

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,

village, or other political subdivision of a State.

**(11) Malicious cyber command and control**

The term “malicious cyber command and control” has the meaning given the term in section 650 of this title.

**(12) Malicious reconnaissance**

The term “malicious reconnaissance” has the meaning given the term in section 650 of this title.

**(13) Monitor**

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

**(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” has the meaning given the term in section 650 of this title.

**(17) Security vulnerability**

The term “security vulnerability” has the meaning given the term in section 650 of this title.

**(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; Pub. L. 117–263, div. G, title LXXI, §7143(b)(4), Dec. 23, 2022, 136 Stat. 3661.)

**Editorial Notes**

AMENDMENTS

2022—Pars. (4) to (7). Pub. L. 117–263, §7143(b)(4)(A), added pars. (4) to (7) and struck out former pars. (4) to (7) which defined cybersecurity purpose, cybersecurity threat, cyber threat indicator, and defensive measure, respectively.

Par. (9). Pub. L. 117–263, §7143(b)(4)(B), added par. (9) and struck out former par. (9) which defined information system.

Pars. (11) to (13). Pub. L. 117–263, §7143(b)(4)(C), added pars. (11) to (13) and struck out former pars. (11) to (13) which defined malicious cyber command and control, malicious reconnaissance, and monitor, respectively.

Pars. (16), (17). Pub. L. 117–263, §7143(b)(4)(D), added pars. (16) and (17) and struck out former pars. (16) and (17) which defined security control and security vulnerability, respectively.

**Statutory Notes and Related Subsidiaries**

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-Federal entities that have received a cyber threat indicator or defensive measure from a Federal entity under this subchapter that is known or determined to be in error or in contravention of the requirements of this subchapter or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any infor-

mation not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this subchapter.

### **(2) Consultation**

In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 15801 of title 42), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

### **(c) Submittal to Congress**

Not later than 60 days after December 18, 2015, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

(Pub. L. 114–113, div. N, title I, § 103, Dec. 18, 2015, 129 Stat. 2939.)

## **§ 1503. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats**

### **(a) Authorization for monitoring**

#### **(1) In general**

Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

#### **(2) Construction**

Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this subchapter; or

(B) to limit otherwise lawful activity.

### **(b) Authorization for operation of defensive measures**

#### **(1) In general**

Notwithstanding any other provision of law, a private entity may, for cybersecurity pur-

poses, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

**(2) Construction**

Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

**(c) Authorization for sharing or receiving cyber threat indicators or defensive measures**

**(1) In general**

Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

**(2) Lawful restriction**

A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

**(3) Construction**

Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

**(d) Protection and use of information**

**(1) Security of information**

A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

**(2) Removal of certain personal information**

A non-Federal entity sharing a cyber threat indicator pursuant to this subchapter shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator

contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

**(3) Use of cyber threat indicators and defensive measures by non-Federal entities**

**(A) In general**

Consistent with this subchapter, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by a non-Federal entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the non-Federal entity; or

(II) an information system of another non-Federal entity or a Federal entity upon the written consent of that other non-Federal entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by a non-Federal entity subject to—

(I) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

**(B) Construction**

Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

**(4) Use of cyber threat indicators by State, tribal, or local government**

**(A) Law enforcement use**

A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this subchapter may use such cyber threat indicator or defensive measure for the purposes described in section 1504(d)(5)(A) of this title.

**(B) Exemption from disclosure**

A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

**(C) State, tribal, and local regulatory authority****(i) In general**

Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this subchapter shall not be used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-Federal entity or any activity taken by a non-Federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

**(ii) Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats**

A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

**(e) Antitrust exemption****(1) In general**

Except as provided in section 1507(e) of this title, it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this subchapter.

**(2) Applicability**

Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

**(f) No right or benefit**

The sharing of a cyber threat indicator or defensive measure with a non-Federal entity under this subchapter shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

(Pub. L. 114-113, div. N, title I, §104, Dec. 18, 2015, 129 Stat. 2940.)

