuals, from an internet ecosystem company to an agency, officer, or employee of the Federal Government unless otherwise authorized by another provision of law.

“(2) STORED COMMUNICATIONS ACT.—Nothing in this section may be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the ‘Stored Communications Act’).

“(3) THIRD PARTY CUSTOMERS.—Nothing in this section may be construed to require a third party, such as a customer or managed service provider of an internet ecosystem company, to participate in the pilot program under subsection (a).

“(j) BRIEFINGS.—

“(1) INITIAL.—

“(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary, in coordination with the Secretary of Defense and the National Cyber Director, shall brief the appropriate committees of Congress on the pilot program required under subsection (a).

“(B) ELEMENTS.—The briefing required under subparagraph (A) shall include the following:

“(i) The plans of the Secretary for the implementation of the pilot program.

“(ii) Identification of key priorities for the pilot program.

“(iii) Identification of any potential challenges in standing up the pilot program or impediments, such as a lack of liability protection, to private sector participation in the pilot program.

“(iv) A description of the roles and responsibilities in the pilot program of each participating Federal entity.

“(2) ANNUAL.—

“(A) IN GENERAL.—Not later than two years after the date of the enactment of this Act and annually thereafter for three years, the Secretary, in coordination with the Secretary of Defense and the National Cyber Director, shall brief the appropriate committees of Congress on the progress of the pilot program required under subsection (a).

“(B) ELEMENTS.—Each briefing required under subparagraph (A) shall include the following:

“(i) Recommendations for addressing relevant policy, budgetary, and legislative gaps to increase the effectiveness of the pilot program.

“(ii) Recommendations, such as providing liability protection, for increasing private sector participation in the pilot program.

“(iii) A description of the challenges encountered in carrying out the pilot program, including any concerns expressed by internet ecosystem companies regarding participation in the pilot program.

“(iv) The findings of the Secretary with respect to the feasibility and advisability of extending or expanding the pilot program.

“(v) Such other matters as the Secretary considers appropriate.

“(k) TERMINATION.—The pilot program required under subsection (a) shall terminate on the date that is five years after the date of the enactment of this Act [Dec. 27, 2021].

“(l) DEFINITIONS.—In this section:

“(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ‘appropriate committees of Congress’ means—

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

“(B) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives.

“(2) INTERNET ECOSYSTEM COMPANY.—The term ‘internet ecosystem company’ means a business incorporated in the United States that provides cybersecurity services, internet service, content delivery services, Domain Name Service, cloud services, mobile telecommunications services, email and messaging services, internet browser services, or such other services as the Secretary determines appropriate for the purposes of the pilot program under subsection (a).

“(3) SECRETARY.—The term ‘Secretary’ means the Secretary of Homeland Security.”

K-12 CYBERSECURITY

Pub. L. 117–47, Oct. 8, 2021, 135 Stat. 397, provided that:

“SECTION 1. SHORT TITLE.

“This Act may be cited as the ‘K-12 Cybersecurity Act of 2021’.

“SEC. 2. FINDINGS.

“Congress finds the following:

“(1) K–12 educational institutions across the United States are facing cyber attacks.

“(2) Cyber attacks place the information systems of K–12 educational institutions at risk of possible disclosure of sensitive student and employee information, including—

“(A) grades and information on scholastic development;

“(B) medical records;

“(C) family records; and

“(D) personally identifiable information.

“(3) Providing K–12 educational institutions with resources to aid cybersecurity efforts will help K–12 educational institutions prevent, detect, and respond to cyber events.

“SEC. 3. K–12 EDUCATION CYBERSECURITY INITIATIVE.

“(a) DEFINITIONS.—In this section:

“(1) CYBERSECURITY RISK.—The term ‘cybersecurity risk’ has the meaning given the term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) [see 6 U.S.C. 650].

“(2) DIRECTOR.—The term ‘Director’ means the Director of Cybersecurity and Infrastructure Security.

“(3) INFORMATION SYSTEM.—The term ‘information system’ has the meaning given the term in section 3502 of title 44, United States Code.

“(4) K–12 EDUCATIONAL INSTITUTION.—The term ‘K–12 educational institution’ means an elementary school or a secondary school, as those terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

“(b) STUDY.—

“(1) IN GENERAL.—Not later than 120 days after the date of enactment of this Act [Oct. 8, 2021], the Director, in accordance with subsection (g)(1), shall conduct a study on the specific cybersecurity risks facing K–12 educational institutions that—

“(A) analyzes how identified cybersecurity risks specifically impact K–12 educational institutions;

“(B) includes an evaluation of the challenges K–12 educational institutions face in—

“(i) securing—

“(I) information systems owned, leased, or relied upon by K–12 educational institutions; and

“(II) sensitive student and employee records; and

“(ii) implementing cybersecurity protocols;

“(C) identifies cybersecurity challenges relating to remote learning; and

“(D) evaluates the most accessible ways to communicate cybersecurity recommendations and tools.

“(2) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Director shall provide a Congressional briefing on the study conducted under paragraph (1).

“(c) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after the completion of the study required under subsection (b)(1), the Director, in accordance with subsection (g)(1), shall develop recommendations that include cybersecurity guidelines designed to assist K–12 educational institutions in facing the cybersecurity risks described in subsection (b)(1), using the findings of the study.

“(d) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the completion of the development of the recommendations required under subsection (c), the Director shall develop an online training toolkit designed for officials at K–12 educational institutions to—

“(1) educate the officials about the cybersecurity recommendations developed under subsection (c); and

“(2) provide strategies for the officials to implement the recommendations developed under subsection (c).

“(e) PUBLIC AVAILABILITY.—The Director shall make available on the website of the Department of Homeland Security with other information relating to school safety the following:

“(1) The findings of the study conducted under subsection (b)(1).

“(2) The cybersecurity recommendations developed under subsection (c).

“(3) The online training toolkit developed under subsection (d).

“(f) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under [subsection] (c) by K–12 educational institutions shall be voluntary.

“(g) CONSULTATION.—

“(1) IN GENERAL.—In the course of the conduction of the study required under subsection (b)(1) and the development of the recommendations required under subsection (c), the Director shall consult with individuals and entities focused on cybersecurity and education, as appropriate, including—

“(A) teachers;

“(B) school administrators;

“(C) Federal agencies;

“(D) non-Federal cybersecurity entities with experience in education issues; and

“(E) private sector organizations.

“(2) INAPPLICABILITY OF FACA.—The Federal Advisory Committee Act ([former] 5 U.S.C. App.) [see 5 U.S.C. 1001 et seq.] shall not apply to any consultation under paragraph (1).”

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.”

§ 652a. Sector Risk Management Agencies

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

(A) the Committee on Homeland Security and the Committee on Armed Services in the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services in the Senate.

(2) Critical infrastructure

The term “critical infrastructure” has the meaning given that term in section 5195c(e) of title 42.

(3) Department

The term “Department” means the Department of Homeland Security.

(4) Director

The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency of the Department.

(5) Secretary

The term “Secretary” means the Secretary of Homeland Security.

(7)¹ Sector Risk Management Agency

The term “Sector Risk Management Agency” has the meaning given the term in section 650 of this title.

¹ So in original. Probably should be “(6)”.

(b) Critical infrastructure sector designation**(1) Initial review**

Not later than 180 days after January 1, 2021, the Secretary, in consultation with the heads of Sector Risk Management Agencies, shall—

(A) review the current framework for securing critical infrastructure, as described in section 652(c)(4) of this title and Presidential Policy Directive 21; and

(B) submit to the President and appropriate congressional committees a report that includes—

(i) information relating to—

(I) the analysis framework or methodology used to—

(aa) evaluate the current framework for securing critical infrastructure referred to in subparagraph (A); and

(bb) develop recommendations to—

(AA) revise the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) identify and designate any subsectors of such sectors;

(II) the data, metrics, and other information used to develop the recommendations required under clause (ii); and

(ii) recommendations relating to—

(I) revising—

(aa) the current framework for securing critical infrastructure referred to in subparagraph (A);

(bb) the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(cc) the identification and designation of any subsectors of such sectors; and

(II) any revisions to the list of designated Federal departments or agencies that serve as the Sector Risk Management Agency for a sector or subsector of such section, necessary to comply with paragraph (3)(B).

(2) Periodic evaluation by the Secretary

At least once every five years, the Secretary, in consultation with the Director and the heads of Sector Risk Management Agencies, shall—

(A) evaluate the current list of designated critical infrastructure sectors and subsectors of such sectors and the appropriateness of Sector Risk Management Agency designations, as set forth in Presidential Policy Directive 21, any successor or related document, or policy; and

(B) recommend, as appropriate, to the President—

(i) revisions to the current list of designated critical infrastructure sectors or subsectors of such sectors; and

(ii) revisions to the designation of any Federal department or agency designated as the Sector Risk Management Agency for a sector or subsector of such sector.

(3) Review and revision by the President

Not later than 180 days after the Secretary submits a recommendation pursuant to paragraph (1) or (2), the President shall—

(A) review the recommendation and revise, as appropriate, the designation of a critical infrastructure sector or subsector or the designation of a Sector Risk Management Agency; and

(B) submit to the appropriate congressional committees, the Majority and Minority Leaders of the Senate, and the Speaker and Minority Leader of the House of Representatives, a report that includes—

(i) an explanation with respect to the basis for accepting or rejecting the recommendations of the Secretary; and

(ii) information relating to the analysis framework, methodology, metrics, and data used to—

(I) evaluate the current framework for securing critical infrastructure referred to in paragraph (1)(A); and

(II) develop—

(aa) recommendations to revise—

(AA) the list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) the designation of any subsectors of such sectors; and

(bb) the recommendations of the Secretary.

(4) Publication

Any designation of critical infrastructure sectors shall be published in the Federal Register.

(c) Sector Risk Management Agencies**(1) Omitted****(2) Omitted****(3) References**

Any reference to a Sector Specific Agency (including any permutations or conjugations thereof) in any law, regulation, map, document, record, or other paper of the United States shall be deemed to—

(A) be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector; and

(B) have the meaning given such term in section 650 of this title.

(4) Omitted**(d) Report and auditing**

Not later than two years after January 1, 2021 and every four years thereafter for 12 years, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under section 665d of this title.

(Pub. L. 116-283, div. H, title XC, §9002, Jan. 1, 2021, 134 Stat. 4768; Pub. L. 117-263, div. G, title LXXI, §7143(d)(5), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes**CODIFICATION**

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Section is comprised of section 9002 of Pub. L. 116-283. Subsec. (c)(1) of section 9002 of Pub. L. 116-283 enacted section 665d of this title. Subsec. (c)(2) of section 9002 of Pub. L. 116-283 amended sections 195f, 321m, 651, 652, and 664 of this title. Subsec. (c)(4) of section 9002 of Pub. L. 116-283 amended the table of contents in section 1(b) of the Homeland Security Act of 2002.

AMENDMENTS

2022—Subsec. (a)(5). Pub. L. 117-263, § 7143(d)(5)(A)(i), (ii), redesignated par. (6) as (5) and struck out former par. (5). Prior to amendment, text of par (5) read as follows: “The term ‘information sharing and analysis organization’ has the meaning given that term in section 671(5) of this title.”

Subsec. (a)(6), (7). Pub. L. 117-263, § 7143(d)(5)(A)(ii), (iii), which redesignated par. (7) as (6) and then directed the general amendment of par. (7), was executed by making the redesignation and generally amending par. (6) as redesignated, to reflect the probable intent of Congress. As amended, such par. remained designated as (7). Prior to amendment, text of par. (7) read as follows: “The term ‘sector risk management agency’ has the meaning given the term ‘Sector-Specific Agency’ in section 651(5) of this title.”

Subsec. (c)(3)(B). Pub. L. 117-263, § 7143(d)(5)(B), which directed substitution of “given such term in section 650 of this title” for “given such term in section 651(5) of this title”, was executed by making the substitution for “give such term in section 651(5) of this title”, to reflect the probable intent of Congress.

Subsec. (d). Pub. L. 117-263, § 7143(d)(5)(C), made technical amendment to reference in original act which appears in text as reference to section 665d of this title.

§ 653. Cybersecurity Division**(a) Establishment****(1) In general**

There is established in the Agency a Cybersecurity Division.

(2) Executive Assistant Director

The Cybersecurity Division shall be headed by an Executive Assistant Director for Cybersecurity (in this section referred to as “the Executive 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 or Assistant Director for Cybersecurity in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Cybersecurity.

(b) Functions

The Executive 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; amended Pub. L. 116-283, div. H, title XC, § 9001(c)(1), Jan. 1, 2021, 134 Stat. 4766.)

Editorial Notes**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.

AMENDMENTS

2021—Subsec. (a)(2). Pub. L. 116-283, § 9001(c)(1)(A)(i), in heading, substituted “Executive Assistant Director” for “Assistant Director” and, in introductory provisions, substituted “Executive Assistant Director for Cybersecurity” for “Assistant Director for Cybersecurity” and “the Executive Assistant Director” for “the Assistant Director”.

Subsec. (a)(3). Pub. L. 116-283, § 9001(c)(1)(A)(ii), inserted “or Assistant Director for Cybersecurity” after “Assistant Secretary for Cybersecurity” and substituted “Executive Assistant Director for Cybersecurity.” for “Assistant Director for Cybersecurity.”

Subsec. (b). Pub. L. 116-283, § 9001(c)(1)(B), substituted “Executive Assistant Director” for “Assistant Director” in introductory provisions.

Statutory Notes and Related Subsidiaries**CONTINUATION IN OFFICE**

Pub. L. 116-283, div. H, title XC, § 9001(c)(2), Jan. 1, 2021, 134 Stat. 4767, provided that: “The individual serving as the Assistant Director for Cybersecurity of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act [Jan. 1, 2021] may serve as the Executive Assistant Director for Cybersecurity on and after that date without the need for renomination or reappointment.”

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) Executive Assistant Director

The Infrastructure Security Division shall be headed by an Executive Assistant Director

for Infrastructure Security (in this section referred to as “the Executive 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 or Assistant Director for Infrastructure Security in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Infrastructure Security.

(b) Functions

The Executive 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; amended Pub. L. 116-283, div. H, title XC, §9001(d)(1), Jan. 1, 2021, 134 Stat. 4767.)

