

## SHORT TITLE

Pub. L. 110-161, div. E, title VI, §601, Dec. 26, 2007, 121 Stat. 2094, provided that: “This title [enacting this chapter] may be cited as the ‘Border Infrastructure and Technology Modernization Act of 2007’.”

**§§ 1402, 1403. Repealed. Pub. L. 113-188, title X, § 1001(b), Nov. 26, 2014, 128 Stat. 2022**

Section 1402, Pub. L. 110-161, div. E, title VI, §603, Dec. 26, 2007, 121 Stat. 2094, related to the Port of Entry Infrastructure Assessment Study.

Section 1403, Pub. L. 110-161, div. E, title VI, §604, Dec. 26, 2007, 121 Stat. 2095, related to the National Land Border Security Plan.

**§ 1404. Repealed. Pub. L. 114-4, title V, § 566, Mar. 4, 2015, 129 Stat. 73**

Section, Pub. L. 110-161, div. E, title VI, §605, Dec. 26, 2007, 121 Stat. 2096, related to the port of entry technology demonstration program.

**§ 1405. Authorization of appropriations**

**(a) In general**

In addition to any funds otherwise available, there are authorized to be appropriated such sums as may be necessary to carry out this chapter for fiscal years 2009 through 2013.

**(b) International agreements**

Funds authorized to be appropriated under this chapter may be used for the implementation of projects described in the Declaration on Embracing Technology and Cooperation to Promote the Secure and Efficient Flow of People and Commerce across our Shared Border between the United States and Mexico, agreed to March 22, 2002, Monterrey, Mexico (commonly known as the Border Partnership Action Plan) or the Smart Border Declaration between the United States and Canada, agreed to December 12, 2001, Ottawa, Canada that are consistent with the provisions of this chapter.

(Pub. L. 110-161, div. E, title VI, §606, Dec. 26, 2007, 121 Stat. 2097.)

**CHAPTER 6—CYBERSECURITY**

**SUBCHAPTER I—CYBERSECURITY INFORMATION SHARING**

Sec.	
1501.	Definitions.
1502.	Sharing of information by the Federal Government.
1503.	Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.
1504.	Sharing of cyber threat indicators and defensive measures with the Federal Government.
1505.	Protection from liability.
1506.	Oversight of government activities.
1507.	Construction and preemption.
1508.	Report on cybersecurity threats.
1509.	Exception to limitation on authority of Secretary of Defense to disseminate certain information.
1510.	Effective period.

**SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT**

1521.	Definitions.
1522.	Advanced internal defenses.
1523.	Federal cybersecurity requirements.

Sec.	
1524.	Assessment; reports.
1525.	Termination.

**SUBCHAPTER III—OTHER CYBER MATTERS**

1531.	Apprehension and prosecution of international cyber criminals.
1532.	Enhancement of emergency services.
1533.	Improving cybersecurity in the health care industry.

**EX. ORD. NO. 13800. STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE**

Ex. Ord. No. 13800, May 11, 2017, 82 F.R. 22391, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

**SECTION 1. *Cybersecurity of Federal Networks.***

(a) *Policy.* The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) *Findings.*

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor’s support lifecycle, declining to implement a vendor’s security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) *Risk Management.*

(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency’s cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and

(B) a plan to:

(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;

(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and

(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:

(1) be completed within 90 days of the date of this order; and

(2) describe the legal, policy, and budgetary considerations relevant to—as well as the technical feasibility and cost effectiveness, including timelines and milestones, of—transitioning all agencies, or a subset of agencies, to:

(aa) one or more consolidated network architectures; and

(bb) shared IT services, including email, cloud, and cybersecurity services.

(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT

services with respect to cybersecurity, including by making recommendations to ensure consistency with [former] section 227 [now 2209] of the Homeland Security Act ([former] 6 U.S.C. 148) [now 6 U.S.C. 659] and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

**SEC. 2. Cybersecurity of Critical Infrastructure.**

(a) *Policy.* It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.

(b) *Support to Critical Infrastructure at Greatest Risk.* The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;

(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and

(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) *Supporting Transparency in the Marketplace.* The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency

of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(d) *Resilience Against Botnets and Other Automated, Distributed Threats.* The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) *Assessment of Electricity Disruption Incident Response Capabilities.* The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) *Department of Defense Warfighting Capabilities and Industrial Base.* Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

#### SEC. 3. *Cybersecurity for the Nation.*

(a) *Policy.* To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

(b) *Deterrence and Protection.* Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for

National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) *International Cooperation.* As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.

(d) *Workforce Development.* In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

SEC. 4. *Definitions.* For the purposes of this order:

(a) The term “appropriate stakeholders” means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term “information technology” (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems of agencies that monitor and control physical equipment and processes.

(c) The term “IT architecture” refers to the integration and implementation of IT within an agency.

(d) The term “network architecture” refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.

SEC. 5. *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) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be construed to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence or law enforcement operations.

(d) 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 sys-

tem 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 unus-

able, 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-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 information 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 purposes, 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 meas-

ure 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 defen-

sive 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, in-

cluding 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 directly 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 in-

formation 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 disclo-

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

sure 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 department 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.)