**§ 1504. Sharing of cyber threat indicators and defensive measures with the Federal Government****(a) Requirement for policies and procedures****(1) Interim policies and procedures**

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

**(2) Final policies and procedures**

Not later than 180 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly issue and make publicly available final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

**(3) Requirements concerning policies and procedures**

Consistent with the guidelines required by subsection (b), the policies and procedures developed or issued under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 1503(c) of this title through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 1503 of this title in a manner other than the real-time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and



(iii) may be provided to other Federal entities; and

(C) ensure there are—

- (i) audit capabilities; and
- (ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this subchapter in an unauthorized manner.

**(4) Guidelines for entities sharing cyber threat indicators with Federal Government**

**(A) In general**

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall jointly develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this subchapter.

**(B) Contents**

The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this subchapter that would be unlikely to include information that—

(I) is not directly related to a cybersecurity threat; and

(II) is personal information of a specific individual or information that identifies a specific individual.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this subchapter.

**(b) Privacy and civil liberties**

**(1) Interim guidelines**

Not later than 60 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in consultation with heads of the appropriate Federal entities and in consultation with officers designated under section 2000ee-1 of title 42, jointly develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this subchapter.

**(2) Final guidelines**

**(A) In general**

Not later than 180 days after December 18, 2015, the Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 2000ee-1 of title 42 and such private entities with industry expertise as the Attorney General and the Secretary

consider relevant, jointly issue and make publicly available final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this subchapter.

**(B) Periodic review**

The Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every 2 years, jointly review the guidelines issued under subparagraph (A).

**(3) Content**

The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this subchapter;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this subchapter; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) consistent with this subchapter, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled “National Strategy for Trusted Identities in Cyberspace” and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this subchapter, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government;

(E) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(F) protect the confidentiality of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals to the

greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this subchapter; and

(G) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

**(c) Capability and process within the Department of Homeland Security**

**(1) In general**

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any non-Federal entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this subchapter that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 1503 of this title, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

**(2) Certification and designation**

**(A) Certification of capability and process**

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, submit to Congress a certification as to whether the capability and process required by paragraph (1) fully and effectively operates—

(i) as the process by which the Federal Government receives from any non-Federal entity a cyber threat indicator or defensive measure under this subchapter; and

(ii) in accordance with the interim policies, procedures, and guidelines developed under this subchapter.

**(B) Designation**

**(i) In general**

At any time after certification is submitted under subparagraph (A), the President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1) in addition to the capability and process developed under such paragraph by the Secretary of Homeland Security, if, not fewer than 30 days before making such designation, the President submits to Congress a certification and explanation that—

(I) such designation is necessary to ensure that full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this subchapter;

(II) the designated appropriate Federal entity will receive and share cyber threat indicators and defensive measures in accordance with the policies, procedures, and guidelines developed under this subchapter, including subsection (a)(3)(A); and

(III) such designation is consistent with the mission of such appropriate Federal entity and improves the ability of the Federal Government to receive, share, and use cyber threat indicators and defensive measures as authorized under this subchapter.

**(ii) Application to additional capability and process**

If the President designates an appropriate Federal entity to develop and implement a capability and process under clause (i), the provisions of this subchapter that apply to the capability and process required by paragraph (1) shall also be construed to apply to the capability and process developed and implemented under clause (i).

**(3) Public notice and access**

The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any non-Federal entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security consistent with the policies and procedures issued under subsection (a).

**(4) Other Federal entities**

The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

**(d) Information shared with or provided to the Federal Government**

**(1) No waiver of privilege or protection**

The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

**(2) Proprietary information**

Consistent with section 1503(c)(2) of this title and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this subchapter shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity.

**(3) Exemption from disclosure**

A cyber threat indicator or defensive measure shared with the Federal Government under this subchapter shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records.

**(4) Ex parte communications**

The provision of a cyber threat indicator or defensive measure to the Federal Government under this subchapter shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

**(5) Disclosure, retention, and use**

**(A) Authorized activities**

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter may be disclosed to, retained by, and used by, consistent with

otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying—

(I) a cybersecurity threat, including the source of such cybersecurity threat; or

(II) a security vulnerability;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18 (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

**(B) Prohibited activities**

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

**(C) Privacy and civil liberties**

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual.

