''(3) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.);

''(4) title IX of the Education Amendments of 1972 (20 U.S.C. 1681 et seq.); or

''(5) the Age Discrimination Act of 1975 (42 U.S.C. 6101 et seq.).

''(b) PROHIBITION ON FEDERALLY DEVELOPED, MANDATED, OR ENDORSED CURRICULUM.—Nothing in this subtitle or the amendments made by this subtitle shall be construed to authorize any officer or employee of the Federal Government to engage in an activity otherwise prohibited under section 103(b) of the Department of Education Organization Act (20 U.S.C. 3403(b)).''

§ 665*l*. School and daycare protection

(a) In general

Not later than 180 days after December 23, 2022, and annually thereafter, the Secretary of Homeland Security 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 regarding the following:

(1) The Department of Homeland Security's activities, policies, and plans to enhance the security of early childhood education programs, elementary schools, and secondary schools during the preceding year that includes information on the Department's activities through the Federal School Safety Clearinghouse.

(2) Information on all structures or efforts within the Department intended to bolster coordination among departmental components and offices involved in carrying out paragraph (1) and, with respect to each structure or effort, specificity on which components and offices are involved and which component or office leads such structure or effort.

(3) A detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out these activities.

(b) Briefing

Not later than 30 days after the submission of each report required under subsection (a), the Secretary of Homeland Security shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing regarding such report and the status of efforts to carry out plans included in such report for the preceding year.

(c) Definitions

In this section, the terms ''early childhood education program'', ''elementary school'', and ''secondary school'' have the meanings given such terms in section 7801 of title 20.

(Pub. L. 117–263, div. G, title LXXI, § 7103, Dec. 23, 2022, 136 Stat. 3621.)

Editorial Notes

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.

§ 665m. President's Cup Cybersecurity Competition

(a) In general

The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the ''Director'') of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the ''Department of Homeland Security Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition'' (in this section referred to as the ''competition'') for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

(b) Eligibility

To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5) and shall comply with any rules promulgated by the Director regarding the competition.

(c) Competition administration

The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(d) Competition parameters

Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraphs (1), (2), or (3), as determined necessary by the Director.

(e) Use of funds

(1) In general

In order to further the goals and objectives of the competition, the Director may use amounts made available to the Director for the competition for reasonable expenses for the following:

(A) Advertising, marketing, and promoting the competition.

(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition.

(C) Promotional items, including merchandise and apparel.

(D) Consistent with section 4503 of title 5, necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(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 Act[1] 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; and[1]

(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''.