

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)”.