Editorial Notes

AMENDMENTS

2021—Subsec. (a)(2). Pub. L. 116-283, §9001(d)(1)(A)(i), in heading, substituted “Executive Assistant Director” for “Assistant Director” and, in introductory provisions, substituted “Executive Assistant Director for Infrastructure Security” for “Assistant Director for Infrastructure Security” and “the Executive Assistant Director” for “the Assistant Director”.

Subsec. (a)(3). Pub. L. 116-283, §9001(d)(1)(A)(ii), inserted “or Assistant Director for Infrastructure Security” after “Assistant Secretary for Infrastructure Protection” and substituted “Executive Assistant Director for Infrastructure Security.” for “Assistant Director for Infrastructure Security.”

Subsec. (b). Pub. L. 116-283, §9001(d)(1)(B), substituted “Executive Assistant Director” for “Assistant Director” in introductory provisions.

Statutory Notes and Related Subsidiaries

CONTINUATION IN OFFICE

Pub. L. 116-283, div. H, title XC, §9001(d)(2), Jan. 1, 2021, 134 Stat. 4767, provided that: “The individual serving as the Assistant Director for Infrastructure Security of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act [Jan. 1, 2021] may serve as the Executive Assistant Director for Infrastructure Security on and after that date without the need for renomination or reappointment.”

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 the Cybersecurity and Infrastructure Security Agency 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; Pub. L. 117-263, div. G, title LXXI, §7143(c)(6), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes

CODIFICATION

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

AMENDMENTS

2022—Pub. L. 117-263 substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Director of Cybersecurity and Infrastructure Security” in introductory provisions.

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.

Statutory Notes and Related Subsidiaries

RULE 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.

§ 656. NET Guard

The Director of the Cybersecurity and Infrastructure Security Agency 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; Pub. L. 117–263, div. G, title LXXI, §7143(c)(7), Dec. 23, 2022, 136 Stat. 3663.)

Editorial Notes

CODIFICATION

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

AMENDMENTS

2022—Pub. L. 117–263 substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Director of Cybersecurity and Infrastructure Security”.

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”.

Statutory Notes and Related Subsidiaries

RULE 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.

§ 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.)

Editorial Notes

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.)

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 defined 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 tech-

nology 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 be-

fore 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 pursuant 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 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),

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

(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 pre-

viously 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 (I). Pub. L. 114–113, §203(5), added subsecs. (g) to (I).

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, incidents, and ransomware 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 territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(F) set short-term and long-term goals that will improve 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; and

(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

(3) Considerations

In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, shall consider—

(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems owned or operated by State, local, Tribal, and territorial governments; and

(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies.

(4) Exemption

Chapter 35 of title 44 (commonly known as the “Paperwork Reduction Act”) shall not

apply to any action to implement this subsection.

(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; Pub. L. 117–81, div. A, title XV, §§ 1545, 1546, Dec. 27, 2021, 135 Stat. 2057, 2059; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(E), (c)(8), Dec. 23, 2022, 136 Stat. 3660, 3663.)

Editorial Notes

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

2022—Subsec. (a). Pub. L. 117–263, § 7143(b)(2)(E)(i), substituted “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,” for “section—” and struck out pars. (1) to (4) which defined agency information system, cybersecurity risk, information system, intelligence community, and national security system.

Subsec. (c). Pub. L. 117–263, § 7143(c)(8), substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Director of Cybersecurity and Infrastructure Security”.

Pub. L. 117–263, § 7143(b)(2)(E)(ii), substituted “Information Sharing and Analysis Organizations” for “information sharing and analysis organizations (as defined in section 671(5) of this title)” and struck out “(as defined in section 659 of this title)” after “cybersecurity risks”.

Subsec. (e)(1)(B). Pub. L. 117–263, § 7143(b)(2)(E)(iii)(I), which directed striking out “(as such term is defined in section 659 of this title)”, was executed by striking out “(as such term is defined in section 659 of this title)” after “cybersecurity risks” and after “incidents”, to reflect the probable intent of Congress.

Subsec. (e)(3)(C). Pub. L. 117–263, § 7143(b)(2)(E)(iii)(II), struck out “(as such term is defined in section 1501 of this title)” after “information systems”.

2021—Subsec. (c). Pub. L. 117–81, § 1546, substituted “update not less often than biennially” for “regularly update” and inserted “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.” at end.

Subsec. (e). Pub. L. 117–81, § 1545, added subsec. (e).

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).

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. 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.

(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; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(F), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

CODIFICATION

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

AMENDMENTS

2022—Subsec. (h). Pub. L. 117–263 struck out subsec. (h). Text read as follows: “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.”

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 Analysis Organizations, 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; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(G), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

REFERENCES IN TEXT

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

CODIFICATION

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

AMENDMENTS

2022—Pub. L. 117–263 substituted “Information Sharing and Analysis Organizations” for “information sharing and analysis organizations (as defined in section 671(5) of this title)”.

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

(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

¹ So in original. Probably should be “51609”.

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 spe-

cific 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; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(H), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

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

2022—Subsec. (a)(4). Pub. L. 117–263 struck out par. (4) which read as follows: “the terms ‘cybersecurity risk’ and ‘information system’ have the meanings given those terms in section 659 of this title.”

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”.

Statutory Notes and Related Subsidiaries

COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES

Pub. L. 117–81, div. A, title XV, §1544, Dec. 27, 2021, 135 Stat. 2057, provided that: “The Under Secretary for

Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002 [6 U.S.C. 659]) to information systems (as such term is defined in such section 2209) and industrial control systems, including supervisory control and data acquisition systems.”

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 ([former] 5 U.S.C. App.) [see 5 U.S.C. 1001 et seq.] 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 sys-

terms 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 Risk Management 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 se-

curity 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; Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(E), Jan. 1, 2021, 134 Stat. 4773.)

Editorial Notes

CODIFICATION

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

AMENDMENTS

2021—Subsec. (c)(4). Pub. L. 116–283 substituted “Sector Risk Management Agency” for “sector-specific agency”.

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.”

§ 665. Duties and authorities relating to .gov internet domain

(a) Definition

In this section, the term “agency” has the meaning given the term in section 3502 of title 44.

(b) Availability of .gov internet domain

The Director shall make .gov internet domain name registration services, as well as any supporting services described in subsection (e), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (c);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (c); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(c) Requirements

The Director, with the approval of the Director of the Office of Management and Budget for agency .gov internet domain requirements and in consultation with the Director of the Office of Management and Budget for .gov internet domain requirements for entities that are not agencies, shall establish and publish on a publicly available website requirements for the registration and operation of .gov internet domains sufficient to—

(1) minimize the risk of .gov internet domains whose names could mislead or confuse users;

(2) establish that .gov internet domains may not be used for commercial or political campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the .gov internet domain with any other Department component or any other agency for any purpose other than the administration of the .gov internet domain, the services described in subsection (e), and the requirements for establishing a .gov inventory described in subsection (h).

(d) Executive branch

(1) In general

The Director of the Office of Management and Budget shall establish applicable processes and guidelines for the registration and acceptable use of .gov internet domains by agencies.

(2) Approval required

The Director shall obtain the approval of the Director of the Office of Management and Budget before registering a .gov internet domain name for an agency.

(3) Compliance

Each agency shall ensure that any website or digital service of the agency that uses a .gov internet domain is in compliance with the 21st Century IDEA Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

(e) Supporting services

(1) In general

The Director may provide services to the entities described in subsection (b)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered .gov internet domains.

(2) Rule of construction

Nothing in paragraph (1) shall be construed to—

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (b)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of .gov internet domains and the needs of .gov internet domain registrants.

(f) Fees

(1) In general

The Director may provide any service relating to the availability of the .gov internet domain program, including .gov internet domain name registration services described in subsection (b) and supporting services described in subsection (e), to entities described in subsection (b)(1) with or without reimbursement, including variable pricing.

(2) Limitation

The total fees collected for new .gov internet domain registrants or annual renewals of .gov

internet domains shall not exceed the direct operational expenses of improving, maintaining, and operating the .gov internet domain, .gov internet domain services, and .gov internet domain supporting services.

(g) Consultation

The Director shall consult with the Director of the Office of Management and Budget, the Administrator of General Services, other civilian Federal agencies as appropriate, and entities representing State, local, Tribal, or territorial governments in developing the strategic direction of the .gov internet domain and in establishing requirements under subsection (c), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(h) .gov inventory

(1) In general

The Director shall, on a continuous basis—

(A) inventory all hostnames and services in active use within the .gov internet domain; and

(B) provide the data described in subparagraph (A) to domain registrants at no cost.

(2) Requirements

In carrying out paragraph (1)—

(A) data may be collected through analysis of public and non-public sources, including commercial data sets;

(B) the Director shall share with Federal and non-Federal domain registrants all unique hostnames and services discovered within the zone of their registered domain;

(C) the Director shall share any data or information collected or used in the management of the .gov internet domain name registration services relating to Federal executive branch registrants with the Director of the Office of Management and Budget for the purpose of fulfilling the duties of the Director of the Office of Management and Budget under section 3553 of title 44;

(D) the Director shall publish on a publicly available website discovered hostnames that describe publicly accessible agency websites, to the extent consistent with the security of Federal information systems but with the presumption of disclosure;

(E) the Director may publish on a publicly available website any analysis conducted and data collected relating to compliance with Federal mandates and industry best practices, to the extent consistent with the security of Federal information systems but with the presumption of disclosure; and

(F) the Director shall—

(i) collect information on the use of non-.gov internet domain suffixes by agencies for their official online services;

(ii) collect information on the use of non-.gov internet domain suffixes by State, local, Tribal, and territorial governments; and

(iii) publish the information collected under clause (i) on a publicly available website to the extent consistent with the security of the Federal information systems, but with the presumption of disclosure.

(3) National security coordination

(A) In general

In carrying out this subsection, the Director shall inventory, collect, and publish hostnames and services in a manner consistent with the protection of national security information.

(B) Limitation

The Director may not inventory, collect, or publish hostnames or services under this subsection if the Director, in coordination with other heads of agencies, as appropriate, determines that the collection or publication would—

(i) disrupt a law enforcement investigation;

(ii) endanger national security or intelligence activities;

(iii) impede national defense activities or military operations; or

(iv) hamper security remediation actions.

(4) Strategy

Not later than 180 days after December 27, 2020, the Director shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives a strategy to utilize the information collected under this subsection for countering malicious cyber activity.

(Pub. L. 107-296, title XXII, § 2215, as added Pub. L. 116-260, div. U, title IX, § 904(b)(1)(B), Dec. 27, 2020, 134 Stat. 2298; Pub. L. 117-81, div. A, title XV, § 1547(b)(1)(A)(ii), (B), Dec. 27, 2021, 135 Stat. 2060, 2061; Pub. L. 117-263, div. G, title LXXI, § 7143(a)(1), Dec. 23, 2022, 136 Stat. 3654.)

Editorial Notes

REFERENCES IN TEXT

The 21st Century IDEA Act, referred to in subsec. (d)(3), is Pub. L. 115-336, Dec. 20, 2018, 132 Stat. 5025, also known as the 21st Century Integrated Digital Experience Act, which is set out as a note under section 3501 of Title 44, Public Printing and Documents.

CODIFICATION

Other sections 2215 of Pub. L. 107-296 were renumbered sections 2216, 2217, and 2218 and are classified, respectively, to sections 665b, 665c, and 665d of this title.

AMENDMENTS

2022—Pub. L. 117-263 made amendment identical to that made by Pub. L. 117-81, § 1547(b)(1)(B). See 2021 Amendment note below.

2021—Pub. L. 117-81, § 1547(b)(1)(B), made technical amendment to the directory language of section 904(b)(1) of Pub. L. 116-260.

Pub. L. 117-81, § 1547(b)(1)(A)(ii), reenacted section catchline.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2022 AMENDMENT

Amendment by Pub. L. 117-263 effective as if enacted as part of title IX of div. U of Pub. L. 116-260, see sec-

tion 7143(a)(2) of Pub. L. 117-263, set out as a note under section 652 of this title.

FINDINGS

Pub. L. 116-260, div. U, title IX, §902, Dec. 27, 2020, 134 Stat. 2297, provided that: “Congress finds that—

“(1) the .gov internet domain reflects the work of United States innovators in inventing the internet and the role that the Federal Government played in guiding the development and success of the early internet;

“(2) the .gov internet domain is a unique resource of the United States that reflects the history of innovation and global leadership of the United States;

“(3) when online public services and official communications from any level and branch of government use the .gov internet domain, they are easily recognized as official and difficult to impersonate;

“(4) the citizens of the United States deserve online public services that are safe, recognizable, and trustworthy;

“(5) the .gov internet domain should be available at no cost or a negligible cost to any Federal, State, local, or territorial government-operated or publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, for use in their official services, operations, and communications;

“(6) the .gov internet domain provides a critical service to those Federal, State, local, Tribal, and territorial governments; and

“(7) the .gov internet domain should be operated transparently and in the spirit of public accessibility, privacy, and security.”

[For definition of “State” as used in section 902 of Pub. L. 116-260, set out above, see section 903 of Pub. L. 116-260, set out as a note below.]

PURPOSE OF .gov INTERNET DOMAIN PROGRAM

Pub. L. 116-260, div. U, title IX, §904(a), Dec. 27, 2020, 134 Stat. 2298, provided that: “The purpose of the .gov internet domain program is to—

“(1) legitimize and enhance public trust in government entities and their online services;

“(2) facilitate trusted electronic communication and connections to and from government entities;

“(3) provide simple and secure registration of .gov internet domains;

“(4) improve the security of the services hosted within these .gov internet domains, and of the .gov namespace in general; and

“(5) enable the discoverability of government services to the public and to domain registrants.”

[For definition of “online service” as used in section 904(a) of Pub. L. 116-260, set out above, see section 903 of Pub. L. 116-260, set out as a note below.]

