

“(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