cybersecurity purpose.'' for ''section:'' and struck out pars. (1) to (4) which defined cyber defense operation, cybersecurity purpose, cybersecurity risk, incident, and information sharing and analysis organization.

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

§ 665c. Cybersecurity State Coordinator

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(c) Feedback

The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(Pub. L. 107–296, title XXII, § 2217, formerly § 2215, as added Pub. L. 116–283, div. A, title XVII, § 1717(a)(1)(B), Jan. 1, 2021, 134 Stat. 4099; renumbered § 2217 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(iv), Dec. 27, 2021, 135 Stat. 2061.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2217 of Pub. L. 107–296 was renumbered section 2220 and is classified to section 665f of this title.

AMENDMENTS

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

Statutory Notes and Related Subsidiaries

RULE OF CONSTRUCTION

Pub. L. 116–283, div. A, title XVII, § 1717(a)(4), Jan. 1, 2021, 134 Stat. 4100, provided that: ''Nothing in this subsection [enacting this section, amending section 652 of this title, and enacting provisions set out as a note below] or the amendments made by this subsection may be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents.''

COORDINATION PLAN

Pub. L. 116–283, div. A, title XVII, § 1717(a)(2), Jan. 1, 2021, 134 Stat. 4100, provided that: ''Not later than 60 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall establish and submit to the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security in the House of Representatives a plan describing the reporting structure and coordination processes and procedures of Cybersecurity State Coordinators within the Cybersecurity and Infrastructure Security Agency under section 2215 of the Homeland Security Act of 2002 [Pub. L. 107–296], as added by paragraph (1)(B) [6 U.S.C. 665c].''

§ 665d. Sector Risk Management Agencies

(a) In general

Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

(1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and

(2) support programs and associated activities of such sector or subsector of such sector.

(b) Implementation

In carrying out this section, Sector Risk Management Agencies shall—

(1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

(2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

(3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(c) Responsibilities

Consistent with applicable law, Presidential directives, Federal regulations, and strategic

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.