**(D) Federal regulatory authority**

**(i) In general**

Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be used by any

Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

**(ii) Exceptions**

**(I) Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats**

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

**(II) Procedures developed and implemented under this subchapter**

Clause (i) shall not apply to procedures developed and implemented under this subchapter.

(Pub. L. 114–113, div. N, title I, § 105, Dec. 18, 2015, 129 Stat. 2943.)

**§ 1505. Protection from liability**

**(a) Monitoring of information systems**

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 1503(a) of this title that is conducted in accordance with this subchapter.

**(b) Sharing or receipt of cyber threat indicators**

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c) of this title if—

(1) such sharing or receipt is conducted in accordance with this subchapter; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 1504(c)(1)(B) of this title and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 1504(a)(1) of this title and guidelines are submitted to Congress under section 1504(b)(1) of this title; or

(B) the date that is 60 days after December 18, 2015.

**(c) Construction**

Nothing in this subchapter shall be construed—

(1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(Pub. L. 114–113, div. N, title I, § 106, Dec. 18, 2015, 129 Stat. 2950.)

**§ 1506. Oversight of government activities**

**(a) Report on implementation**

**(1) In general**

Not later than 1 year after December 18, 2015, the heads of the appropriate Federal entities shall jointly submit to Congress a detailed report concerning the implementation of this subchapter.

**(2) Contents**

The report required by paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities, policies, procedures, and guidelines under this subchapter and shall include the following:

(A) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 1504(c) of this title, including any impediments to such real-time sharing.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 1504(c) of this title.

(D) A list of Federal entities that have received cyber threat indicators or defensive measures under this subchapter.

**(b) Biennial report on compliance**

**(1) In general**

Not later than 2 years after December 18, 2015 and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this subchapter during the most recent 2-year period.

**(2) Contents**

Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not di-

rectly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this subchapter, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this subchapter, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 1504(c) of this title.

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government<sup>1</sup> entity with the Federal government<sup>1</sup> in contravention of this subchapter, or was shared within the Federal Government in contravention of the guidelines required by this subchapter, including a description of any significant violation of this subchapter.

(iii) The number of times, according to the Attorney General, that information shared under this subchapter was used by a Federal entity to prosecute an offense listed in section 1504(d)(5)(A) of this title.

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 1504(b)(3)(E) of this title.

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this subchapter on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures

among Federal entities to identify inappropriate barriers to sharing information.

### **(3) Recommendations**

Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this subchapter.

### **(c) Independent report on removal of personal information**

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this subchapter. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this subchapter in addressing concerns relating to privacy and civil liberties.

### **(d) Form of reports**

Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

### **(e) Public availability of reports**

The unclassified portions of the reports required under this section shall be made available to the public.

(Pub. L. 114–113, div. N, title I, § 107, Dec. 18, 2015, 129 Stat. 2951.)

## **§ 1507. Construction and preemption**

### **(a) Otherwise lawful disclosures**

Nothing in this subchapter shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this subchapter; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter.

### **(b) Whistle blower protections**

Nothing in this subchapter shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5 (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5 (governing disclosures to Congress), section 1034 of title 10 (governing disclosure to Congress by members of the military), section 3234 of title 50 (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

### **(c) Protection of sources and methods**

Nothing in this subchapter shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or depart-

<sup>1</sup> So in original. Probably should be capitalized.

ment thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

**(d) Relationship to other laws**

Nothing in this subchapter shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

**(e) Prohibited conduct**

Nothing in this subchapter shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

**(f) Information sharing relationships**

Nothing in this subchapter shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 1504(c) of this title.

**(g) Preservation of contractual obligations and rights**

Nothing in this subchapter shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

**(h) Anti-tasking restriction**

Nothing in this subchapter shall be construed to permit a Federal entity—

(1) to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity;

(2) to condition the sharing of cyber threat indicators with a non-Federal entity on such entity's provision of cyber threat indicators to a Federal entity or another non-Federal entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another non-Federal entity.