REFERENCE GUIDE

Pub. L. 116-260, div. U, title IX, §904(b)(2)(B), Dec. 27, 2020, 134 Stat. 2301, provided that: “Not later than 1 year after the date of enactment of this Act [Dec. 27, 2020], the Director, in consultation with the Administrator and entities representing State, local, Tribal, or territorial governments, shall develop and publish on a publicly available website a reference guide for migrating online services to the .gov internet domain, which shall include—

“(i) process and technical information on how to carry out a migration of common categories of online services, such as web and email services;

“(ii) best practices for cybersecurity pertaining to registration and operation of a .gov internet domain; and

“(iii) references to contract vehicles and other private sector resources vetted by the Director that may assist in performing the migration.”

[For definitions of terms used in section 904(b)(2)(B) of Pub. L. 116-260, set out above, see section 903 of Pub. L. 116-260, set out as a note below.]

TRANSITION

Pub. L. 116-260, div. U, title IX, §907, Dec. 27, 2020, 134 Stat. 2303, provided that:

“(a) There shall be transferred to the Director the .gov internet domain program, as operated by the General Services Administration under title 41, Code of Federal Regulations, on the date on which the Director begins operational administration of the .gov internet domain program, in accordance with subsection (c).

“(b) Not later than 30 days after the date of enactment of this Act [probably means “this title”, approved Dec. 27, 2020], the Director shall submit a plan for the operational and contractual transition of the .gov internet domain program to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives.

“(c) Not later than 120 days after the date of enactment of this Act, the Director shall begin operationally administering the .gov internet domain program, and shall publish on a publicly available website the requirements for domain registrants as described in section 2215(b) of the Homeland Security Act of 2002 [6 U.S.C. 665(b)], as added by section 904(b) of this Act.

“(d) On the date on which the Director begins operational administration of the .gov internet domain program, in accordance with subsection (c), the Administrator shall rescind the requirements in part 102-173 of title 41, Code of Federal Regulations.

“(e) During the 5-year period beginning on the date of enactment of this Act [Dec. 27, 2020], any fee charged to entities that are not agencies for new .gov internet domain registrants or annual renewals of .gov internet domains shall be not more than the amount of the fee charged for such registration or renewal as of October 1, 2019.”

[For definition of “Director” as used in section 907 of Pub. L. 116-260, set out above, see section 903 of Pub. L. 116-260, set out as a note below.]

DEFINITIONS

Pub. L. 116-260, div. U, title IX, §903, Dec. 27, 2020, 134 Stat. 2298, provided that: “In this Act [probably means “this title”, see Short Title of 2020 Amendment note set out under section 101 of this title]—

“(1) the term ‘Administrator’ means the Administrator of General Services;

“(2) the term ‘agency’ has the meaning given the term in section 3502 of title 44, United States Code;

“(3) the term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency;

“(4) the term ‘online service’ means any internet-facing service, including a website, email, a virtual private network, or a custom application; and

“(5) the term ‘State’ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.”

§ 665a. Intelligence and cybersecurity diversity fellowship program

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term “appropriate committees of Congress” means—

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

(B) the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) Excepted service

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

(3) Historically Black college or university

The term “historically Black college or university” has the meaning given the term “part B institution” in section 1061 of title 20.

(4) Institution of higher education

The term “institution of higher education” has the meaning given that term in section 1001 of title 20.

(5) Minority-serving institution

The term “minority-serving institution” means an institution of higher education described in section 1067q(a) of title 20.

(b) Program

The Secretary shall carry out an intelligence and cybersecurity diversity fellowship program (in this section referred to as the “Program”) under which an eligible individual may—

(1) participate in a paid internship at the Department that relates to intelligence, cybersecurity, or some combination thereof;

(2) receive tuition assistance from the Secretary; and

(3) upon graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), receive an offer of employment to work in an intelligence or cybersecurity position of the Department that is in the excepted service.

(c) Eligibility

To be eligible to participate in the Program, an individual shall—

(1) be a citizen of the United States; and

(2) as of the date of submitting the application to participate in the Program—

(A) have a cumulative grade point average of at least 3.2 on a 4.0 scale;

(B) be a socially disadvantaged individual (as that term in¹ defined in section 124.103 of title 13, Code of Federal Regulations, or successor regulation); and

(C) be a sophomore, junior, or senior at an institution of higher education.

(d) Direct hire authority

If an individual who receives an offer of employment under subsection (b)(3) accepts such offer, the Secretary shall appoint, without regard to provisions of subchapter I of chapter 33 of title 5 (except for section 3328 of such title) such individual to the position specified in such offer.

(e) Reports**(1) Reports**

Not later than 1 year after December 27, 2020, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program.

(2) Matters

Each report under paragraph (1) shall include, with respect to the most recent year, the following:

(A) A description of outreach efforts by the Secretary to raise awareness of the Program among institutions of higher education in which eligible individuals are enrolled.

(B) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(C) The number of individuals participating in the Program, listed by the institution of higher education in which the individual is enrolled at the time of participation, and information on the nature of such participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(D) The number of individuals who accepted an offer of employment under the Program and an identification of the element within the Department to which each individual was appointed.

(Pub. L. 107-296, title XIII, §1333, as added Pub. L. 116-260, div. W, title IV, §404(a), Dec. 27, 2020, 134 Stat. 2378.)

Editorial Notes**CODIFICATION**

Section was enacted as part of title XIII of Pub. L. 107-296, and not as part of title XXII of 107-296 which comprises this subchapter.

§ 665b. Joint cyber planning office**(a) Establishment of Office**

There is established in the Agency an office for joint cyber planning (in this section referred to as the “Office”) to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) Planning and execution

In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

(1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;

(2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;

(3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(4) ensure that plans for cyber defense operations, as appropriate, are responsive to po-

¹ So in original. Probably should be “is”.

tential adversary activity conducted in response to United States offensive cyber operations;

(5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

(7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) Composition

The Office shall be composed of—

- (1) a central planning staff; and
- (2) appropriate representatives of Federal departments and agencies, including—
 - (A) the Department;
 - (B) United States Cyber Command;
 - (C) the National Security Agency;
 - (D) the Federal Bureau of Investigation;
 - (E) the Department of Justice; and
 - (F) the Office of the Director of National Intelligence.

(d) Consultation

In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

- (1) State, local, federally-recognized Tribal, and territorial governments;
- (2) Information Sharing and Analysis Organizations, including information sharing and analysis centers;
- (3) owners and operators of critical information systems;
- (4) private entities; and
- (5) other appropriate representatives or entities, as determined by the Secretary.

(e) Interagency agreements

The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) Definitions

In this section, the term “cyber defense operation” means the defensive activities performed for a cybersecurity purpose.

(Pub. L. 107–296, title XXII, § 2216, formerly § 2215, as added Pub. L. 116–283, div. A, title XVII, § 1715(a), Jan. 1, 2021, 134 Stat. 4092; renumbered § 2216 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(iii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(I), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2216 of Pub. L. 107–296 was renumbered section 2219 and is classified to section 665e of this title.

AMENDMENTS

2022—Subsec. (d)(2). Pub. L. 117–263, § 7143(b)(2)(I)(i), substituted “Information Sharing and Analysis Organizations” for “information sharing and analysis organizations”.

Subsec. (f). Pub. L. 117–263, § 7143(b)(2)(I)(ii), substituted “section, the term ‘cyber defense operation’ means the defensive activities performed for a cybersecurity purpose.” for “section:” and struck out pars. (1) to (4) which defined cyber defense operation, cybersecurity purpose, cybersecurity risk, incident, and information sharing and analysis organization.

2021—Pub. L. 117–81 reenacted section catchline.

§ 665c. Cybersecurity State Coordinator

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in

the United States and reducing the impact of cyber threats to non-Federal entities.

(c) Feedback

The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(Pub. L. 107–296, title XXII, § 2217, formerly § 2215, as added Pub. L. 116–283, div. A, title XVII, § 1717(a)(1)(B), Jan. 1, 2021, 134 Stat. 4099; renumbered § 2217 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(iv), Dec. 27, 2021, 135 Stat. 2061.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2217 of Pub. L. 107–296 was renumbered section 2220 and is classified to section 665f of this title.

AMENDMENTS

2021—Pub. L. 117–81 reenacted section catchline.

Statutory Notes and Related Subsidiaries

RULE OF CONSTRUCTION

Pub. L. 116–283, div. A, title XVII, § 1717(a)(4), Jan. 1, 2021, 134 Stat. 4100, provided that: “Nothing in this subsection [enacting this section, amending section 652 of this title, and enacting provisions set out as a note below] or the amendments made by this subsection may be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents.”

COORDINATION PLAN

Pub. L. 116–283, div. A, title XVII, § 1717(a)(2), Jan. 1, 2021, 134 Stat. 4100, provided that: “Not later than 60 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall establish and submit to the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security in the House of Representatives a plan describing the reporting structure and coordination processes and procedures of Cybersecurity State Coordinators within the Cybersecurity and Infrastructure Security Agency under section 2215 of the Homeland Security Act of 2002 [Pub. L. 107–296], as added by paragraph (1)(B) [6 U.S.C. 665c].”

§ 665d. Sector Risk Management Agencies

(a) In general

Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

- (1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and
- (2) support programs and associated activities of such sector or subsector of such sector.

(b) Implementation

In carrying out this section, Sector Risk Management Agencies shall—

- (1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

- (2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

- (3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(c) Responsibilities

Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of such sector and authorities under applicable law to—

- (1) support sector risk management, in coordination with the Director, including—

- (A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

- (B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

- (2) assess sector risk, in coordination with the Director, including—

- (A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

- (B) supporting national risk assessment efforts led by the Department;

- (3) sector coordination, including—

- (A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

- (B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

- (C) participating in cross-sector coordinating councils, as appropriate;

- (4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

- (A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through Information Sharing and Analysis Organizations and the national cybersecurity and communications integration center established pursuant to section 659 of this title;

- (B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(5) supporting incident management, including—

(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

(6) contributing to emergency preparedness efforts, including—

(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

(B) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and

(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.

(Pub. L. 107–296, title XXII, § 2218, formerly § 2215, as added Pub. L. 116–283, div. H, title XC, § 9002(c)(1), Jan. 1, 2021, 134 Stat. 4770; renumbered § 2218 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(v), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(J), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2218 of Pub. L. 107–296 was renumbered section 2220A and is classified to section 665g of this title.

AMENDMENTS

2022—Subsec. (c)(4)(A). Pub. L. 117–263 substituted “Information Sharing and Analysis Organizations” for “information sharing and analysis organizations”.

2021—Pub. L. 117–81 reenacted section catchline.

§ 665e. Cybersecurity Advisory Committee

(a) Establishment

The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the “Advisory Committee”).

(b) Duties

(1) In general

The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) Recommendations

(A) In general

The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) Recommendations of subcommittees

Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) Periodic reports

The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) Annual report

(A) In general

The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) Publication

Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5.

(5) Feedback

Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) Congressional notification

Not less frequently than once per year after January 1, 2021, the Director shall provide to

the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) Governance rules

The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) Membership

(1) Appointment

(A) In general

Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020,¹ the Director shall appoint the members of the Advisory Committee.

(B) Composition

The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) Representation

(i) In general

The membership of the Advisory Committee shall satisfy the following criteria:

- (I) Consist of subject matter experts.
- (II) Be geographically balanced.
- (III) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:
 - (aa) Defense.
 - (bb) Education.
 - (cc) Financial services and insurance.
 - (dd) Healthcare.
 - (ee) Manufacturing.
 - (ff) Media and entertainment.
 - (gg) Chemicals.
 - (hh) Retail.
 - (ii) Transportation.
 - (jj) Energy.
 - (kk) Information Technology.
 - (ll) Communications.
 - (mm) Other relevant fields identified by the Director.

(ii) Prohibition

Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) Publication of membership list

The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) Term of office

(A) Terms

The term of each member of the Advisory Committee shall be two years, except that a

member may continue to serve until a successor is appointed.

(B) Removal

The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

(C) Reappointment

A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) Prohibition on compensation

The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) Meetings

(A) In general

The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) Public meetings

At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) Attendance

The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) Member access to classified information

(A) In general

Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted from reviewing, discussing, or possessing classified information.

(B) Access

Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) Protections

A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) Rule of construction

Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) Chairperson

The Advisory Committee shall select, from among the members of the Advisory Committee—

¹ See References in Text note below.

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) Subcommittees

(1) In general

The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

- (A) Information exchange.
- (B) Critical infrastructure.
- (C) Risk management.
- (D) Public and private partnerships.

(2) Meetings and reporting

Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) Subject matter experts

The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

(Pub. L. 107–296, title XXII, § 2219, formerly § 2216, as added Pub. L. 116–283, div. A, title XVII, § 1718(a), Jan. 1, 2021, 134 Stat. 4102; renumbered § 2219 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(vi), Dec. 27, 2021, 135 Stat. 2061.)

Editorial Notes

REFERENCES IN TEXT

The date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, referred to in subsec. (c)(1)(A), probably means the date of enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116–283, which was approved Jan. 1, 2021. No act named the Cybersecurity Advisory Committee Authorization Act of 2020 has been enacted. However, a bill, S. 4024, entitled “Cybersecurity Advisory Committee Authorization Act of 2020” was introduced to Senate on June 22, 2020.

Executive Order No. 13526, referred to in subsec. (c)(5)(B), is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, set out as a note under section 3161 of Title 50, War and National Defense.

AMENDMENTS

2021—Pub. L. 117–81 reenacted section catchline.

§ 665f. Cybersecurity education and training programs

(a) Establishment

(1) In general

The Cybersecurity Education and Training Assistance Program (referred to in this section as “CETAP”) is established within the Agency.

(2) Purpose

The purpose of CETAP shall be to support the effort of the Agency in building and

strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

- (A) providing foundational cybersecurity awareness and literacy;
- (B) encouraging cybersecurity career exploration; and
- (C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) Requirements

In carrying out CETAP, the Director shall—

- (1) ensure that the program—
 - (A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;
 - (B) conducts professional development sessions for teachers;
 - (C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);
 - (D) provides direct student engagement opportunities through camps and other programming;
 - (E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;
 - (F) integrates with existing post-secondary education and workforce development programs at the Department;
 - (G) promotes and supports national standards for elementary and secondary cyber education;
 - (H) partners with cybersecurity and education stakeholder groups to expand outreach; and
 - (I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and
- (2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) Briefings

(1) In general

Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) Contents

Each briefing conducted under paragraph (1) shall include—

- (A) estimated figures on the number of students reached and teachers engaged;
- (B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);
- (C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to en-

hance cybersecurity education for underserved populations or communities;

(D) information on new curricula offerings and teacher training platforms; and

(E) information on coordination with post-secondary education and workforce development programs at the Department.

