

(E) Monetary and nonmonetary awards for competition participants, including members of the uniformed services, subject to subsection (f).

(2) Application

This subsection shall apply to amounts appropriated on or after December 23, 2022.

(f) Prize limitation

(1) Awards by the Director

The Director may make one or more awards per competition, except that the amount or value of each shall not exceed \$10,000.

(2) Awards by the Secretary of Homeland Security

The Secretary of Homeland Security may make one or more awards per competition, except the amount or the value of each shall not exceed \$25,000.

(3) Regular pay

A monetary award under this section shall be in addition to the regular pay of the recipient.

(4) Overall yearly award limit

The total amount or value of awards made under this Act¹ during a fiscal year may not exceed \$100,000.

(g) Reporting requirements

The Director shall annually 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 report that includes the following with respect to each competition conducted in the preceding year:

- (1) A description of available amounts.
- (2) A description of authorized expenditures.
- (3) Information relating to participation.
- (4) Information relating to lessons learned, and how such lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(Pub. L. 117–263, div. G, title LXXI, § 7121, Dec. 23, 2022, 136 Stat. 3638.)

Editorial Notes

REFERENCES IN TEXT

This Act, referred to in subsec. (f)(4), is Pub. L. 117–263, Dec. 23, 2022, 136 Stat. 2395, known as the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, but probably means H.R. 6824, 117th Cong., 2d Sess. (as reported to the Senate), known as the President's Cup Cybersecurity Competition Act, which consisted only of the section containing the short title and this section. The reference to “this Act” from the original was not updated when the text of H.R. 6824 was incorporated into Pub. L. 117–263.

CODIFICATION

Section was enacted as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

¹ So in original. Probably should refer to “this section”. See References in Text note below.

§ 665n. Industrial Control Systems Cybersecurity Training Initiative

(a) Establishment

(1) In general

The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the “Initiative”) is established within the Agency.

(2) Purpose

The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

(b) Requirements

In carrying out the Initiative, the Director shall—

- (1) ensure the Initiative includes—

(A) virtual and in-person trainings and courses provided at no cost to participants;

(B) trainings and courses available at different skill levels, including introductory level courses;

(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and

(D) appropriate consideration regarding the availability of trainings and courses in different regions of the United States; and¹

- (2) engage in—

(A) collaboration with the National Laboratories of the Department of Energy in accordance with section 189 of this title;

(B) consultation with Sector Risk Management Agencies;²

(C) as appropriate, consultation with private sector entities with relevant expertise, such as vendors of industrial control systems technologies; and

(3) consult, to the maximum extent practicable, with commercial training providers and academia to minimize the potential for duplication of other training opportunities.

(c) Reports

(1) In general

Not later than one year after December 23, 2022, and annually thereafter, the Director 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 Initiative.

(2) Contents

Each report submitted under paragraph (1) shall include the following:

(A) A description of the courses provided under the Initiative.

(B) A description of outreach efforts to raise awareness of the availability of such courses.

¹ So in original. The word “and” probably should not appear.

² So in original. Probably should be followed by “and”.

(C) The number of participants in each course.

(D) Voluntarily provided information on the demographics of participants in such courses, including by sex, race, and place of residence.

(E) Information on the participation in such courses of workers from each critical infrastructure sector.

(F) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

(G) Recommendations regarding how to strengthen the state of industrial control systems cybersecurity education and training.

(Pub. L. 107–296, title XXII, §2220E, as added Pub. L. 117–263, div. G, title LXXI, §7122(a), Dec. 23, 2022, 136 Stat. 3640.)

PART B—CRITICAL INFRASTRUCTURE INFORMATION

Editorial Notes

CODIFICATION

Subtitle B of title XXII of Pub. L. 107–296, comprising this part, was originally added as subtitle B of title II of Pub. L. 107–296, and was classified to part B (§131 et seq.) of subchapter II of this chapter. Subtitle B of title II of Pub. L. 107–296 was subsequently redesignated subtitle B of title XXII of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.

§ 671. Definitions

In this part:

(1) Agency

The term “agency” has the meaning given it in section 551 of title 5.

(2) Covered Federal agency

The term “covered Federal agency” means the Department of Homeland Security.

(3) Critical infrastructure information

The term “critical infrastructure information” has the meaning given the term in section 650 of this title.

(4) Critical infrastructure protection program

The term “critical infrastructure protection program” means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) Protected system

The term “protected system”—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing

instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(6) Voluntary

(A) In general

The term “voluntary”, in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency’s exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) Exclusions

The term “voluntary”—

(i) in the case of any action brought under the securities laws as is defined in section 78c(a)(47) of title 15—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 78l(i) of title 15; and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(Pub. L. 107–296, title XXII, §2222, formerly title II, §212, Nov. 25, 2002, 116 Stat. 2150; Pub. L. 114–113, div. N, title II, §204, Dec. 18, 2015, 129 Stat. 2961; renumbered title XXII, §2222, and amended Pub. L. 115–278, §2(g)(2)(H), (9)(B)(i), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–263, div. G, title LXXI, §7143(b)(2)(M), Dec. 23, 2022, 136 Stat. 3661.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 131 of this title prior to renumbering by Pub. L. 115–278.

AMENDMENTS

2022—Par. (3). Pub. L. 117–263, §7143(b)(2)(M)(i), added par. (3) and struck out former par. (3) which defined critical infrastructure information.

Pars. (5) to (8). Pub. L. 117–263, §7143(b)(2)(M)(ii), (iii), redesignated pars. (6) and (7) as (5) and (6), respectively, and struck out former pars. (5) and (8) which defined Information Sharing and Analysis Organization and cybersecurity risk and incident, respectively.

2018—Par. (8). Pub. L. 115–278, §2(g)(9)(B)(i), substituted “section 659 of this title” for “section 148 of this title”.

2015—Par. (5)(A). Pub. L. 114–113, §204(1)(A), inserted “, including information related to cybersecurity risks and incidents,” after “critical infrastructure information” and “, including cybersecurity risks and incidents,” after “related to critical infrastructure”.

Par. (5)(B). Pub. L. 114–113, §204(1)(B), inserted “, including cybersecurity risks and incidents,” after