

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;