(d) Mission promotion

The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

(e) Grants and cooperative agreements

The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 1001 of title 20), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

(1) carry out the purposes of CETAP; and

(2) enhance CETAP to address the national shortfall of cybersecurity professionals.

(Pub. L. 107–296, title XXII, § 2220, formerly § 2217, as added Pub. L. 116–283, div. A, title XVII, § 1719(c), Jan. 1, 2021, 134 Stat. 4106; renumbered § 2220 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(vii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7104, Dec. 23, 2022, 136 Stat. 3622.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c)(2)(C) to (E). Pub. L. 117–263, § 7104(b), added subpar. (C) and redesignated former subpars. (C) and (D) as (D) and (E), respectively.

Subsec. (e). Pub. L. 117–263, § 7104(a), added subsec. (e).
2021—Pub. L. 117–81 reenacted section catchline.

§ 665g. State and Local Cybersecurity Grant Program

(a) Definitions

In this section:

(1) Cybersecurity Plan

The term “Cybersecurity Plan” means a plan submitted by an eligible entity under subsection (e)(1).

(2) Eligible entity

The term “eligible entity” means a—

(A) State; or

(B) Tribal government.

(3) Multi-entity group

The term “multi-entity group” means a group of 2 or more eligible entities desiring a grant under this section.

(4) Online service

The term “online service” means any internet-facing service, including a website, email, virtual private network, or custom application.

(5) Rural area

The term “rural area” has the meaning given the term in section 5302 of title 49.

(6) State and Local Cybersecurity Grant Program

The term “State and Local Cybersecurity Grant Program” means the program established under subsection (b).

(7) Tribal government

The term “Tribal government” means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 5131 of title 25.

(b) Establishment

(1) In general

There is established within the Department a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments.

(2) Application

An eligible entity desiring a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(c) Administration

The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 604 and 605 of this title.

(d) Use of funds

An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate, shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity;

(3) pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;

(4) assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or

(5) fund any other appropriate activity determined by the Secretary, acting through the Director.

(e) Cybersecurity plans

(1) In general

An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for review in accordance with subsection (i).

(2) Required elements

A Cybersecurity Plan of an eligible entity shall—

(A) incorporate, to the extent practicable—

(i) any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments; and

(ii) if the eligible entity is a State, consultation and feedback from local governments and associations of local governments within the jurisdiction of the eligible entity;

(B) describe, to the extent practicable, how the eligible entity will—

(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

(ii) monitor, audit, and,¹ track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(iii) enhance the preparation, response, and resiliency of information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, against cybersecurity risks and cybersecurity threats;

(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(v) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, such as—

(I) the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

(II) cyber chain supply chain risk management best practices identified by the

National Institute of Standards and Technology; and

(III) knowledge bases of adversary tools and tactics;

(vi) promote the delivery of safe, recognizable, and trustworthy online services by the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including through the use of the .gov internet domain;

(vii) ensure continuity of operations of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident;

(viii) use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

(ix) if the eligible entity is a State, ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local governments within the jurisdiction of the eligible entity in the event of an incident involving those communications or data networks;

(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and—

(I) if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including by expanding information sharing agreements with the Department; and

(II) the Department;

(xii) leverage cybersecurity services offered by the Department;

(xiii) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(xiv) develop and coordinate strategies to address cybersecurity risks and

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

cybersecurity threats in consultation with—

(I) if the eligible entity is a State, local governments and associations of local governments within the jurisdiction of the eligible entity; and

(II) as applicable—

(aa) eligible entities that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an Information Sharing and Analysis Organization; and

(bb) countries that neighbor the jurisdiction of the eligible entity;

(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the jurisdiction of the eligible entity; and

(xvi) distribute funds, items, services, capabilities, or activities to local governments under subsection (n)(2)(A), including the fraction of that distribution the eligible entity plans to distribute to rural areas under subsection (n)(2)(B);

(C) assess the capabilities of the eligible entity relating to the actions described in subparagraph (B);

(D) describe, as appropriate and to the extent practicable, the individual responsibilities of the eligible entity and local governments within the jurisdiction of the eligible entity in implementing the plan;

(E) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(F) describe the metrics the eligible entity will use to measure progress towards—

(i) implementing the plan; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(3) Discretionary elements

In drafting a Cybersecurity Plan, an eligible entity may—

(A) consult with the Multi-State Information Sharing and Analysis Center;

(B) include a description of cooperative programs developed by groups of local governments within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

(C) include a description of programs provided by the eligible entity to support local governments and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

(f) Multi-entity grants

(1) In general

The Secretary may award grants under this section to a multi-entity group to support multi-entity efforts to address cybersecurity risks and cybersecurity threats to information

systems within the jurisdictions of the eligible entities that comprise the multi-entity group.

(2) Satisfaction of other requirements

In order to be eligible for a multi-entity grant under this subsection, each eligible entity that comprises a multi-entity group shall have—

(A) a Cybersecurity Plan that has been reviewed by the Secretary in accordance with subsection (i); and

(B) a cybersecurity planning committee established in accordance with subsection (g).

(3) Application

(A) In general

A multi-entity group applying for a multi-entity grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) Multi-entity project plan

An application for a grant under this section of a multi-entity group under subparagraph (A) shall include a plan describing—

(i) the division of responsibilities among the eligible entities that comprise the multi-entity group;

(ii) the distribution of funding from the grant among the eligible entities that comprise the multi-entity group; and

(iii) how the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) Planning committees

(1) In general

An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

(A) assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(B) approve the Cybersecurity Plan of the eligible entity; and

(C) assist with the determination of effective funding priorities for a grant under this section in accordance with subsections (d) and (j).

(2) Composition

A committee of an eligible entity established under paragraph (1) shall—

(A) be comprised of representatives from—

(i) the eligible entity;

(ii) if the eligible entity is a State, counties, cities, and towns within the jurisdiction of the eligible entity; and

(iii) institutions of public education and health within the jurisdiction of the eligible entity; and

(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(3) Cybersecurity expertise

Not less than one-half of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

(4) Rule of construction regarding existing planning committees

Nothing in this subsection shall be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that—

(A) meets the requirements of this subsection; or

(B) may be expanded or leveraged to meet the requirements of this subsection, including through the formation of a cybersecurity planning subcommittee.

(5) Rule of construction regarding control of information systems of eligible entities

Nothing in this subsection shall be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems owned or operated by, or on behalf of, the eligible entity.

(h) Special rule for Tribal governments

With respect to any requirement under subsection (e) or (g), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe an alternative substantively similar requirement for Tribal governments if the Secretary finds that the alternative requirement is necessary for the effective delivery and administration of grants to Tribal governments under this section.

(i) Review of plans

(1) Review as condition of grant

(A) In general

Subject to paragraph (3), before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall—

(i) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and

(ii) determine that the Cybersecurity Plan reviewed under clause (i) satisfies the requirements under paragraph (2).

(B) Duration of determination

In the case of a determination under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the 2-year period beginning on the date of the determination.

(C) Annual renewal

Not later than 2 years after the date on which the Secretary determines under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), and annually thereafter, the Secretary, acting through the Director, shall—

(i) determine whether the Cybersecurity Plan and any revisions continue to meet the criteria described in paragraph (2); and

(ii) renew the determination if the Secretary, acting through the Director, makes a positive determination under clause (i).

(2) Plan requirements

In reviewing a Cybersecurity Plan of an eligible entity under this subsection, the Secretary, acting through the Director, shall ensure that the Cybersecurity Plan—

(A) satisfies the requirements of subsection (e)(2); and

(B) has been approved by—

(i) the cybersecurity planning committee of the eligible entity established under subsection (g); and

(ii) the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity.

(3) Exception

Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary for review before September 30, 2023, if the eligible entity certifies to the Secretary that—

(A) the activities that will be supported by the grant are—

(i) integral to the development of the Cybersecurity Plan of the eligible entity; or

(ii) necessary to assist with activities described in subsection (d)(4), as confirmed by the Director; and

(B) the eligible entity will submit to the Secretary a Cybersecurity Plan for review under this subsection by September 30, 2023.

(4) Rule of construction

Nothing in this subsection shall be construed to provide authority to the Secretary to—

(A) regulate the manner by which an eligible entity or local government improves the cybersecurity of the information systems owned or operated by, or on behalf of, the eligible entity or local government; or

(B) condition the receipt of grants under this section on—

(i) participation in a particular Federal program; or

(ii) the use of a specific product or technology.

(j) Limitations on uses of funds

(1) In general

Any entity that receives funds from a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any recipient cost-sharing contribution;

(C) to pay a ransom;

(D) for recreational or social purposes; or

(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

(2) Compliance oversight

In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant

under this section uses the grant for the purposes for which the grant is awarded.

(3) Rule of construction

Nothing in paragraph (1)(A) shall be construed to prohibit the use of funds from a grant under this section awarded to a State, local, or Tribal government for otherwise permissible uses under this section on the basis that the State, local, or Tribal government has previously used State, local, or Tribal funds to support the same or similar uses.

(k) Opportunity to amend applications

In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct any defects in those applications before making final awards, including by allowing applicants to revise a submitted Cybersecurity Plan.

(l) Apportionment

For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among eligible entities as follows:

(1) Baseline amount

The Secretary shall first apportion—

(A) 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands;

(B) 1 percent of such amounts to each of the remaining States; and

(C) 3 percent of such amounts to Tribal governments.

(2) Remainder

The Secretary shall apportion the remainder of such amounts to States as follows:

(A) 50 percent of such remainder in the ratio that the population of each State, bears to the population of all States; and

(B) 50 percent of such remainder in the ratio that the population of each State that resides in rural areas, bears to the population of all States that resides in rural areas.

(3) Apportionment among Tribal governments

In determining how to apportion amounts to Tribal governments under paragraph (1)(C), the Secretary shall consult with the Secretary of the Interior and Tribal governments.

(4) Multi-entity grants

An amount received from a multi-entity grant awarded under subsection (f)(1) by a State or Tribal government that is a member of the multi-entity group shall qualify as an apportionment for the purpose of this subsection.

(m) Federal share

(1) In general

The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

(A) in the case of a grant to an eligible entity—

(i) for fiscal year 2022, 90 percent;

(ii) for fiscal year 2023, 80 percent;

(iii) for fiscal year 2024, 70 percent; and

(iv) for fiscal year 2025, 60 percent; and

(B) in the case of a grant to a multi-entity group—

(i) for fiscal year 2022, 100 percent;

(ii) for fiscal year 2023, 90 percent;

(iii) for fiscal year 2024, 80 percent; and

(iv) for fiscal year 2025, 70 percent.

(2) Waiver

(A) In general

The Secretary may waive or modify the requirements of paragraph (1) if an eligible entity or multi-entity group demonstrates economic hardship.

(B) Guidelines

The Secretary shall establish and publish guidelines for determining what constitutes economic hardship for the purposes of this subsection.

(C) Considerations

In developing guidelines under subparagraph (B), the Secretary shall consider, with respect to the jurisdiction of an eligible entity—

(i) changes in rates of unemployment in the jurisdiction from previous years;

(ii) changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) from previous years; and

(iii) any other factors the Secretary considers appropriate.

(3) Waiver for Tribal governments

Notwithstanding paragraph (2), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may waive or modify the requirements of paragraph (1) for 1 or more Tribal governments if the Secretary determines that the waiver is in the public interest.

(n) Responsibilities of grantees

(1) Certification

Each eligible entity or multi-entity group that receives a grant under this section shall certify to the Secretary that the grant will be used—

(A) for the purpose for which the grant is awarded; and

(B) in compliance with subsections (d) and (j).

(2) Availability of funds to local governments and rural areas

(A) In general

Subject to subparagraph (C), not later than 45 days after the date on which an eligible entity or multi-entity group receives a grant under this section, the eligible entity or multi-entity group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local governments within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group, consistent

with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multi-entity group—

- (i) not less than 80 percent of funds available under the grant;
- (ii) with the consent of the local governments, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or
- (iii) with the consent of the local governments, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

(B) Availability to rural areas

In obligating funds, items, services, capabilities, or activities to local governments under subparagraph (A), the eligible entity or eligible entities that comprise the multi-entity group shall ensure that rural areas within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group receive not less than—

- (i) 25 percent of the amount of the grant awarded to the eligible entity;
- (ii) items, services, capabilities, or activities having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or
- (iii) grant funds combined with other items, services, capabilities, or activities having the total value of not less than 25 percent of the grant awarded to the eligible entity.

(C) Exceptions

This paragraph shall not apply to—

- (i) any grant awarded under this section that solely supports activities that are integral to the development or revision of the Cybersecurity Plan of the eligible entity; or
- (ii) the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

(3) Certifications regarding distribution of grant funds to local governments

An eligible entity or multi-entity group shall certify to the Secretary that the eligible entity or multi-entity group has made the distribution to local governments required under paragraph (2).

(4) Extension of period

(A) In general

An eligible entity or multi-entity group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

(B) Approval

The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the pur-

pose of the State and Local Cybersecurity Grant Program.

(5) Direct funding

If an eligible entity does not make a distribution to a local government required under paragraph (2) in a timely fashion, the local government may petition the Secretary to request the Secretary to provide funds directly to the local government.

(6) Limitation on construction

A grant awarded under this section may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities.

(7) Consultation in allocating funds

An eligible entity applying for a grant under this section shall agree to consult the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity in allocating funds from a grant awarded under this section.

(8) Penalties

In addition to other remedies available to the Secretary, if an eligible entity violates a requirement of this subsection, the Secretary may—

- (A) terminate or reduce the amount of a grant awarded under this section to the eligible entity; or
- (B) distribute grant funds previously awarded to the eligible entity—
 - (i) in the case of an eligible entity that is a State, directly to the appropriate local government as a replacement grant in an amount determined by the Secretary; or
 - (ii) in the case of an eligible entity that is a Tribal government, to another Tribal government or Tribal governments as a replacement grant in an amount determined by the Secretary.

