(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, §2216, as added Pub. L. 116–283, div. A, title XVII, §1718(a), Jan. 1, 2021, 134 Stat. 4102.)

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.

§ 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, § 2217, as added Pub. L. 116–283, div. A, title XVII, § 1719(c), Jan. 1, 2021, 134 Stat. 4106.)

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'' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(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) Information Sharing and Analysis Organization

The term ''Information Sharing and Analysis Organization'' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a[1] interference, compromise, or a[2] incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) 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.

(7) 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—

[1] So in original. Probably should be ''an''.

[2] So in original. The word ''a'' probably should not appear.