**(i) No liability for non-participation**

Nothing in this subchapter shall be construed to subject any entity to liability for choosing

not to engage in the voluntary activities authorized in this subchapter.

**(j) Use and retention of information**

Nothing in this subchapter shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this subchapter for any use other than permitted in this subchapter.

**(k) Federal preemption**

**(1) In general**

This subchapter supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this subchapter.

**(2) State law enforcement**

Nothing in this subchapter shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

**(l) Regulatory authority**

Nothing in this subchapter shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized to be issued under this subchapter;

(2) to establish or limit any regulatory authority not specifically established or limited under this subchapter; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

**(m) Authority of Secretary of Defense to respond to malicious cyber activity carried out by foreign powers**

Nothing in this subchapter shall be construed to limit the authority of the Secretary of Defense under section 394 of title 10.

**(n) Criminal prosecution**

Nothing in this subchapter shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this subchapter in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.

(Pub. L. 114–113, div. N, title I, § 108, Dec. 18, 2015, 129 Stat. 2953; Pub. L. 115–232, div. A, title XVI, § 1631(b), Aug. 13, 2018, 132 Stat. 2123.)

**Editorial Notes**

**AMENDMENTS**

2018—Subsec. (m). Pub. L. 115–232 substituted “section 394” for “section 130g”.

**§ 1508. Report on cybersecurity threats**

**(a) Report required**

Not later than 180 days after December 18, 2015, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall

submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

**(b) Contents**

The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

**(c) Form of report**

The report required by subsection (a) shall be made available in classified and unclassified forms.

**(d) Intelligence community defined**

In this section, the term “intelligence community” has the meaning given that term in section 3003 of title 50.

(Pub. L. 114–113, div. N, title I, § 109, Dec. 18, 2015, 129 Stat. 2955.)

**§ 1509. Exception to limitation on authority of Secretary of Defense to disseminate certain information**

Notwithstanding subsection (c)(3) of section 393 of title 10, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this subchapter.

(Pub. L. 114–113, div. N, title I, § 110, Dec. 18, 2015, 129 Stat. 2956.)

**§ 1510. Effective period**

**(a) In general**

Except as provided in subsection (b), this subchapter and the amendments made by this subchapter shall be effective during the period beginning on December 18, 2015 and ending on September 30, 2025.

**(b) Exception**

With respect to any action authorized by this subchapter or information obtained pursuant to an action authorized by this subchapter, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this subchapter shall continue in effect.

(Pub. L. 114–113, div. N, title I, § 111, Dec. 18, 2015, 129 Stat. 2956.)

**Editorial Notes**

**REFERENCES IN TEXT**

The amendments made by this subchapter, referred to in subsec. (a), was in the original “the amendments made by this title”, meaning title I of div. N of Pub. L. 114–113, which is classified generally to this subchapter.

**SUBCHAPTER II—FEDERAL  
CYBERSECURITY ENHANCEMENT**

**§ 1521. Definitions**

In this subchapter:

**(1) Agency**

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

**(2) Agency information system**

The term “agency information system” has the meaning given the term in section 660 of this title.

**(3) Appropriate congressional committees**

The term “appropriate congressional committees” means—

- (A) the Committee on Homeland Security and Governmental Affairs of the Senate; and
- (B) the Committee on Homeland Security of the House of Representatives.

**(4) Cybersecurity risk; information system**

The terms “cybersecurity risk” and “information system” have the meanings given those terms in section 650 of this title.

**(5) Director**

The term “Director” means the Director of the Office of Management and Budget.

**(6) Intelligence community**

The term “intelligence community” has the meaning given the term in section 3003(4) of title 50.

**(7) National security system**

The term “national security system” has the meaning given the term in section 11103 of title 40.

**(8) Secretary**

The term “Secretary” means the Secretary of Homeland Security.