(o) Consultation with State, local, and Tribal representatives

In carrying out this section, the Secretary shall consult with State, local, and Tribal representatives with professional experience relating to cybersecurity, including representatives of associations representing State, local, and Tribal governments, to inform—

- (1) guidance for applicants for grants under this section, including guidance for Cybersecurity Plans;
- (2) the study of risk-based formulas required under subsection (q)(4);
- (3) the development of guidelines required under subsection (m)(2)(B); and
- (4) any modifications described in subsection (q)(2)(D).

(p) Notification to Congress

Not later than 3 business days before the date on which the Department announces the award of a grant to an eligible entity under this section, including an announcement to the eligible entity, the Secretary shall provide to the appropriate congressional committees notice of the announcement.

(q) Reports, study, and review**(1) Annual reports by grant recipients****(A) In general**

Not later than 1 year after the date on which an eligible entity receives a grant under this section for the purpose of implementing the Cybersecurity Plan of the eligible entity, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in—

- (i) implementing the Cybersecurity Plan of the eligible entity; and
- (ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(B) Absence of plan

Not later than 1 year after the date on which an eligible entity that does not have a Cybersecurity Plan receives funds under this section, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to—

- (i) develop or revise a Cybersecurity Plan; or
- (ii) assist with the activities described in subsection (d)(4).

(2) Annual reports to Congress

Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

- (A) the use of grants awarded under this section;
- (B) the proportion of grants used to support cybersecurity in rural areas;
- (C) the effectiveness of the State and Local Cybersecurity Grant Program;
- (D) any necessary modifications to the State and Local Cybersecurity Grant Program; and
- (E) any progress made toward—
 - (i) developing, implementing, or revising Cybersecurity Plans; and
 - (ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, State, local, or Tribal governments as a result of the award of grants under this section.

(3) Public availability**(A) In general**

The Secretary, acting through the Director, shall make each report submitted under paragraph (2) publicly available, including

by making each report available on the website of the Agency.

(B) Redactions

In making each report publicly available under subparagraph (A), the Director may make redactions that the Director, in consultation with each eligible entity, determines necessary to protect classified or other information exempt from disclosure under section 552 of title 5 (commonly referred to as the “Freedom of Information Act”).

(4) Study of risk-based formulas**(A) In general**

Not later than September 30, 2024, the Secretary, acting through the Director, shall submit to the appropriate congressional committees a study and legislative recommendations on the potential use of a risk-based formula for apportioning funds under this section, including—

- (i) potential components that could be included in a risk-based formula, including the potential impact of those components on support for rural areas under this section;
- (ii) potential sources of data and information necessary for the implementation of a risk-based formula;
- (iii) any obstacles to implementing a risk-based formula, including obstacles that require a legislative solution;
- (iv) if a risk-based formula were to be implemented for fiscal year 2026, a recommended risk-based formula for the State and Local Cybersecurity Grant Program; and
- (v) any other information that the Secretary, acting through the Director, determines necessary to help Congress understand the progress towards, and obstacles to, implementing a risk-based formula.

(B) Inapplicability of Paperwork Reduction Act

The requirements of chapter 35 of title 44 (commonly referred to as the “Paperwork Reduction Act”), shall not apply to any action taken to carry out this paragraph.

(5) Tribal cybersecurity needs report

Not later than 2 years after November 15, 2021, the Secretary, acting through the Director, shall submit to Congress a report that—

- (A) describes the cybersecurity needs of Tribal governments, which shall be determined in consultation with the Secretary of the Interior and Tribal governments; and
- (B) includes any recommendations for addressing the cybersecurity needs of Tribal governments, including any necessary modifications to the State and Local Cybersecurity Grant Program to better serve Tribal governments.

(6) GAO review

Not later than 3 years after November 15, 2021, the Comptroller General of the United States shall conduct a review of the State and Local Cybersecurity Grant Program, including—

(A) the grant selection process of the Secretary; and

(B) a sample of grants awarded under this section.

(r) Authorization of appropriations

(1) In general

There are authorized to be appropriated for activities under this section—

(A) for fiscal year 2022, \$200,000,000;

(B) for fiscal year 2023, \$400,000,000;

(C) for fiscal year 2024, \$300,000,000; and

(D) for fiscal year 2025, \$100,000,000.

(2) Transfers authorized

(A) In general

During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to paragraph (1) or other amounts appropriated to carry out the State and Local Cybersecurity Grant Program for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.

(B) Additional appropriations

Any funds transferred under subparagraph (A) shall be in addition to any funds appropriated to the Department or the components described in subparagraph (A) for salaries, expenses, and other administrative costs.

(s) Termination

(1) In general

Subject to paragraph (2), the requirements of this section shall terminate on September 30, 2025.

(2) Exception

The reporting requirements under subsection (q) shall terminate on the date that is 1 year after the date on which the final funds from a grant under this section are expended or returned.

(Pub. L. 107–296, title XXII, § 2220A, formerly § 2218, as added Pub. L. 117–58, div. G, title VI, § 70612(a), Nov. 15, 2021, 135 Stat. 1272; renumbered § 2220A and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(viii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(K), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

REFERENCES IN TEXT

The Food and Nutrition Act of 2008, referred to in subsec. (m)(2)(C)(ii), is Pub. L. 88–525, Aug. 31, 1964, 78 Stat. 703, which is classified generally to chapter 51 (§ 2011 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 7 and Tables.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, § 7143(b)(2)(K)(i), redesignated pars. (3), (4), and (8) to (12) as pars. (1) to (7), respectively, and struck out former pars. (1), (2), and (5)

to (7) which defined appropriate committees of Congress, cyber threat indicator, incident, information sharing and analysis organization, and information system, respectively.

Subsec. (e)(2)(B)(xiv)(II)(aa). Pub. L. 117–263, § 7143(b)(2)(K)(ii), substituted “Information Sharing and Analysis Organization” for “information sharing and analysis organization”.

Subsec. (p). Pub. L. 117–263, § 7143(b)(2)(K)(iii), substituted “appropriate congressional committees” for “appropriate committees of Congress”.

Subsec. (q)(4)(A). Pub. L. 117–263, § 7143(b)(2)(K)(iv), which directed amendment of subsec. (q)(4) by substituting “appropriate congressional committees” for “appropriate committees of Congress” “in the matter preceding clause (i)”, was executed by making the substitution in the introductory provisions of subsec. (q)(4)(A), to reflect the probable intent of Congress.

2021—Pub. L. 117–81 reenacted section catchline.

§ 665h. National Cyber Exercise Program

(a) Establishment of program

(1) In general

There is established in the Agency the National Cyber Exercise Program (referred to in this section as the “Exercise Program”) to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) Requirements

(A) In general

The Exercise Program shall be—

(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(B) Model exercise selection

The Exercise Program shall—

(i) include a selection of model exercises that government and private entities can readily adapt for use; and

(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) Consultation

In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Di-

rector, cybersecurity research stakeholders, and Sector Coordinating Councils.

(b) Definitions

In this section:

(1) State

The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) Private entity

The term “private entity” has the meaning given such term in section 1501 of this title.

(c) Rule of construction

Nothing in this section shall be construed to affect the authorities or responsibilities of the Administrator of the Federal Emergency Management Agency pursuant to section 748 of this title.

(Pub. L. 107–296, title XXII, §2220B, as added Pub. L. 117–81, div. A, title XV, §1547(a), Dec. 27, 2021, 135 Stat. 2059.)

§ 665i. CyberSentry program

(a) Establishment

There is established in the Agency a program, to be known as “CyberSentry”, to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, upon request and subject to the consent of such owner or operator.

(b) Activities

The Director, through CyberSentry, shall—

(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such owner or operator;

(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such vulnerabilities;

(4) produce aggregated, anonymized analytic products, based on threat hunting and contin-

uous monitoring and detection activities and partnerships, with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022.

(c) Privacy review

Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency under section 652(h) of this title shall—

(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

(2) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report certifying compliance with all applicable privacy laws as referred to in paragraph (1), or identifying any instances of noncompliance with such privacy laws.

(d) Report to Congress

Not later than one year after December 27, 2021, the Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing and written report on implementation of this section.

(e) Savings

Nothing in this section may be construed to permit the Federal Government to gain access to information of a remote computing service provider to the public or an electronic service provider to the public, the disclosure of which is not permitted under section 2702 of title 18.

(f) Definition

In this section, the term “industrial control system” means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (DCSSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

(g) Termination

The authority to carry out a program under this section shall terminate on the date that is seven years after December 27, 2021.

(Pub. L. 107–296, title XXII, §2220C, as added Pub. L. 117–81, div. A, title XV, §1548(a), Dec. 27, 2021, 135 Stat. 2061; amended Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(L), Dec. 23, 2022, 136 Stat. 3661.)

Editorial Notes

REFERENCES IN TEXT

Section 1501 of the National Defense Authorization Act for Fiscal Year 2022, referred to in subsec. (b)(5), is section 1501 of Pub. L. 117–81, div. A, title XV, Dec. 27, 2021, 135 Stat. 2020, related to development of taxonomy

of cyber capabilities, which is not classified to the Code.

CODIFICATION

Section 1548(a) of Pub. L. 117-81, which directed that this section be added at the end of title XXII of the Homeland Security Act of 2002, was executed by adding this section at the end of this part as if the directory language had added the section at the end of subtitle A of title XXII of the Act, to reflect the probable intent of Congress.

AMENDMENTS

2022—Subsec. (f). Pub. L. 117-263 added subsec. (f) and struck out former subsec. (f) which defined cybersecurity risk, industrial control system, and information system.

§ 665j. Ransomware threat mitigation activities

(a) Joint Ransomware Task Force

(1) In general

Not later than 180 days after March 15, 2022, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) Composition

The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) Responsibilities

The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify¹ metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

¹ So in original.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

(b) Rule of construction

Nothing in this section shall be construed to provide any additional authority to any Federal agency.

(Pub. L. 117-103, div. Y, §106, Mar. 15, 2022, 136 Stat. 1056.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Statutory Notes and Related Subsidiaries

DEFINITIONS

Pub. L. 117-103, div. Y, §102, Mar. 15, 2022, 136 Stat. 1038, provided that: “In this division [see Short Title of 2022 Amendment note set out under section 101 of this title]:

“(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ‘covered cyber incident’, ‘covered entity’, ‘cyber incident’, ‘information system’, ‘ransom payment’, ‘ransomware attack’, and ‘security vulnerability’ have the meanings given those terms in section 2240 of the Homeland Security Act of 2002 [6 U.S.C. 681], as added by section 103 of this division [see also 6 U.S.C. 650].

“(2) DIRECTOR.—The term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency.”

§ 665k. Federal Clearinghouse on School Safety Evidence-based Practices

(a) Establishment

(1) In general

The Secretary, in coordination with the Secretary of Education, the Attorney General, and the Secretary of Health and Human Services, shall establish a Federal Clearinghouse on School Safety Evidence-based Practices (in this section referred to as the “Clearinghouse”) within the Department.

(2) Purpose

The Clearinghouse shall serve as a Federal resource to identify and publish online through SchoolSafety.gov, or any successor website, evidence-based practices and recommendations to improve school safety for use by State and local educational agencies, institutions of higher education, State and local law enforcement agencies, health professionals, and the general public.

(3) Personnel

(A) Assignments

The Clearinghouse shall be assigned such personnel and resources as the Secretary

considers appropriate to carry out this section.

(B) Detailees

The Secretary of Education, the Attorney General, and the Secretary of Health and Human Services may detail personnel to the Clearinghouse.

(4) Exemptions

(A) Paperwork Reduction Act

Chapter 35 of title 44 (commonly known as the “Paperwork Reduction Act”), shall not apply to any rulemaking or information collection required under this section.

(B) Federal Advisory Committee Act

The Federal Advisory Committee Act (5 U.S.C. App.)¹ shall not apply for the purposes of carrying out this section.

(b) Clearinghouse contents

(1) Consultation

In identifying the evidence-based practices and recommendations for the Clearinghouse, the Secretary shall—

(A) consult with appropriate Federal, State, local, Tribal, private sector, and nongovernmental organizations, including civil rights and disability rights organizations; and

(B) consult with the Secretary of Education to ensure that evidence-based practices published by the Clearinghouse are aligned with evidence-based practices to support a positive and safe learning environment for all students.

(2) Criteria for evidence-based practices and recommendations

The evidence-based practices and recommendations of the Clearinghouse shall—

(A) include comprehensive evidence-based school safety measures;

(B) include the evidence or research rationale supporting the determination of the Clearinghouse that the evidence-based practice or recommendation under subparagraph (A) has been shown to have a significant effect on improving the health, safety, and welfare of persons in school settings, including—

(i) relevant research that is evidence-based, as defined in section 7801 of title 20, supporting the evidence-based practice or recommendation;

(ii) findings and data from previous Federal or State commissions recommending improvements to the safety posture of a school; or

(iii) other supportive evidence or findings relied upon by the Clearinghouse in determining evidence-based practices and recommendations, as determined in consultation with the officers described in subsection (a)(3)(B);

(C) include information on Federal programs for which implementation of each evidence-based practice or recommendation is an eligible use for the program;

(D) be consistent with Federal civil rights laws, including title II of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.); and

(E) include options for developmentally appropriate recommendations for use in educational settings with respect to children’s ages and physical, social, sensory, and emotionally developmental statuses.

(3) Past commission recommendations

The Clearinghouse shall present, as determined in consultation with the officers described in subsection (a)(3)(B), Federal, State, local, Tribal, private sector, and nongovernmental organization issued best practices and recommendations and identify any best practice or recommendation of the Clearinghouse that was previously issued by any such organization or commission.

(c) Assistance and training

The Secretary may produce and publish materials on the Clearinghouse to assist and train educational agencies and law enforcement agencies on the implementation of the evidence-based practices and recommendations.

