(C) Reappointment

A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) Prohibition on compensation

The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) Meetings

(A) In general

The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) Public meetings

At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) Attendance

The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) Member access to classified information

(A) In general

Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted from reviewing, discussing, or possessing classified information.

(B) Access

Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) Protections

A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) Rule of construction

Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) Chairperson

The Advisory Committee shall select, from among the members of the Advisory Committee—

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) Subcommittees

(1) In general

The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

(2) Meetings and reporting

Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) Subject matter experts

The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

(Pub. L. 107–296, title XXII, § 2219, formerly § 2216, as added Pub. L. 116–283, div. A, title XVII, § 1718(a), Jan. 1, 2021, 134 Stat. 4102; renumbered § 2219 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(vi), Dec. 27, 2021, 135 Stat. 2061.)

Editorial Notes

REFERENCES IN TEXT

The date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, referred to in subsec. (c)(1)(A), probably means the date of enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116–283, which was approved Jan. 1, 2021. No act named the Cybersecurity Advisory Committee Authorization Act of 2020 has been enacted. However, a bill, S. 4024, entitled ''Cybersecurity Advisory Committee Authorization Act of 2020'' was introduced to Senate on June 22, 2020.

Executive Order No. 13526, referred to in subsec. (c)(5)(B), is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, set out as a note under section 3161 of Title 50, War and National Defense.

AMENDMENTS

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

§ 665f. Cybersecurity education and training programs

(a) Establishment

(1) In general

The Cybersecurity Education and Training Assistance Program (referred to in this section as ''CETAP'') is established within the Agency.

(2) Purpose

The purpose of CETAP shall be to support the effort of the Agency in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

(A) providing foundational cybersecurity awareness and literacy;

(B) encouraging cybersecurity career exploration; and

(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) Requirements

In carrying out CETAP, the Director shall—

(1) ensure that the program—

(A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

(D) provides direct student engagement opportunities through camps and other programming;

(E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(F) integrates with existing post-secondary education and workforce development programs at the Department;

(G) promotes and supports national standards for elementary and secondary cyber education;

(H) partners with cybersecurity and education stakeholder groups to expand outreach; and

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

(2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) Briefings

(1) In general

Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) Contents

Each briefing conducted under paragraph (1) shall include—

(A) estimated figures on the number of students reached and teachers engaged;

(B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);

(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;

(D) information on new curricula offerings and teacher training platforms; and

(E) information on coordination with post-secondary education and workforce development programs at the Department.

(d) Mission promotion

The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

(e) Grants and cooperative agreements

The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 1001 of title 20), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

(1) carry out the purposes of CETAP; and

(2) enhance CETAP to address the national shortfall of cybersecurity professionals.

(Pub. L. 107–296, title XXII, § 2220, formerly § 2217, as added Pub. L. 116–283, div. A, title XVII, § 1719(c), Jan. 1, 2021, 134 Stat. 4106; renumbered § 2220 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(vii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7104, Dec. 23, 2022, 136 Stat. 3622.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c)(2)(C) to (E). Pub. L. 117–263, § 7104(b), added subpar. (C) and redesignated former subpars. (C) and (D) as (D) and (E), respectively.

Subsec. (e). Pub. L. 117–263, § 7104(a), added subsec. (e).

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

§ 665g. State and Local Cybersecurity Grant Program

(a) Definitions

In this section:

(1) Cybersecurity Plan

The term ''Cybersecurity Plan'' means a plan submitted by an eligible entity under subsection (e)(1).

(2) Eligible entity

The term ''eligible entity'' means a—

(A) State; or

(B) Tribal government.

(3) Multi-entity group

The term ''multi-entity group'' means a group of 2 or more eligible entities desiring a grant under this section.

(4) Online service

The term ''online service'' means any internet-facing service, including a website, email, virtual private network, or custom application.

(5) Rural area

The term ''rural area'' has the meaning given the term in section 5302 of title 49.

(6) State and Local Cybersecurity Grant Program

The term ''State and Local Cybersecurity Grant Program'' means the program established under subsection (b).

(7) Tribal government

The term ''Tribal government'' means the recognized governing body of any Indian or