

(A) the grant selection process of the Secretary; and

(B) a sample of grants awarded under this section.

**(r) Authorization of appropriations**

**(1) In general**

There are authorized to be appropriated for activities under this section—

(A) for fiscal year 2022, \$200,000,000;

(B) for fiscal year 2023, \$400,000,000;

(C) for fiscal year 2024, \$300,000,000; and

(D) for fiscal year 2025, \$100,000,000.

**(2) Transfers authorized**

**(A) In general**

During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to paragraph (1) or other amounts appropriated to carry out the State and Local Cybersecurity Grant Program for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.

**(B) Additional appropriations**

Any funds transferred under subparagraph (A) shall be in addition to any funds appropriated to the Department or the components described in subparagraph (A) for salaries, expenses, and other administrative costs.

**(s) Termination**

**(1) In general**

Subject to paragraph (2), the requirements of this section shall terminate on September 30, 2025.

**(2) Exception**

The reporting requirements under subsection (q) shall terminate on the date that is 1 year after the date on which the final funds from a grant under this section are expended or returned.

(Pub. L. 107–296, title XXII, § 2220A, formerly § 2218, as added Pub. L. 117–58, div. G, title VI, § 70612(a), Nov. 15, 2021, 135 Stat. 1272; renumbered § 2220A and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(viii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(K), Dec. 23, 2022, 136 Stat. 3660.)

**Editorial Notes**

**REFERENCES IN TEXT**

The Food and Nutrition Act of 2008, referred to in subsec. (m)(2)(C)(ii), is Pub. L. 88–525, Aug. 31, 1964, 78 Stat. 703, which is classified generally to chapter 51 (§ 2011 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 7 and Tables.

**AMENDMENTS**

2022—Subsec. (a). Pub. L. 117–263, § 7143(b)(2)(K)(i), redesignated pars. (3), (4), and (8) to (12) as pars. (1) to (7), respectively, and struck out former pars. (1), (2), and (5)

to (7) which defined appropriate committees of Congress, cyber threat indicator, incident, information sharing and analysis organization, and information system, respectively.

Subsec. (e)(2)(B)(xiv)(II)(aa). Pub. L. 117–263, § 7143(b)(2)(K)(ii), substituted “Information Sharing and Analysis Organization” for “information sharing and analysis organization”.

Subsec. (p). Pub. L. 117–263, § 7143(b)(2)(K)(iii), substituted “appropriate congressional committees” for “appropriate committees of Congress”.

Subsec. (q)(4)(A). Pub. L. 117–263, § 7143(b)(2)(K)(iv), which directed amendment of subsec. (q)(4) by substituting “appropriate congressional committees” for “appropriate committees of Congress” “in the matter preceding clause (i)”, was executed by making the substitution in the introductory provisions of subsec. (q)(4)(A), to reflect the probable intent of Congress.

2021—Pub. L. 117–81 reenacted section catchline.

**§ 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 Di-

rector, 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 contin-

uous 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 (DCSSs), 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