6 USCS § 665d

Current through Public Law 118-62, approved May 13, 2024.

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 1. HOMELAND SECURITY ORGANIZATION (§§ 101 — 681g) > CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (§§ 650 — 681g) > CYBERSECURITY AND INFRASTRUCTURE SECURITY (§§ 651 — 665n)

§ 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 [6 USCS §§ 651 et seq.];

(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 2209 [6 USCS § 659];

(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.

History

Nov. 25, 2002, P. L. 107-296, Title XXII, Subtitle A, § 2218 [2215], as added Jan. 1, 2021, P.L. 116-283, Div H, Title XC, § 9002(c)(1), 134 Stat. 4770; Dec. 27, 2021, P.L. 117-81, Div A, Title XV, Subtitle C, § 1547(b)(1)(A)(v), 135 Stat. 2061; Dec. 23, 2022, P.L. 117-263, Div G, Title LXXI, Subtitle E, § 7143(b)(2)(J), 136 Stat. 3660.

End of Document