6 USCS § 1500

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

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 6. CYBERSECURITY (§§ 1500 — 1534) > CYBERSECURITY INFORMATION SHARING (§§ 1500 — 1510)

§ 1500. National Cyber Director

(a) Establishment. There is established, within the Executive Office of the President, the Office of the National Cyber Director (in this section referred to as the "Office").

(b) National Cyber Director.

(1) In general. The Office shall be headed by the National Cyber Director (in this section referred to as the "Director") who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) Position. The Director shall hold office at the pleasure of the President.

(3) Pay and allowances. The Director shall be entitled to receive the same pay and allowances as are provided for level II of the Executive Schedule under section 5313 of title 5, United States Code.

(c) Duties of the National Cyber Director.

(1) In general. Subject to the authority, direction, and control of the President, the Director shall—

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of—

(i) information security and data protection;

(ii) programs and policies intended to improve the cybersecurity posture of the United States;

(iii) efforts to understand and deter malicious cyber activity;

(iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

(vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and

(vii) such other cybersecurity matters as the President considers appropriate;

(B) offer advice and consultation to the National Security Council and its staff, the Homeland Security Council and its staff, and relevant Federal departments and agencies, for their consideration, relating to the development and coordination of national cyber policy and strategy, including the National Cyber Strategy;

(C) lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy, by—

(i) in coordination with the heads of relevant Federal departments or agencies, monitoring and assessing the effectiveness, including cost-effectiveness, of the implementation of such national cyber policy and strategy by Federal departments and agencies;

(ii) making recommendations, relevant to changes in the organization, personnel, and resource allocation and to policies of Federal departments and agencies, to the heads of relevant Federal departments and agencies in order to implement such national cyber policy and strategy;

(iii) reviewing the annual budget proposals for relevant Federal departments and agencies and advising the heads of such departments and agencies whether such proposals are consistent with such national cyber policy and strategy;

(iv) continuously assessing and making relevant recommendations to the President on the appropriate level of integration and interoperability across the Federal cyber centers;

(v) coordinating with the Attorney General, the Federal Chief Information Officer, the Director of the Office of Management and Budget, the Director of National Intelligence, and the Director of the Cybersecurity and Infrastructure Security Agency, on the streamlining of Federal policies and guidelines, including with respect to implementation of subchapter II of chapter 35 of title 44, United States Code [44 USCS §§ 3531 et seq.], and, as appropriate or applicable, regulations relating to cybersecurity;

(vi) reporting annually to the President, the Assistant to the President for National Security Affairs, and Congress on the state of the cybersecurity posture of the United States, the effectiveness of such national cyber policy and strategy, and the status of the implementation of such national cyber policy and strategy by Federal departments and agencies; and

(vii) such other activity as the President considers appropriate to further such national cyber policy and strategy;

(D) lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, including—

(i) ensuring and facilitating coordination among relevant Federal departments and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response, that feature—

(I) clear lines of authority and lines of effort across the Federal Government;

(II) authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government; and

(III) support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States;

(ii) ensuring the exercising of defensive operational plans, processes, and playbooks for incident response;

(iii) ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and

(iv) reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private sector entities, as appropriate;

(E) preparing the response by the Federal Government to cyberattacks and cyber campaigns of significant consequence across Federal departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private sector entities, including—

(i) developing for the approval of the President, in coordination with the Assistant to the President for National Security Affairs and the heads of relevant Federal departments and agencies, operational priorities, requirements, and plans;

(ii) ensuring incident response is executed consistent with the plans described in clause (i); and

(iii) ensuring relevant Federal department and agency consultation with relevant private sector entities in incident response;

(F) coordinate and consult with private sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate;

(G) annually report to Congress on cybersecurity threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law; and

(H) be responsible for such other functions as the President may direct.

(2) Delegation of authority.