(d) Continuous improvement

The Secretary shall—

(1) collect for the purpose of continuous improvement of the Clearinghouse—

(A) Clearinghouse data analytics;

(B) user feedback on the implementation of resources, evidence-based practices, and recommendations identified by the Clearinghouse; and

(C) any evaluations conducted on implementation of the evidence-based practices and recommendations of the Clearinghouse; and

(2) in coordination with the Secretary of Education, the Secretary of Health and Human Services, and the Attorney General—

(A) regularly assess and identify Clearinghouse evidence-based practices and recommendations for which there are no resources available through Federal Government programs for implementation; and

(B) establish an external advisory board, which shall be comprised of appropriate State, local, Tribal, private sector, and nongovernmental organizations, including organizations representing parents of elementary and secondary school students, representative² from civil rights organizations, representatives of disability rights organizations, representatives of educators, representatives of law enforcement, and non-profit school safety and security organizations, to—

(i) provide feedback on the implementation of evidence-based practices and recommendations of the Clearinghouse; and

(ii) propose additional recommendations for evidence-based practices for inclusion

¹ See References in Text note below.

² So in original. Probably should be “representatives”.

in the Clearinghouse that meet the requirements described in subsection (b)(2)(B).

(e) Parental assistance

The Clearinghouse shall produce materials in accessible formats to assist parents and legal guardians of students with identifying relevant Clearinghouse resources related to supporting the implementation of Clearinghouse evidence-based practices and recommendations.

(Pub. L. 107–296, title XXII, §2220D, as added Pub. L. 117–159, div. A, title III, §13302(a), June 25, 2022, 136 Stat. 1334.)

Editorial Notes

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (a)(4)(B), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, which was set out in the Appendix to Title 5, Government Organization and Employees, and was substantially repealed and restated in chapter 10 (§1001 et seq.) of Title 5 by Pub. L. 117–286, §§3(a), 7, Dec. 27, 2022, 136 Stat. 4197, 4361. For disposition of sections of the Act into chapter 10 of Title 5, see Disposition Table preceding section 101 of Title 5.

The Americans with Disabilities Act of 1990, referred to in subsec. (b)(2)(D), is Pub. L. 101–336, July 26, 1990, 104 Stat. 327. Title II of the Act is classified generally to subchapter II (§12131 et seq.) of chapter 126 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 12101 of Title 42 and Tables.

The Rehabilitation Act of 1973, referred to in subsec. (b)(2)(D), is Pub. L. 93–112, Sept. 26, 1973, 87 Stat. 355, which is classified generally to chapter 16 (§701 et seq.) of Title 29, Labor. For complete classification of this Act to the Code, see Short Title note set out under section 701 of Title 29 and Tables.

The Civil Rights Act of 1964, referred to in subsec. (b)(2)(D), is Pub. L. 88–352, July 2, 1964, 78 Stat. 241. Title VI of the Act is classified generally to subchapter V (§2000d et seq.) of chapter 21 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 2000a of Title 42 and Tables.

Statutory Notes and Related Subsidiaries

LUKE AND ALEX SCHOOL SAFETY ACT OF 2022

Pub. L. 117–159, div. A, title III, subtitle C, June 25, 2022, 136 Stat. 1334, provided that:

“SEC. 13301. SHORT TITLE.

“This subtitle may be cited as the ‘Luke and Alex School Safety Act of 2022’.

“SEC. 13302. FEDERAL CLEARINGHOUSE ON SCHOOL SAFETY EVIDENCE-BASED PRACTICES.

“(a) IN GENERAL.—[Enacted this section.]

“(b) TECHNICAL AMENDMENTS.—[Amended table of contents of the Homeland Security Act of 2002.]

“SEC. 13303. NOTIFICATION OF CLEARINGHOUSE.

“(a) NOTIFICATION BY THE SECRETARY OF EDUCATION.—The Secretary of Education shall provide written notification of the publication of the Federal Clearinghouse on School Safety Evidence-based Practices (referred to in this section and section 13304 as the ‘Clearinghouse’), as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

“(1) every State and local educational agency; and

“(2) other Department of Education partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Education.

“(b) NOTIFICATION BY THE SECRETARY OF HOMELAND SECURITY.—The Secretary of Homeland Security shall provide written notification of the publication of the Clearinghouse, as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

“(1) every State homeland security advisor;

“(2) every State department of homeland security; and

“(3) other Department of Homeland Security partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Homeland Security.

“(c) NOTIFICATION BY THE SECRETARY OF HEALTH AND HUMAN SERVICES.—The Secretary of Health and Human Services shall provide written notification of the publication of the Clearinghouse, as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

“(1) every State department of public health; and

“(2) other Department of Health and Human Services partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Health and Human Services.

“(d) NOTIFICATION BY THE ATTORNEY GENERAL.—The Attorney General shall provide written notification of the publication of the Clearinghouse, as required to be established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by section 13302 of this Act, to—

“(1) every State department of justice; and

“(2) other Department of Justice partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Attorney General.

“SEC. 13304. GRANT PROGRAM REVIEW.

“(a) FEDERAL GRANTS AND RESOURCES.—Not later than 1 year after the date of enactment of this Act [June 25, 2022], the Clearinghouse or the external advisory board established under section 2220D of the Homeland Security Act of 2002 [6 U.S.C. 665k], as added by this subtitle, shall—

“(1) review grant programs and identify any grant program that may be used to implement evidence-based practices and recommendations of the Clearinghouse;

“(2) identify any evidence-based practices and recommendations of the Clearinghouse for which there is not a Federal grant program that may be used for the purposes of implementing the evidence-based practice or recommendation as applicable to the agency; and

“(3) periodically report any findings under paragraph (2) to the appropriate committees of Congress.

“(b) STATE GRANTS AND RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—

“(1) each agency responsible for school safety in the State, or any State that does not have such an agency designated;

“(2) any grant program that may be used for the purposes of implementing evidence-based practices and recommendations of the Clearinghouse; and

“(3) any resources other than grant programs that may be used to assist in implementation of evidence-based practices and recommendations of the Clearinghouse.

“SEC. 13305. RULES OF CONSTRUCTION.

“(a) WAIVER OF REQUIREMENTS.—Nothing in this subtitle or the amendments made by this subtitle shall be construed to create, satisfy, or waive any requirement under—

“(1) title II of the Americans With [sic] Disabilities Act of 1990 (42 U.S.C. 12131 et seq.);

“(2) the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.);

“(3) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.);

“(4) title IX of the Education Amendments of 1972 (20 U.S.C. 1681 et seq.); or

“(5) the Age Discrimination Act of 1975 (42 U.S.C. 6101 et seq.).

“(b) PROHIBITION ON FEDERALLY DEVELOPED, MAN-DATED, OR ENDORSED CURRICULUM.—Nothing in this subtitle or the amendments made by this subtitle shall be construed to authorize any officer or employee of the Federal Government to engage in an activity otherwise prohibited under section 103(b) of the Department of Education Organization Act (20 U.S.C. 3403(b)).”

§ 665L. School and daycare protection

(a) In general

Not later than 180 days after December 23, 2022, and annually thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report regarding the following:

(1) The Department of Homeland Security’s activities, policies, and plans to enhance the security of early childhood education programs, elementary schools, and secondary schools during the preceding year that includes information on the Department’s activities through the Federal School Safety Clearinghouse.

(2) Information on all structures or efforts within the Department intended to bolster coordination among departmental components and offices involved in carrying out paragraph (1) and, with respect to each structure or effort, specificity on which components and offices are involved and which component or office leads such structure or effort.

(3) A detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out these activities.

(b) Briefing

Not later than 30 days after the submission of each report required under subsection (a), the Secretary of Homeland Security shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing regarding such report and the status of efforts to carry out plans included in such report for the preceding year.

(c) Definitions

In this section, the terms “early childhood education program”, “elementary school”, and “secondary school” have the meanings given such terms in section 7801 of title 20.

(Pub. L. 117–263, div. G, title LXXI, § 7103, Dec. 23, 2022, 136 Stat. 3621.)

Editorial Notes

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§ 665m. President’s Cup Cybersecurity Competition

(a) In general

The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the “Director”) of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the “Department of Homeland Security Cybersecurity and Infrastructure Security Agency’s President’s Cup Cybersecurity Competition” (in this section referred to as the “competition”) for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government’s best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

(b) Eligibility

To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5) and shall comply with any rules promulgated by the Director regarding the competition.

(c) Competition administration

The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(d) Competition parameters

Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraphs (1), (2), or (3), as determined necessary by the Director.

(e) Use of funds

(1) In general

In order to further the goals and objectives of the competition, the Director may use amounts made available to the Director for the competition for reasonable expenses for the following:

(A) Advertising, marketing, and promoting the competition.

(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition.

(C) Promotional items, including merchandise and apparel.

(D) Consistent with section 4503 of title 5, necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(E) Monetary and nonmonetary awards for competition participants, including members of the uniformed services, subject to subsection (f).

(2) Application

This subsection shall apply to amounts appropriated on or after December 23, 2022.

(f) Prize limitation

(1) Awards by the Director

The Director may make one or more awards per competition, except that the amount or value of each shall not exceed \$10,000.

(2) Awards by the Secretary of Homeland Security

The Secretary of Homeland Security may make one or more awards per competition, except the amount or the value of each shall not exceed \$25,000.

(3) Regular pay

A monetary award under this section shall be in addition to the regular pay of the recipient.

(4) Overall yearly award limit

The total amount or value of awards made under this Act¹ during a fiscal year may not exceed \$100,000.

(g) Reporting requirements

The Director shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following with respect to each competition conducted in the preceding year:

- (1) A description of available amounts.
- (2) A description of authorized expenditures.
- (3) Information relating to participation.
- (4) Information relating to lessons learned, and how such lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(Pub. L. 117–263, div. G, title LXXI, § 7121, Dec. 23, 2022, 136 Stat. 3638.)

Editorial Notes

REFERENCES IN TEXT

This Act, referred to in subsec. (f)(4), is Pub. L. 117–263, Dec. 23, 2022, 136 Stat. 2395, known as the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, but probably means H.R. 6824, 117th Cong., 2d Sess. (as reported to the Senate), known as the President's Cup Cybersecurity Competition Act, which consisted only of the section containing the short title and this section. The reference to “this Act” from the original was not updated when the text of H.R. 6824 was incorporated into Pub. L. 117–263.

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

¹ So in original. Probably should refer to “this section”. See References in Text note below.

§ 665n. Industrial Control Systems Cybersecurity Training Initiative

(a) Establishment

(1) In general

The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the “Initiative”) is established within the Agency.

(2) Purpose

The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

(b) Requirements

In carrying out the Initiative, the Director shall—

- (1) ensure the Initiative includes—

(A) virtual and in-person trainings and courses provided at no cost to participants;

(B) trainings and courses available at different skill levels, including introductory level courses;

(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and

(D) appropriate consideration regarding the availability of trainings and courses in different regions of the United States; and¹

- (2) engage in—

(A) collaboration with the National Laboratories of the Department of Energy in accordance with section 189 of this title;

(B) consultation with Sector Risk Management Agencies;²

(C) as appropriate, consultation with private sector entities with relevant expertise, such as vendors of industrial control systems technologies; and

(3) consult, to the maximum extent practicable, with commercial training providers and academia to minimize the potential for duplication of other training opportunities.

(c) Reports

(1) In general

Not later than one year after December 23, 2022, and annually thereafter, the Director shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the Initiative.

(2) Contents

Each report submitted under paragraph (1) shall include the following:

(A) A description of the courses provided under the Initiative.

(B) A description of outreach efforts to raise awareness of the availability of such courses.

¹ So in original. The word “and” probably should not appear.

² So in original. Probably should be followed by “and”.

(C) The number of participants in each course.

(D) Voluntarily provided information on the demographics of participants in such courses, including by sex, race, and place of residence.

(E) Information on the participation in such courses of workers from each critical infrastructure sector.

(F) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

(G) Recommendations regarding how to strengthen the state of industrial control systems cybersecurity education and training.

(Pub. L. 107–296, title XXII, §2220E, as added Pub. L. 117–263, div. G, title LXXI, §7122(a), Dec. 23, 2022, 136 Stat. 3640.)

PART B—CRITICAL INFRASTRUCTURE INFORMATION

Editorial Notes

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” has the meaning given the term in section 650 of this title.

(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) 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.

(6) 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 78l(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.

(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; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(M), Dec. 23, 2022, 136 Stat. 3661.)

Editorial Notes

CODIFICATION

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

AMENDMENTS

2022—Par. (3). Pub. L. 117–263, §7143(b)(2)(M)(i), added par. (3) and struck out former par. (3) which defined critical infrastructure information.

Pars. (5) to (8). Pub. L. 117–263, §7143(b)(2)(M)(ii), (iii), redesignated pars. (6) and (7) as (5) and (6), respectively, and struck out former pars. (5) and (8) which defined Information Sharing and Analysis Organization and cybersecurity risk and incident, respectively.

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).

Statutory Notes and Related Subsidiaries

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.

“(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] [see now 6 U.S.C. 650].

“(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.)

Editorial Notes

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.

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

(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 chapter 10 of title 5.

(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 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; Pub. L. 117-286, §4(a)(18), Dec. 27, 2022, 136 Stat. 4307.)

Editorial Notes**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.

CODIFICATION

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

AMENDMENTS

2022—Subsec. (b). Pub. L. 117–286 substituted “chapter 10 of title 5.” for “the Federal Advisory Committee Act.”

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”.

Statutory Notes and Related Subsidiaries

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.)

Editorial Notes

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.

PART C—DECLARATION OF A SIGNIFICANT INCIDENT

§ 677. Sense of Congress

It is the sense of Congress that—

(1) the purpose of this part is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and

(2) the authorities established under this part are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.

(Pub. L. 107–296, title XXII, § 2231, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1267.)

§ 677a. Definitions

For the purposes of this part:

(1) Asset response activity

The term “asset response activity” means an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—

(A) furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;

(B) assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;

(C) developing courses of action to mitigate the risks assessed under subparagraph (B);

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

(E) providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

(2) Declaration

The term “declaration” means a declaration of the Secretary under section 677b(a)(1) of this title.

(3) Director

The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency.

(4) Federal agency

The term “Federal agency” has the meaning given the term “agency” in section 3502 of title 44.

(5) Fund

The term “Fund” means the Cyber Response and Recovery Fund established under section 677c(a) of this title.

(6) Incident

The term “incident” has the meaning given the term in section 3552 of title 44.

(7) Renewal

The term “renewal” means a renewal of a declaration under section 677b(d) of this title.

