guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of such sector and authorities under applicable law to—

(1) support sector risk management, in coordination with the Director, including—

(A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

(B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

(2) assess sector risk, in coordination with the Director, including—

(A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

(B) supporting national risk assessment efforts led by the Department;

(3) sector coordination, including—

(A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

(B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

(C) participating in cross-sector coordinating councils, as appropriate;

(4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

(A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through Information Sharing and Analysis Organizations and the national cybersecurity and communications integration center established pursuant to section 659 of this title;

(B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(5) supporting incident management, including—

(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

(6) contributing to emergency preparedness efforts, including—

(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

(B) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and

(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.

(Pub. L. 107–296, title XXII, § 2218, formerly § 2215, as added Pub. L. 116–283, div. H, title XC, § 9002(c)(1), Jan. 1, 2021, 134 Stat. 4770; renumbered § 2218 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(v), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(J), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2218 of Pub. L. 107–296 was renumbered section 2220A and is classified to section 665g of this title.

AMENDMENTS

2022—Subsec. (c)(4)(A). Pub. L. 117–263 substituted ''Information Sharing and Analysis Organizations'' for ''information sharing and analysis organizations''.

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

§ 665e. Cybersecurity Advisory Committee

(a) Establishment

The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the ''Advisory Committee'').

(b) Duties

(1) In general

The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) Recommendations

(A) In general

The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) Recommendations of subcommittees

Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) Periodic reports

The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) Annual report

(A) In general

The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) Publication

Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5.

(5) Feedback

Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) Congressional notification

Not less frequently than once per year after January 1, 2021, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) Governance rules

The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) Membership

(1) Appointment

(A) In general

Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020,[1] the Director shall appoint the members of the Advisory Committee.

(B) Composition

The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) Representation

(i) In general

The membership of the Advisory Committee shall satisfy the following criteria:

(I) Consist of subject matter experts.

(II) Be geographically balanced.

(III) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(aa) Defense.

(bb) Education.

(cc) Financial services and insurance.

(dd) Healthcare.

(ee) Manufacturing.

(ff) Media and entertainment.

(gg) Chemicals.

(hh) Retail.

(ii) Transportation.

(jj) Energy.

(kk) Information Technology.

(*ll*) Communications.

(mm) Other relevant fields identified by the Director.

(ii) Prohibition

Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) Publication of membership list

The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) Term of office

(A) Terms

The term of each member of the Advisory Committee shall be two years, except that a member may continue to serve until a successor is appointed.

(B) Removal

The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

[1] See References in Text note below.

(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