(A) The Director may—

(i) serve as the senior representative to any organization that the President may establish for the purpose of providing the President advice on cybersecurity;

(ii) subject to subparagraph (B), be included as a participant in preparations for and, when appropriate, the execution of domestic and international summits and other international meetings at which cybersecurity is a major topic;

(iii) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate; and

(iv) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate.

(B) In acting under subparagraph (A)(ii) in the case of a summit or a meeting with an international partner, the Director shall act in coordination with the Secretary of State.

(d) [Omitted]

(e) Powers of the Director.

(1) In general. The Director may, for the purposes of carrying out the functions of the Director under this section—

(A) subject to the civil service and classification laws, select, appoint, employ, and fix the compensation of such officers and employees as are necessary and prescribe their duties, except that not more than 75 individuals may be employed without regard to any provision of law regulating the employment or compensation at rates not to exceed the basic rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5, United States Code;

(B) employ experts and consultants in accordance with section 3109 of title 5, United States Code, and compensate individuals so employed for each day (including travel time) at rates not in excess of the maximum rate of basic pay for grade GS-15 as provided in section 5332 of such title [5 USCS § 5332], and while such experts and consultants are so serving away from their homes or regular place of business, to pay such employees travel expenses and per diem in lieu of subsistence at rates authorized by section 5703 of such title 5 [5 USCS § 5703] for persons in Federal Government service employed intermittently;

(C) accept officers or employees of the United States or members of the Armed Forces on a detail from an element of the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) or from another element of the Federal Government on a nonreimbursable basis, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed three years;

(D) promulgate such rules and regulations as may be necessary to carry out the functions, powers, and duties vested in the Director;

(E) utilize, with their consent, the services, personnel, and facilities of other Federal agencies;

(F) enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary in the conduct of the work of the Office and on such terms as the Director may determine appropriate, with any Federal agency, or with any public or private person or entity;

(G) accept voluntary and uncompensated services, notwithstanding the provisions of section 1342 of title 31, United States Code;

(H) adopt an official seal, which shall be judicially noticed; and

(I) provide, where authorized by law, copies of documents to persons at cost, except that any funds so received shall be credited to, and be available for use from, the account from which expenditures relating thereto were made.

(2) Rules of construction regarding details. Nothing in paragraph (1)(C) may be construed as imposing any limitation on any other authority for reimbursable or nonreimbursable details. A nonreimbursable detail made pursuant to such paragraph shall not be considered an augmentation of the appropriations of the receiving element of the Office of the National Cyber Director.

(f) Rules of construction. Nothing in this section may be construed as—

(1) modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency;

(2) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation;

(3) amending a legal restriction that was in effect on the day before the date of the enactment of this Act [enacted Jan. 1, 2021] that requires a law enforcement agency to keep confidential information learned in the course of a criminal or national security investigation;

(4) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a military operation;

(5) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct any diplomatic or consular activity;

(6) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct an intelligence activity, resource, or operation; or

(7) authorizing the Director or any person acting under the authority of the Director to modify the classification of intelligence information.

(g) Definitions. In this section:

(1) The term "cybersecurity posture" means the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or cyber campaign of significant consequence.

(2) The term "cyber attack and cyber campaign of significant consequence" means an incident or series of incidents that has the purpose or effect of—

(A) causing a significant disruption to the confidentiality, integrity, or availability of a Federal information system;

(B) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(C) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) otherwise constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

(3) The term "incident" has the meaning given such term in section 3552 of title 44, United States Code.

(4) The term "incident response" means a government or private sector activity that detects, mitigates, or recovers from a cyber attack or cyber campaign of significant consequence.

(5) The term "information security" has the meaning given such term in section 3552 of title 44, United States Code.

(6) The term "intelligence" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

History

Jan. 1, 2021, P.L. 116-283, Div A, Title XVII, § 1752, 134 Stat. 4149; Dec. 27, 2021, P.L. 117-81, Div A, Title XV, Subtitle C, § 1552, 135 Stat. 2070.