(8) Significant incident

The term “significant incident”—

(A) means an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—

(i) the national security interests, foreign relations, or economy of the United States; or

(ii) the public confidence, civil liberties, or public health and safety of the people of the United States; and

(B) does not include an incident or a portion of a group of related incidents that occurs on—

(i) a national security system (as defined in section 3552 of title 44); or

(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44.

(Pub. L. 107–296, title XXII, § 2232, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1267.)

§ 677b. Declaration

(a) In general

(1) Declaration

The Secretary, in consultation with the National Cyber Director, may make a declaration of a significant incident in accordance with this section for the purpose of enabling the activities described in this part if the Secretary determines that—

(A) a specific significant incident—

(i) has occurred; or

(ii) is likely to occur imminently; and

(B) otherwise available resources, other than the Fund, are likely insufficient to respond effectively to, or to mitigate effectively, the specific significant incident described in subparagraph (A).

(2) Prohibition on delegation

The Secretary may not delegate the authority provided to the Secretary under paragraph (1).

(b) Asset response activities

Upon a declaration, the Director shall coordinate—

(1) the asset response activities of each Federal agency in response to the specific significant incident associated with the declaration; and

(2) with appropriate entities, which may include—

(A) public and private entities and State and local governments with respect to the asset response activities of those entities and governments; and

(B) Federal, State, local, and Tribal law enforcement agencies with respect to investigations and threat response activities of those law enforcement agencies; and

(3) Federal, State, local, and Tribal emergency management and response agencies.

(c) Duration

Subject to subsection (d), a declaration shall terminate upon the earlier of—

(1) a determination by the Secretary that the declaration is no longer necessary; or

(2) the expiration of the 120-day period beginning on the date on which the Secretary makes the declaration.

(d) Renewal

The Secretary, without delegation, may renew a declaration as necessary.

(e) Publication

(1) In general

Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.

(2) Prohibition

A declaration or renewal published under paragraph (1) may not include the name of any affected individual or private company.

(f) Advance actions

(1) In general

The Secretary—

(A) shall assess the resources available to respond to a potential declaration; and

(B) may take actions before and while a declaration is in effect to arrange or procure additional resources for asset response activities or technical assistance the Secretary determines necessary, which may include entering into standby contracts with private entities for cybersecurity services or incident responders in the event of a declaration.

(2) Expenditure of funds

Any expenditure from the Fund for the purpose of paragraph (1)(B) shall be made from amounts available in the Fund, and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purpose.

(Pub. L. 107–296, title XXII, § 2233, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1268.)

§ 677c. Cyber Response and Recovery Fund

(a) In general

There is established a Cyber Response and Recovery Fund, which shall be available for—

(1) the coordination of activities described in section 677b(b) of this title;

(2) response and recovery support for the specific significant incident associated with a declaration to Federal, State, local, and Tribal, entities and public and private entities on a reimbursable or non-reimbursable basis, including through asset response activities and technical assistance, such as—

(A) vulnerability assessments and mitigation;

(B) technical incident mitigation;

(C) malware analysis;

(D) analytic support;

(E) threat detection and hunting; and

(F) network protections;

(3) as the Director determines appropriate, grants for, or cooperative agreements with, Federal, State, local, and Tribal public and private entities to respond to, and recover from, the specific significant incident associated with a declaration, such as—

(A) hardware or software to replace, update, improve, harden, or enhance the functionality of existing hardware, software, or systems; and

(B) technical contract personnel support; and

(4) advance actions taken by the Secretary under section 677b(f)(1)(B) of this title.

(b) Deposits and expenditures

(1) In general

Amounts shall be deposited into the Fund from—

(A) appropriations to the Fund for activities of the Fund; and

(B) reimbursement from Federal agencies for the activities described in paragraphs (1),

(2), and (4) of subsection (a), which shall only be from amounts made available in advance in appropriations Acts for such reimbursement.

(2) Expenditures

Any expenditure from the Fund for the purposes of this part shall be made from amounts available in the Fund from a deposit described in paragraph (1), and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purposes.

(c) Supplement not supplant

Amounts in the Fund shall be used to supplement, not supplant, other Federal, State, local, or Tribal funding for activities in response to a declaration.

(d) Reporting

The Secretary shall require an entity that receives amounts from the Fund to submit a report to the Secretary that details the specific use of the amounts.

(Pub. L. 107–296, title XXII, § 2234, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1270.)

§ 677d. Notification and reporting

(a) Notification

Upon a declaration or renewal, the Secretary shall immediately notify the National Cyber Director and appropriate congressional committees and include in the notification—

(1) an estimation of the planned duration of the declaration;

(2) with respect to a notification of a declaration, the reason for the declaration, including information relating to the specific significant incident or imminent specific significant incident, including—

(A) the operational or mission impact or anticipated impact of the specific significant incident on Federal and non-Federal entities;

(B) if known, the perpetrator of the specific significant incident; and

(C) the scope of the Federal and non-Federal entities impacted or anticipated to be impacted by the specific significant incident;

(3) with respect to a notification of a renewal, the reason for the renewal;

(4) justification as to why available resources, other than the Fund, are insufficient to respond to or mitigate the specific significant incident; and

(5) a description of the coordination activities described in section 677b(b) of this title that the Secretary anticipates the Director to perform.

(b) Report to Congress

Not later than 180 days after the date of a declaration or renewal, the Secretary shall submit to the appropriate congressional committees a report that includes—

(1) the reason for the declaration or renewal, including information and intelligence relat-

ing to the specific significant incident that led to the declaration or renewal;

(2) the use of any funds from the Fund for the purpose of responding to the incident or threat described in paragraph (1);

(3) a description of the actions, initiatives, and projects undertaken by the Department and State and local governments and public and private entities in responding to and recovering from the specific significant incident described in paragraph (1);

(4) an accounting of the specific obligations and outlays of the Fund; and

(5) an analysis of—

(A) the impact of the specific significant incident described in paragraph (1) on Federal and non-Federal entities;

(B) the impact of the declaration or renewal on the response to, and recovery from, the specific significant incident described in paragraph (1); and

(C) the impact of the funds made available from the Fund as a result of the declaration or renewal on the recovery from, and response to, the specific significant incident described in paragraph (1).

(c) Classification

Each notification made under subsection (a) and each report submitted under subsection (b)—

(1) shall be in an unclassified form with appropriate markings to indicate information that is exempt from disclosure under section 552 of title 5 (commonly known as the “Freedom of Information Act”); and

(2) may include a classified annex.

(d) Consolidated report

The Secretary shall not be required to submit multiple reports under subsection (b) for multiple declarations or renewals if the Secretary determines that the declarations or renewals substantively relate to the same specific significant incident.

(e) Exemption

The requirements of subchapter I of chapter 35 of title 44 (commonly known as the “Paperwork Reduction Act”) shall not apply to the voluntary collection of information by the Department during an investigation of, a response to, or an immediate post-response review of, the specific significant incident leading to a declaration or renewal.

(Pub. L. 107–296, title XXII, § 2235, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1270.)

§ 677e. Rule of construction

Nothing in this part shall be construed to impair or limit the ability of the Director to carry out the authorized activities of the Cybersecurity and Infrastructure Security Agency.

(Pub. L. 107–296, title XXII, § 2236, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

§ 677f. Authorization of appropriations

There are authorized to be appropriated to the Fund \$20,000,000 for fiscal year 2022 and each fis-

cal year thereafter until September 30, 2028, which shall remain available until September 30, 2028.

(Pub. L. 107-296, title XXII, § 2237, as added Pub. L. 117-58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

§ 677g. Sunset

The authorities granted to the Secretary or the Director under this part shall expire on the date that is 7 years after November 15, 2021.

(Pub. L. 107-296, title XXII, § 2238, as added Pub. L. 117-58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

PART D—CYBER INCIDENT REPORTING

§ 681. Definitions

In this part:

(1) Center

The term “Center” means the center established under section 659 of this title.

(2) Council

The term “Council” means the Cyber Incident Reporting Council described in section 681f of this title.

(3) Covered cyber incident

The term “covered cyber incident” means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title.

(4) Covered entity

The term “covered entity” means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title.

(5) Cyber incident

The term “cyber incident”—

(A) has the meaning given the term “incident” in section 659¹ of this title; and

(B) does not include an occurrence that imminently, but not actually, jeopardizes—

- (i) information on information systems; or
- (ii) information systems.

(6) Cyber threat

The term “cyber threat” has the meaning given the term “cybersecurity threat” in section 650 of this title.

(7) Federal entity

The term “Federal entity” has the meaning given the term in section 1501 of this title.

(8) Ransom payment

The term “ransom payment” means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

(9) Significant cyber incident

The term “significant cyber incident” means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

(10) Virtual currency

The term “virtual currency” means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

(11) Virtual currency address

The term “virtual currency address” means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

(Pub. L. 107-296, title XXII, § 2240, as added Pub. L. 117-103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1039; amended Pub. L. 117-263, div. G, title LXXI, § 7143(b)(2)(N), Dec. 23, 2022, 136 Stat. 3661.)

Editorial Notes

REFERENCES IN TEXT

Section 659 of this title, referred to in par. (5)(A), was subsequently amended, and section 659(a) no longer defines the term “incident”. Reference to term, “incident”, as defined in this chapter deemed to be a reference to that term as defined in section 650(12) of this title, see section 7143(f)(2) of Pub. L. 117-263, set out as a Rule of Construction note under section 650 of this title.

AMENDMENTS

2022—Par. (2). Pub. L. 117-263, § 7143(b)(2)(N)(i), (ii), redesignated par. (3) as (2) and struck out former par. (2). Prior to amendment, text of par. (2) read as follows: “The term ‘cloud service provider’ means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto.”

Pars. (3) to (5). Pub. L. 117-263, § 7143(b)(2)(N)(ii), redesignated pars. (4) to (6) as pars. (3) to (5), respectively. Former par. (3) redesignated (2).

Par. (6). Pub. L. 117-263, § 7143(b)(2)(N)(ii), (iii), redesignated par. (7) as (6) and substituted “section 650 of this title” for “section 651 of this title”. Former par. (6) redesignated (5).

Par. (7). Pub. L. 117-263, § 7143(b)(2)(N)(iv), added par. (7). Former par. (7) redesignated (6).

Par. (8). Pub. L. 117-263, § 7143(b)(2)(N)(iv), (vi), redesignated par. (13) as (8) and struck out former par. (8). Prior to amendment, text of par. (8) read as follows: “The terms ‘cyber threat indicator’, ‘cybersecurity purpose’, ‘defensive measure’, ‘Federal entity’, and ‘security vulnerability’ have the meanings given those terms in section 1501 of this title.”

Par. (9). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (16) as (9) and struck out former par. (9). Prior to amendment, text of par. (9) read as follows: “The terms ‘incident’ and ‘sharing’ have the meanings given those terms in section 659 of this title.”

Par. (10). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (18) as (10) and struck out former par. (10). Prior to amendment, text of par. (10) read as follows: “The term ‘Information Sharing and Analysis Organization’ has the meaning given the term in section 671 of this title.”

Par. (11). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (19) as (11) and struck out former par. (11).

¹ See References in Text note below.

Prior to amendment, text of par. (11) read as follows: “The term ‘information system’—

“(A) has the meaning given the term in section 3502 of title 44; and

“(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.”

Par. (12). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (12). Text read as follows: “The term ‘managed service provider’ means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.”

Par. (13). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated par. (13) as (8).

Par. (14). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (14). Text read as follows: “The term ‘ransomware attack’—

“(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

“(B) does not include any such event where the demand for payment is—

“(i) not genuine; or

“(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.”

Par. (15). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (15). Text read as follows: “The term ‘Sector Risk Management Agency’ has the meaning given the term in section 651 of this title.”

Par. (16). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated par. (16) as (9).

Par. (17). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (17). Text read as follows: “The term ‘supply chain compromise’ means an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.”

Par. (18). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated par. (18) as (10).

§ 681a. Cyber incident review

(a) Activities

The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

(3) leverage information gathered about cyber incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 681e of this title;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under section¹ 681b(a) and 681c of this title involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

(9) proactively identify opportunities, consistent with the protections in section 681e of this title, to leverage and utilize data on cyber incidents in a manner that enables and

¹ So in original. Probably should be “sections”.

strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

(10) in accordance with section 681e of this title and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 681c of this title, or information received pursuant to a request for information or subpoena under section 681d of this title, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

(b) Interagency sharing

The President or a designee of the President—

(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

(2) shall determine the appropriate Federal agencies under subsection (a)(10).

(c) Periodic briefing

Not later than 60 days after the effective date of the final rule required under section 681b(b) of this title, and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

(1) include the total number of reports submitted under sections 681b and 681c of this title during the preceding month, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 681b and 681c of this title, including—

(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

(3) include a summary of the known uses of the information in reports submitted under sections 681b and 681c of this title; and

(4) include an unclassified portion, but may include a classified component.

(Pub. L. 107-296, title XXII, §2241, as added Pub. L. 117-103, div. Y, §103(a)(2), Mar. 15, 2022, 136 Stat. 1040.)

Editorial Notes

REFERENCES IN TEXT

The Cybersecurity Information Sharing Act of 2015, referred to in subsec. (a)(1), is title I of div. N of Pub. L. 114-113, Dec. 18, 2015, 129 Stat. 2936, which is classified generally to subchapter I (§1501 et seq.) of chapter 6 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1501 of this title and Tables.

§ 681b. Required reporting of certain cyber incidents

(a) In general

(1) Covered cyber incident reports

(A) In general

A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

(B) Limitation

The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

(2) Ransom payment reports

(A) In general

A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

(B) Application

The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

(3) Supplemental reports

A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until such date that such covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

(4) Preservation of information

Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

(5) Exceptions

(A) Reporting of covered cyber incident with ransom payment

If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement

under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

(B) Substantially similar reported information

(i) In general

Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements of section 681g(a) of this title, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

(ii) Limitation

The exemption in clause (i) shall take effect with respect to a covered entity once an agency agreement and sharing mechanism is in place between the Agency and the respective Federal agency, pursuant to section 681g(a) of this title.

(iii) Rules of construction

Nothing in this paragraph shall be construed to—

(I) exempt a covered entity from the reporting requirements under paragraph (3) unless the supplemental report also meets the requirements of clauses (i) and (ii) of this paragraph;¹

(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant to section 681g of this title; or

(III) prevent an entity from communicating with the Agency.

