

members who win these competitions as having skills at a time when there is a critical shortage of such skills within the uniformed services. The plan should also address how the uniformed services may provide winning service members with a combination of bonuses, advancements, and meritorious recognition to be determined by the Secretaries of the agencies concerned.

(f) The Director of OMB shall, in consultation with appropriate agencies, develop annually a list of agencies 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 accomplishment—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

§ 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” means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5) Cybersecurity threat**(A) In general**

Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) Exclusion

The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) Cyber threat indicator

The term “cyber threat indicator” means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(7) Defensive measure**(A) In general**

Except as provided in subparagraph (B), the term “defensive measure” means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) Exclusion

The term “defensive measure” does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(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”—

(A) has the meaning given the term in section 3502 of title 44; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(10) Local government

The term “local government” means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(11) Malicious cyber command and control

The term “malicious cyber command and control” means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(12) Malicious reconnaissance

The term “malicious reconnaissance” means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) Monitor

The term “monitor” means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(14) Non-Federal entity**(A) In general**

Except as otherwise provided in this paragraph, the term “non-Federal entity” means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) Inclusions

The term “non-Federal entity” includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern

Mariana Islands, and any other territory or possession of the United States.

(C) Exclusion

The term “non-Federal entity” does not include a foreign power as defined in section 1801 of title 50.

(15) Private entity

(A) In general

Except as otherwise provided in this paragraph, the term “private entity” means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or non-profit entity, including an officer, employee, or agent thereof.

(B) Inclusion

The term “private entity” includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) Exclusion

The term “private entity” does not include a foreign power as defined in section 1801 of title 50.

(16) Security control

The term “security control” means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(17) Security vulnerability

The term “security vulnerability” means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) Tribal

The term “tribal” has the meaning given the term “Indian tribe” in section 5304 of title 25.

(Pub. L. 114–113, div. N, title I, § 102, Dec. 18, 2015, 129 Stat. 2936.)

SHORT TITLE

Pub. L. 114–113, div. N, § 1(a), Dec. 18, 2015, 129 Stat. 2935, provided that: “This division [enacting this chapter and sections 149 and 151 of this title, amending sections 131, 148, 149, and 150 of this title, section 1029 of Title 18, Crimes and Criminal Procedure, and sections 3553 and 3554 of Title 44, Public Printing and Documents, enacting provisions set out as notes under this section and sections 101, 131, and 151 of this title and section 301 of Title 5, Government Organization and Employees] may be cited as the ‘Cybersecurity Act of 2015.’”

Pub. L. 114–113, div. N, title I, § 101, Dec. 18, 2015, 129 Stat. 2936, provided that: “This title [enacting this subchapter] may be cited as the ‘Cybersecurity Information Sharing Act of 2015.’”

Pub. L. 114–113, div. N, title II, § 221, Dec. 18, 2015, 129 Stat. 2963, provided that: “This subtitle [subtitle B (§§ 221–229) of title II of div. N of Pub. L. 114–113, enacting subchapter II of this chapter and sections 149 and 151 of this title, amending sections 148, 149, and 150 of this title and sections 3553 and 3554 of Title 44, Public Printing and Documents, and enacting provisions set out as a note under section 151 of this title] may be cited as the ‘Federal Cybersecurity Enhancement Act of 2015.’”

§ 1502. Sharing of information by the Federal Government

(a) In general

Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;

(2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;

(4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 632 of title 15).

(b) Development of procedures

(1) In general

The procedures developed under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, Federal entities and non-