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.)

## 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 659 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.

(Pub. L. 114–113, div. N, title II, §222, Dec. 18, 2015, 129 Stat. 2963; Pub. L. 115–278, §2(h)(1)(D), Nov. 16, 2018, 132 Stat. 4182.)

## REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, which is classified principally to this subchapter. For complete classification of subtitle B to the Code, see Tables.

## AMENDMENTS

2018—Par. (2). Pub. L. 115–278, §2(h)(1)(D)(i), substituted “section 660 of this title” for “section 149 of this title, as added by section 223(a)(4) of this division”.

Par. (4). Pub. L. 115–278, §2(h)(1)(D)(ii), substituted “section 659 of this title” for “section 148 of this title, as so redesignated by section 223(a)(3) of this division”.

**§ 1522. Advanced internal defenses****(a) Advanced network security tools****(1) In general**

The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

**(2) Development of plan**

The Director shall develop and the Secretary shall implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

**(b) Prioritizing advanced security tools**

The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

**(c) Improved metrics**

The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44 to include measures of intrusion and incident detection and response times.

**(d) Transparency and accountability**

The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro-agencies.

**(e) Omitted****(f) Exception**

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, §224, Dec. 18, 2015, 129 Stat. 2967.)

## CODIFICATION

Section is comprised of section 224 of title II of div. N of Pub. L. 114–113. Subsec. (e) of section 224 of title II of div. N of Pub. L. 114–113 amended section 3553 of Title 44, Public Printing and Documents.

**§ 1523. Federal cybersecurity requirements****(a) Implementation of Federal cybersecurity standards**

Consistent with section 3553 of title 44, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40 for securing agency information systems.

**(b) Cybersecurity requirements at agencies****(1) In general**

Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section 11331 of title 40 and except as provided in paragraph (2), not later than 1 year after December 18, 2015, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 7464 of title 15, including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

**(2) Exception**

The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

### (3) Construction

Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

### (c) Exception

The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(Pub. L. 114–113, div. N, title II, §225, Dec. 18, 2015, 129 Stat. 2967.)

## § 1524. Assessment; reports

### (a) Definitions

In this section:

#### (1) Agency information

The term “agency information” has the meaning given the term in section 2213 of the Homeland Security Act of 2002 [6 U.S.C. 663].

#### (2) Cyber threat indicator; defensive measure

The terms “cyber threat indicator” and “defensive measure” have the meanings given those terms in section 1501 of this title.

#### (3) Intrusion assessments

The term “intrusion assessments” means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems.

#### (4) Intrusion assessment plan

The term “intrusion assessment plan” means the plan required under section 2210(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 660(b)(1)].

#### (5) Intrusion detection and prevention capabilities

The term “intrusion detection and prevention capabilities” means the capabilities re-

quired under section 2213(b) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)].

### (b) Third-party assessment

Not later than 3 years after December 18, 2015, the Comptroller General of the United States shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

### (c) Reports to Congress

#### (1) Intrusion detection and prevention capabilities

##### (A) Secretary of Homeland Security report

Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 2213(c)(5) of the Homeland Security Act of 2002 [6 U.S.C. 663(c)(5)], including the number of new technologies tested and the number of participating agencies.

##### (B) OMB report

Not later than 18 months after December 18, 2015, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

**(C) Chief information officer**

Not earlier than 18 months after December 18, 2015, and not later than 2 years after December 18, 2015, the Federal Chief Information Officer shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities, including—

(i) the effectiveness of the system in detecting, disrupting, and preventing cyber-threat actors, including advanced persistent threats, from accessing agency information and agency information systems;

(ii) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed under subtitle D<sup>1</sup> of title II of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) are effective in securing Federal information systems;

(iii) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools and including the value of classified cyber threat indicators; and

(iv) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

**(2) OMB report on development and implementation of intrusion assessment plan, advanced internal defenses, and Federal cybersecurity requirements**

The Director shall—

(A) not later than 6 months after December 18, 2015, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after December 18, 2015, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) a description of the advanced network security tools included in the efforts to continuously diagnose and mitigate cybersecurity risks pursuant to section 1522(a)(1) of this title; and

(iv) a list by agency of compliance with the requirements of section 1523(b) of this title; and

(C) not later than 1 year after December 18, 2015, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 1522(a)(2) of this title; and

(ii) the improved metrics developed pursuant to section 1522(c) of this title.

**(d) Form**

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

(Pub. L. 114–113, div. N, title II, §226, Dec. 18, 2015, 129 Stat. 2969; Pub. L. 115–278, §2(h)(1)(F), Nov. 16, 2018, 132 Stat. 4182.)

REFERENCES IN TEXT

Subtitle D of title II of the Homeland Security Act of 2002, referred to in subsec. (c)(1)(C)(ii), is subtitle D (§§231–237) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2159, which enacted part D (§161 et seq.) of subchapter II of chapter 1 of this title and amended sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement. Subtitle D was redesignated subtitle C of title II of the Homeland Security Act of 2002 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and is classified principally to part C (§161 et seq.) of subchapter II of chapter 1 of this title. For complete classification of subtitle C to the Code, see Tables.

