§ 665h. National Cyber Exercise Program

(a) Establishment of program

(1) In general

There is established in the Agency the National Cyber Exercise Program (referred to in this section as the ''Exercise Program'') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) Requirements

(A) In general

The Exercise Program shall be—

(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(B) Model exercise selection

The Exercise Program shall—

(i) include a selection of model exercises that government and private entities can readily adapt for use; and

(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) Consultation

In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

(b) Definitions

In this section:

(1) State

The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) Private entity

The term ''private entity'' has the meaning given such term in section 1501 of this title.

(c) Rule of construction

Nothing in this section shall be construed to affect the authorities or responsibilities of the Administrator of the Federal Emergency Management Agency pursuant to section 748 of this title.

(Pub. L. 107–296, title XXII, § 2220B, as added Pub. L. 117–81, div. A, title XV, § 1547(a), Dec. 27, 2021, 135 Stat. 2059.)

§ 665i. CyberSentry program

(a) Establishment

There is established in the Agency a program, to be known as ''CyberSentry'', to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, upon request and subject to the consent of such owner or operator.

(b) Activities

The Director, through CyberSentry, shall—

(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such owner or operator;

(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such vulnerabilities;

(4) produce aggregated, anonymized analytic products, based on threat hunting and continuous monitoring and detection activities and partnerships, with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022.

(c) Privacy review

Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency under section 652(h) of this title shall—

(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

(2) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and

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

(d) Report to Congress

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

(e) Savings

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

(f) Definition

In this section, the term ''industrial control system'' means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (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.