(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 new curricula offerings and teacher training platforms; and

(D) 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.

(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.)

Editorial Notes

AMENDMENTS

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

§ 665g. State and Local Cybersecurity Grant Program

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(2) Cyber threat indicator

The term ''cyber threat indicator'' has the meaning given the term in section 1501 of this title.

(3) Cybersecurity Plan

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

(4) Eligible entity

The term ''eligible entity'' means a—

(A) State; or

(B) Tribal government.

(5) Incident

The term ''incident'' has the meaning given the term in section 659 of this title.

(6) Information sharing and analysis organization

The term ''information sharing and analysis organization'' has the meaning given the term in section 671 of this title.

(7) Information system

The term ''information system'' has the meaning given the term in section 1501 of this title.

(8) Multi-entity group

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

(9) Online service

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

(10) Rural area

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

(11) State and Local Cybersecurity Grant Program

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

(12) Tribal government

The term ''Tribal government'' means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 5131 of title 25.

(b) Establishment

(1) In general

There is established within the Department a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments.

(2) Application

An eligible entity desiring a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(c) Administration

The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 604 and 605 of this title.

(d) Use of funds

An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate, shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity;

(3) pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;

(4) assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or

(5) fund any other appropriate activity determined by the Secretary, acting through the Director.

(e) Cybersecurity plans

(1) In general

An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for review in accordance with subsection (i).

(2) Required elements

A Cybersecurity Plan of an eligible entity shall—