6 USCS § 665b

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)

§ 665b. Joint cyber planning office

(a) Establishment of Office. There is established in the Agency an office for joint cyber planning (in this section referred to as the "Office") to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) Planning and execution. In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

(1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;

(2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;

(3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(4) ensure that plans for cyber defense operations, as appropriate, are responsive to potential adversary activity conducted in response to United States offensive cyber operations;

(5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

(7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) Composition. The Office shall be composed of—

(1) a central planning staff; and

(2) appropriate representatives of Federal departments and agencies, including—

(A) the Department;

(B) United States Cyber Command;

(C) the National Security Agency;

(D) the Federal Bureau of Investigation;

(E) the Department of Justice; and

(F) the Office of the Director of National Intelligence.

(d) Consultation. In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

(1) State, local, federally-recognized Tribal, and territorial governments;

(2) Information Sharing and Analysis Organizations, including information sharing and analysis centers;

(3) owners and operators of critical information systems;

(4) private entities; and

(5) other appropriate representatives or entities, as determined by the Secretary.

(e) Interagency agreements. The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) Definitions. In this section, the term "cyber defense operation" means the defensive activities performed for a cybersecurity purpose.

History

Nov. 25, 2002, P. L. 107-296, Title XXII, Subtitle A, § 2216 [2215], as added Jan. 1, 2021, P.L. 116-283, Div A, Title XVII, § 1715(a), 134 Stat. 4092; Dec. 27, 2021, P.L. 117-81, Div A, Title XV, Subtitle C, § 1547(b)(1)(A)(iii), 135 Stat. 2061; Dec. 23, 2022, P.L. 117-263, Div G, Title LXXI, Subtitle E, § 7143(b)(2)(I), 136 Stat. 3660.