(C) Domain name system

The requirements under paragraphs (1), (2) and (3) shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

(6) Manner, timing, and form of reports

Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

(7) Effective date

Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

(b) Rulemaking

(1) Notice of proposed rulemaking

Not later than 24 months after March 15, 2022, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

(2) Final rule

Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

(3) Subsequent rulemakings

(A) In general

The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

(B) Procedures

Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, including the issuance of a notice of proposed rulemaking under section 553 of such title.

(c) Elements

The final rule issued pursuant to subsection (b) shall be composed of the following elements:

(1) A clear description of the types of entities that constitute covered entities, based on—

(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

(A) at a minimum, require the occurrence of—

(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against²

(I) an information system or network; or

(II) an operational technology system or process; or

(iii) unauthorized access or disruption of business or industrial operations due to

¹ So in original. Probably should be “subparagraph”.

² So in original. Probably should be followed by a dash.

loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

(B) consider—

(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;

(ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and

(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

(C) exclude—

(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and

(ii) the threat of disruption as extortion, as described in section 681(14)(A)³ of this title.

(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the covered entity shall comply with the requirements in this part in reporting the covered cyber incident or ransom payment.

(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

(A) A description of the covered cyber incident, including—

(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such cyber incident;

(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

(iii) the estimated date range of such incident; and

(iv) the impact to the operations of the covered entity.

(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.

(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have

been, accessed or acquired by an unauthorized person.

(E) The name and other information that clearly identifies the covered entity impacted by the covered cyber incident, including, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers.

(F) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this part.

(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

(A) A description of the ransomware attack, including the estimated date range of the attack.

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

(D) The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.

(E) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that covered entity to assist with compliance with the requirements of this part.

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

(I) The amount of the ransom payment.

(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4), the period of time for which the data is required to be preserved, and allowable uses, processes, and procedures.

(7) Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—

(A) be established by the Director in consultation with the Council;

(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting require-

³ See References in Text note below.

ments to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable;

(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and

(D) provide a clear description of what constitutes substantial new or different information.

(8) Procedures for—

(A) entities, including third parties pursuant to subsection (d)(1), to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the Agency to carry out—

(i) the enforcement provisions of section 681d of this title, including with respect to the issuance, service, withdrawal, referral process, and enforcement of subpoenas, appeals and due process procedures;

(ii) other available enforcement mechanisms including acquisition, suspension and debarment procedures; and

(iii) other aspects of noncompliance;

(C) implementing the exceptions provided in subsection (a)(5); and

(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 1504(b) of this title and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

(9) Other procedural measures directly necessary to implement subsection (a).

(d) Third party report submission and ransom payment

(1) Report submission

A covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).

(2) Ransom payment

If a covered entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

(3) Duty to report

Third-party reporting under this subparagraph⁴ does not relieve a covered entity from the duty to comply with the requirements for

covered cyber incident report or ransom payment report submission.

(4) Responsibility to advise

Any third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this section.

(e) Outreach to covered entities

(1) In general

The Agency shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

(2) Elements

The outreach and education campaign under paragraph (1) shall include the following:

(A) An overview of the final rule issued pursuant to subsection (b).

(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken under section 681d of this title when a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

(F) An overview of the privacy and civil liberties requirements in this part.

(3) Coordination

In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

(A) the Critical Infrastructure Partnership Advisory Council established under section 451 of this title;

(B) Information Sharing and Analysis Organizations;

(C) trade associations;

(D) information sharing and analysis centers;

(E) sector coordinating councils; and

(F) any other entity as determined appropriate by the Director.

(f) Exemption

Sections 3506(c), 3507, 3508, and 3509 of title 44 shall not apply to any action to carry out this section.

(g) Rule of construction

Nothing in this section shall affect the authorities of the Federal Government to imple-

⁴ So in original. Probably should be "subsection".

ment the requirements of Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), including changes to the Federal Acquisition Regulations and remedies to include suspension and debarment.

(h) Savings provision

Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

(Pub. L. 107–296, title XXII, § 2242, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1042.)

Editorial Notes

REFERENCES IN TEXT

Section 681(14)(A) of this title, referred to in subsec. (c)(2)(C)(ii), was repealed by section 7143(b)(2)(N)(v) of Pub. L. 117–263. See section 650(22)(A) of this title. References to terms defined in this chapter deemed to be references to those terms as defined in section 650 of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

Executive Order 14028, referred to in subsec. (g), is Ex. Ord. No. 14028, May 12, 2021, 86 F.R. 26633, which is set out as a note under section 3551 of Title 44, Public Printing and Documents.

§ 681c. Voluntary reporting of other cyber incidents

(a) In general

Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) of section 681b(a) of this title, but may enhance the situational awareness of cyber threats.

(b) Voluntary provision of additional information in required reports

Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 681b(a) of this title information that is not required to be included, but may enhance the situational awareness of cyber threats.

(c) Application of section 681e of this title

Section 681e of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b) as it applies to reports and information submitted under section 681b of this title.

(Pub. L. 107–296, title XXII, § 2243, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1049; amended Pub. L. 117–263, div. G, title LXXI, § 7143(e)(1), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c). Pub. L. 117–263 added subsec. (c) and struck out former subsec. (c). Prior to amendment, text read as follows: “The protections under section 681e of this title applicable to reports made under section 681b of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).”

§ 681d. Noncompliance with required reporting

(a) Purpose

In the event that a covered entity that is required to submit a report under section 681b(a) of this title fails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

(b) Initial request for information

(1) In general

If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 681a(a) of this title, that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 681b(a) of this title, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) Treatment

Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 681b of this title¹ including that section 681e of this title shall apply to such information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 681b of this title.

(c) Enforcement

(1) In general

If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from which such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 681b of this title and any implementing regulations, and assess potential impacts to national security, economic security, or public health and safety.

(2) Civil action

(A) In general

If a covered entity fails to comply with a subpoena, the Director may refer the matter

¹ So in original. Probably should be followed by a comma.

to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

(B) Venue

An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

(C) Contempt of court

A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

(3) Non-delegation

The authority of the Director to issue a subpoena under this subsection may not be delegated.

(4) Authentication

(A) In general

Any subpoena issued electronically 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 electronically 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.

(d) Provision of certain information to Attorney General

(1) In general

Notwithstanding section 681e(a)(5) of this title and paragraph (b)(2) of this section, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution.

(2) Consultation

The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

(e) Considerations

When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

- (1) the complexity in determining if a covered cyber incident has occurred; and
- (2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

(f) Exclusions

This section shall not apply to a State, local, Tribal, or territorial government entity.

(g) Report to Congress

The Director shall submit to Congress an annual report on the number of times the Director—

- (1) issued an initial request for information pursuant to subsection (b);
- (2) issued a subpoena pursuant to subsection (c); or
- (3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

(h) Publication of the annual report

The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

- (1) issued an initial request for information pursuant to subsection (b); or
- (2) issued a subpoena pursuant to subsection (c).

(i) Anonymization of reports

The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

(Pub. L. 107-296, title XXII, § 2244, as added Pub. L. 117-103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1049; amended Pub. L. 117-263, div. G, title LXXI, § 7143(e)(2), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

AMENDMENTS

2022—Subsec. (b)(2). Pub. L. 117-263 inserted “including that section 681e of this title shall apply to such information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 681b of this title” after “section 681b of this title”.

§ 681e. Information shared with or provided to the Federal Government

(a) Disclosure, retention, and use

(1) Authorized activities

Information provided to the Agency pursuant to section 681b or 681c of this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

- (A) a cybersecurity purpose;
- (B) the purpose of identifying—
 - (i) a cyber threat, including the source of the cyber threat; or
 - (ii) a security vulnerability;

(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 681b or 681c of this title or any of the offenses listed in section 1504(d)(5)(A)(v) of this title.

(2) Agency actions after receipt

(A) Rapid, confidential sharing of cyber threat indicators

Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

(B) Principles for sharing security vulnerabilities

With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

(3) Privacy and civil liberties

Information contained in covered cyber incident and ransom payment reports submitted to the Agency pursuant to section 681b of this title shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 1504 of this title and in a manner that protects personal information from unauthorized use or unauthorized disclosure.

(4) Digital security

The Agency shall ensure that reports submitted to the Agency pursuant to section 681b of this title, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

(5) Prohibition on use of information in regulatory actions

(A) In general

A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this part to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, un-

less the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

(B) Clarification

A report submitted to the Agency pursuant to section 681b or 681c of this title may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.

(b) Protections for reporting entities and information

Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 681b of this title, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 681c of this title, shall—

(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

(2) be exempt from disclosure under section 552(b)(3) of title 5 (commonly known as the “Freedom of Information Act”), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

(4) not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) Liability protections

(1) In general

No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 681b(a) of this title that is submitted in conformance with this part and the rule promulgated under section 681b(b) of this title, except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 681d(c)(2) of this title.

(2) Scope

The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

(3) Restrictions

Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this part or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court,

regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this part shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

(d) Sharing with non-Federal entities

The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 681b of this title available to critical infrastructure owners and operators and the general public.

(e) Stored Communications Act

Nothing in this part shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18 (commonly known as the “Stored Communications Act”).

(Pub. L. 107–296, title XXII, § 2245, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1051.)

§ 681f. Cyber Incident Reporting Council

(a) Responsibility of the Secretary

The Secretary shall lead an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations.

(b) Rule of construction

Nothing in subsection (a) shall be construed to provide any additional regulatory authority to any Federal entity.

(Pub. L. 107–296, title XXII, § 2246, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1054.)

§ 681g. Federal sharing of incident reports

(a) Cyber incident reporting sharing

(1) In general

Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Department of Homeland Security (including the Cybersecurity and Infrastructure Security Agency) and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 681a(b) of this title, as added by section 103 of this division.

(2) Rule of construction

The requirements described in paragraph (1) and section 681e(d) of this title, as added by section 103 of this division, may not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure or provision of information within the executive branch.

(3) Protection of information

The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this division or the amendments made by this division.

(4) Effective date

This subsection shall take effect on the effective date of the final rule issued pursuant to section 681b(b) of this title, as added by section 103 of this division.

(5) Agency agreements

(A) In general

The Agency and any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives incident reports from entities, including due to ransomware attacks, shall, as appropriate, enter into a documented agreement to establish policies, processes, procedures, and mechanisms to ensure reports are shared with the Agency pursuant to paragraph (1).

(B) Availability

To the maximum extent practicable, each documented agreement required under subparagraph (A) shall be made publicly available.

(C) Requirement

The documented agreements required by subparagraph (A) shall require reports be shared from Federal agencies with the Agency in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments established in section 681b of this title, as added by section 103 of this division.

(b) Harmonizing reporting requirements

The Secretary of Homeland Security, acting through the Director, shall, in consultation with the Cyber Incident Reporting Council described in section 681f of this title, as added by section 103 of this division, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with appropriate Federal partners and regulatory authorities that receive reports relating to incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agree-

ments between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of the Agency to gain timely situational awareness of a covered cyber incident or ransom payment.

(Pub. L. 117–103, div. Y, §104, Mar. 15, 2022, 136 Stat. 1054.)

Editorial Notes

REFERENCES IN TEXT

Section 103 of this division, referred to in text, is section 103 of div. Y of Pub. L. 117–103, which enacted this part and amended section 659 of this title.

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of terms used in this section, see section 102 of div. Y of Pub. L. 117–103, which is set out as a note under section 665j of this title.

CHAPTER 2—NATIONAL EMERGENCY MANAGEMENT

Sec.

701. Definitions.

SUBCHAPTER I—PERSONNEL PROVISIONS

PART A—FEDERAL EMERGENCY MANAGEMENT AGENCY PERSONNEL

711. Surge Capacity Force.

PART B—EMERGENCY MANAGEMENT CAPABILITIES

- 721. Evacuation preparedness technical assistance.
- 722. Urban Search and Rescue Response System.
- 723. Metropolitan Medical Response Grant Program.
- 724. Logistics.
- 725. Prepositioned equipment program.
- 726. Basic life supporting first aid and education.
- 727. Improvements to information technology systems.
- 728. Disclosure of certain information to law enforcement agencies.

SUBCHAPTER II—COMPREHENSIVE PREPAREDNESS SYSTEM

PART A—NATIONAL PREPAREDNESS SYSTEM

- 741. Definitions.
- 742. National preparedness.
- 743. National preparedness goal.
- 744. Establishment of national preparedness system.
- 745. National planning scenarios.
- 746. Target capabilities and preparedness priorities.
- 747. Equipment and training standards.
- 748. Training and exercises.
- 748a. Prioritization of facilities.
- 749. Comprehensive assessment system.
- 750. Remedial action management program.
- 751. Federal response capability inventory.
- 752. Reporting requirements.
- 753. Federal preparedness.
- 754. Use of existing resources.

Sec.

PART B—ADDITIONAL PREPAREDNESS

- 761. Emergency Management Assistance Compact grants.
- 762. Emergency management performance grants program.
- 763. Transfer of Noble Training Center.
- 763a. Training for Federal Government, foreign governments, or private entities.
- 764. National exercise simulation center.
- 765. Real property transactions.

PART C—MISCELLANEOUS AUTHORITIES

- 771. National Disaster Recovery Strategy.
- 772. National Disaster Housing Strategy.
- 773. Individuals with disabilities guidelines.
- 774. Reunification.
- 775. National Emergency Family Registry and Locator System.
- 776. Individuals and households pilot program.
- 777. Public assistance pilot program.

PART D—PREVENTION OF FRAUD, WASTE, AND ABUSE

- 791. Advance contracting.
- 792. Repealed.
- 793. Oversight and accountability of Federal disaster expenditures.
- 794. Limitation on length of certain noncompetitive contracts.
- 795. Fraud, waste, and abuse controls.
- 796. Registry of disaster response contractors.
- 797. Fraud prevention training program.

PART E—AUTHORIZATION OF APPROPRIATIONS

- 811. Authorization of appropriations.

PART F—GLOBAL CATASTROPHIC RISK MANAGEMENT

- 821. Definitions.
- 822. Assessment of global catastrophic risk.
- 823. Report required.
- 824. Enhanced catastrophic incident annex.
- 825. Rules of construction.

§ 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

¹ See References in Text note below.