

cies and subdivisions related to cybersecurity that have a primary function of intelligence, counterintelligence, investigative, or national security work, including descriptions of such functions. The Director of OMB shall provide this list to the President, through the Deputy Assistant to the President for Homeland Security and Counterterrorism (DAPHSCT), every year starting September 1, 2019, for consideration of whether those agencies or subdivisions should be exempted from coverage under the Federal Labor-Management Relations Program, consistent with the requirements of section 7103(b)(1) of title 5, United States Code.

SEC. 3. *Strengthening the Nation's Cybersecurity Workforce.* (a) The Secretary of Commerce and the Secretary of Homeland Security (Secretaries), in coordination with the Secretary of Education and the heads of other agencies as the Secretaries determine is appropriate, shall execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (Workforce Report) developed pursuant to Executive Order 13800. The Secretaries shall develop a consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce. To fulfill the Workforce Report's vision of preparing, growing, and sustaining a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity, priority consideration will be given to the following imperatives:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

(b) To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly cyber-physical systems for which safety and reliability depend on secure control systems, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Secretary of Homeland Security, in coordination with the Director of OPM and the Secretary of Labor, shall provide a report to the President, through the DAPHSCT, within 180 days of the date of this order that:

(i) Identifies and evaluates skills gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense's platform information technologies; and

(ii) Recommends curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

(c) Within 1 year of the date of this order, the Secretary of Education, in consultation with the DAPHSCT and the National Science Foundation, shall develop and implement, consistent with applicable law, an annual Presidential Cybersecurity Education Award to be presented to one elementary and one secondary school educator per year who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects. In developing and implementing this award, the Secretary of Education shall emphasize demonstrated superior educator ac-

complishment—without respect to research, scholarship, or technology development—as well as academic achievement by the educator's students.

(d) The Secretary of Commerce, the Secretary of Labor, the Secretary of Education, the Secretary of Homeland Security, and the heads of other appropriate agencies shall encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law. The Secretary of Commerce shall provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

SEC. 4. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

SUBCHAPTER I—CYBERSECURITY INFORMATION SHARING

§ 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.

(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, 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 se-

curity, 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;

(B) employ experts and consultants in accordance with section 3109 of title 5, 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, 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 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 3003(4) of title 50) 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;

(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 January 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.

(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.

(6) The term “intelligence” has the meaning given such term in section 3003 of title 50.

(Pub. L. 116–283, div. A, title XVII, §1752, Jan. 1, 2021, 134 Stat. 4144; Pub. L. 117–81, div. A, title XV, §1552, Dec. 27, 2021, 135 Stat. 2070.)

Editorial Notes

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Cybersecurity Information Sharing Act of 2015 which comprises this subchapter and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

Section is comprised of section 1752 of Pub. L. 116–283. Subsec. (d) of section 1752 of Pub. L. 116–283 amended section 3021 of Title 50, War and National Defense.

AMENDMENTS

2021—Subsec. (e). Pub. L. 117–81, §1552(1), (2), (4), designated existing provisions as par. (1) and inserted heading, redesignated former pars. (1) to (8) as subpars. (A) to (H), respectively, of par. (1) and realigned margins, and added par. (2).

Subsec. (e)(1)(C) to (I). Pub. L. 117–81, §1552(3), added subpar. (C) and redesignated former subpars. (C) to (H) (as redesignated by section 1552(1) of Pub. L. 117–81, see above) as (D) to (I), respectively.

Statutory Notes and Related Subsidiaries

SHORT TITLE OF 2022 AMENDMENT

Pub. L. 117–260, §1, Dec. 21, 2022, 136 Stat. 2389, provided that: “This Act [enacting section 1526 of this title and provisions set out as notes under section 1526 of this title] may be cited as the ‘Quantum Computing Cybersecurity Preparedness Act’.”

§ 1501. Definitions

In this subchapter:

(1) Agency

The term “agency” has the meaning given the term in section 3502 of title 44.

(2) Antitrust laws

The term “antitrust laws”—

(A) has the meaning given the term in section 12 of title 15;

(B) includes section 45 of title 15 to the extent that section 45 of title 15 applies to unfair methods of competition; and

(C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) or the law referred to in subparagraph (B).

(3) Appropriate Federal entities

The term “appropriate Federal entities” means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) Cybersecurity purpose

The term “cybersecurity purpose” has the meaning given the term in section 650 of this title.

(5) Cybersecurity threat

The term “cybersecurity threat” has the meaning given the term in section 650 of this title.

(6) Cyber threat indicator

The term “cyber threat indicator” has the meaning given the term in section 650 of this title.

(7) Defensive measure

The term “defensive measure” has the meaning given the term in section 650 of this title.

(8) Federal entity

The term “Federal entity” means a department or agency of the United States or any component of such department or agency.

(9) Information system

The term “information system” has the meaning given the term in section 650 of this title.

(10) Local government

The term “local government” means any borough, city, county, parish, town, township,