Governmental Affairs of the Senate a report certifying compliance with all applicable privacy laws as referred to in paragraph (1), or identifying any instances of noncompliance with such privacy laws.

(d) Report to Congress

Not later than one year after December 27, 2021, the Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing and written report on implementation of this section.

(e) Savings

Nothing in this section may be construed to permit the Federal Government to gain access to information of a remote computing service provider to the public or an electronic service provider to the public, the disclosure of which is not permitted under section 2702 of title 18.

(f) Definition

In this section, the term ''industrial control system'' means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (DCSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

(g) Termination

The authority to carry out a program under this section shall terminate on the date that is seven years after December 27, 2021.

(Pub. L. 107–296, title XXII, § 2220C, as added Pub. L. 117–81, div. A, title XV, § 1548(a), Dec. 27, 2021, 135 Stat. 2061; amended Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(L), Dec. 23, 2022, 136 Stat. 3661.)

Editorial Notes

REFERENCES IN TEXT

Section 1501 of the National Defense Authorization Act for Fiscal Year 2022, referred to in subsec. (b)(5), is section 1501 of Pub. L. 117–81, div. A, title XV, Dec. 27, 2021, 135 Stat. 2020, related to development of taxonomy of cyber capabilities, which is not classified to the Code.

CODIFICATION

Section 1548(a) of Pub. L. 117–81, which directed that this section be added at the end of title XXII of the Homeland Security Act of 2002, was executed by adding this section at the end of this part as if the directory language had added the section at the end of subtitle A of title XXII of the Act, to reflect the probable intent of Congress.

AMENDMENTS

2022—Subsec. (f). Pub. L. 117–263 added subsec. (f) and struck out former subsec. (f) which defined cybersecurity risk, industrial control system, and information system.

§ 665j. Ransomware threat mitigation activities

(a) Joint Ransomware Task Force

(1) In general

Not later than 180 days after March 15, 2022, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) Composition

The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) Responsibilities

The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify[1] metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

(b) Rule of construction

Nothing in this section shall be construed to provide any additional authority to any Federal agency.

(Pub. L. 117–103, div. Y, § 106, Mar. 15, 2022, 136 Stat. 1056.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and also

[1] So in original.

as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Statutory Notes and Related Subsidiaries

DEFINITIONS

Pub. L. 117–103, div. Y, §102, Mar. 15, 2022, 136 Stat. 1038, provided that: ''In this division [see Short Title of 2022 Amendment note set out under section 101 of this title]:

''(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms 'covered cyber incident', 'covered entity', 'cyber incident', 'information system', 'ransom payment', 'ransomware attack', and 'security vulnerability' have the meanings given those terms in section 2240 of the Homeland Security Act of 2002 [6 U.S.C. 681], as added by section 103 of this division [see also 6 U.S.C. 650].

''(2) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.''

§ 665k. Federal Clearinghouse on School Safety Evidence-based Practices

(a) Establishment

(1) In general

The Secretary, in coordination with the Secretary of Education, the Attorney General, and the Secretary of Health and Human Services, shall establish a Federal Clearinghouse on School Safety Evidence-based Practices (in this section referred to as the ''Clearinghouse'') within the Department.

(2) Purpose

The Clearinghouse shall serve as a Federal resource to identify and publish online through SchoolSafety.gov, or any successor website, evidence-based practices and recommendations to improve school safety for use by State and local educational agencies, institutions of higher education, State and local law enforcement agencies, health professionals, and the general public.

(3) Personnel

(A) Assignments

The Clearinghouse shall be assigned such personnel and resources as the Secretary considers appropriate to carry out this section.

(B) Detailees

The Secretary of Education, the Attorney General, and the Secretary of Health and Human Services may detail personnel to the Clearinghouse.

(4) Exemptions

(A) Paperwork Reduction Act

Chapter 35 of title 44 (commonly known as the ''Paperwork Reduction Act''), shall not apply to any rulemaking or information collection required under this section.

(B) Federal Advisory Committee Act

The Federal Advisory Committee Act (5 U.S.C. App.)[1] shall not apply for the purposes of carrying out this section.

(b) Clearinghouse contents

(1) Consultation

In identifying the evidence-based practices and recommendations for the Clearinghouse, the Secretary shall—

(A) consult with appropriate Federal, State, local, Tribal, private sector, and nongovernmental organizations, including civil rights and disability rights organizations; and

(B) consult with the Secretary of Education to ensure that evidence-based practices published by the Clearinghouse are aligned with evidence-based practices to support a positive and safe learning environment for all students.

(2) Criteria for evidence-based practices and recommendations

The evidence-based practices and recommendations of the Clearinghouse shall—

(A) include comprehensive evidence-based school safety measures;

(B) include the evidence or research rationale supporting the determination of the Clearinghouse that the evidence-based practice or recommendation under subparagraph (A) has been shown to have a significant effect on improving the health, safety, and welfare of persons in school settings, including—

(i) relevant research that is evidence-based, as defined in section 7801 of title 20, supporting the evidence-based practice or recommendation;

(ii) findings and data from previous Federal or State commissions recommending improvements to the safety posture of a school; or

(iii) other supportive evidence or findings relied upon by the Clearinghouse in determining evidence-based practices and recommendations, as determined in consultation with the officers described in subsection (a)(3)(B);

(C) include information on Federal programs for which implementation of each evidence-based practice or recommendation is an eligible use for the program;

(D) be consistent with Federal civil rights laws, including title II of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.); and

(E) include options for developmentally appropriate recommendations for use in educational settings with respect to children's ages and physical, social, sensory, and emotionally developmental statuses.

(3) Past commission recommendations

The Clearinghouse shall present, as determined in consultation with the officers described in subsection (a)(3)(B), Federal, State, local, Tribal, private sector, and nongovernmental organization issued best practices and recommendations and identify any best practice or recommendation of the Clearinghouse that was previously issued by any such organization or commission.

[1] See References in Text note below.