AMENDMENTS

2018—Subsec. (a)(1). Pub. L. 115–278, §2(h)(1)(F)(i)(I), substituted “section 2213” for “section 230” and struck out before period at end “, as added by section 223(a)(6) of this division”.

Subsec. (a)(4). Pub. L. 115–278, §2(h)(1)(F)(i)(II), substituted “section 2210(b)(1)” for “section 228(b)(1)” and struck out before period at end “, as added by section 223(a)(4) of this division”.

Subsec. (a)(5). Pub. L. 115–278, §2(h)(1)(F)(i)(III), substituted “section 2213(b)” for “section 230(b)” and struck out before period at end “, as added by section 223(a)(6) of this division”.

Subsec. (c)(1)(A)(vi). Pub. L. 115–278, §2(h)(1)(F)(ii), substituted “section 2213(c)(5)” for “section 230(c)(5)” and struck out “, as added by section 223(a)(6) of this division” after “Homeland Security Act of 2002”.

**§ 1525. Termination**

**(a) In general**

The authority provided under section 663 of this title, and the reporting requirements under section 1524(c) of this title shall terminate on the date that is 7 years after December 18, 2015.

**(b) Rule of construction**

Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 663(d)(2) of this title, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

<sup>1</sup> See References in Text note below.

(Pub. L. 114–113, div. N, title II, §227, Dec. 18, 2015, 129 Stat. 2971; Pub. L. 115–278, §2(h)(1)(G), Nov. 16, 2018, 132 Stat. 4182.)

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(G)(i), substituted “section 663 of this title” for “section 151 of this title, as added by section 223(a)(6) of this division.”.

Subsec. (b). Pub. L. 115–278, §2(h)(1)(G)(ii), substituted “section 663(d)(2) of this title” for “section 151(d)(2) of this title, as added by section 223(a)(6) of this division.”.

SUBCHAPTER III—OTHER CYBER MATTERS

**§ 1531. Apprehension and prosecution of international cyber criminals**

**(a) International cyber criminal defined**

In this section, the term “international cyber criminal” means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a “Red Notice”) has been circulated by Interpol.

**(b) Consultations for noncooperation**

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

**(c) Annual report**

**(1) In general**

The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

**(2) Form**

The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

**(3) Appropriate congressional committees**

For purposes of this subsection, the term “appropriate congressional committees” means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(Pub. L. 114–113, div. N, title IV, §403, Dec. 18, 2015, 129 Stat. 2979.)

**§ 1532. Enhancement of emergency services**

**(a) Collection of data**

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, acting through the center established under section 659 of this title, in coordination with appropriate Federal entities and the Assistant Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 101 of this title) within the State.

**(b) Analysis of data**

Not later than 1 year after December 18, 2015, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Assistant Director for Emergency Communications, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

**(c) Best practices**

**(1) In general**

Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facili-

tate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 272(e) of title 15.

**(2) Report**

The Director of the National Institute of Standards and Technology shall submit to Congress a report on the result of the activities of the Director under paragraph (1), including any methods developed by the Director under such paragraph, and shall make such report publicly available on the website of the National Institute of Standards and Technology.

**(d) Rule of construction**

Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require a non-Federal entity (as defined in section 1501 of this title) to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the result of the activities carried out under subsection (c), including any methods developed under such subsection.

(Pub. L. 114–113, div. N, title IV, §404, Dec. 18, 2015, 129 Stat. 2980; Pub. L. 115–278, §2(h)(1)(H), Nov. 16, 2018, 132 Stat. 4183.)

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–278, §2(h)(1)(H), substituted “section 659 of this title” for “section 148 of this title, as redesignated by section 223(a)(3) of this division,” and “Assistant Director for Emergency Communications” for “Director for Emergency Communications”.

Subsec. (b). Pub. L. 115–278, §2(h)(1)(H)(ii), substituted “Assistant Director for Emergency Communications” for “Director for Emergency Communications”.

**§ 1533. Improving cybersecurity in the health care industry**

**(a) Definitions**

In this section:

**(1) Appropriate congressional committees**

The term “appropriate congressional committees” means—

(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

**(2) Business associate**

The term “business associate” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(3) Covered entity**

The term “covered entity” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(4) Cybersecurity threat; cyber threat indicator; defensive measure; Federal entity; non-Federal entity; private entity**

The terms “cybersecurity threat”, “cyber threat indicator”, “defensive measure”, “Federal entity”, “non-Federal entity”, and “private entity” have the meanings given such terms in section 1501 of this title.

**(5) Health care clearinghouse; health care provider; health plan**

The terms “health care clearinghouse”, “health care provider”, and “health plan” have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(6) Health care industry stakeholder**

The term “health care industry stakeholder” means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) advocate for patients or consumers;

(C) pharmacist;

(D) developer or vendor of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

**(7) Secretary**

The term “Secretary” means the Secretary of Health and Human Services.

**(b) Report**

**(1) In general**

Not later than 1 year after December 18, 2015, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.

**(2) Contents of report**

With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report under paragraph (1) shall include—

(A) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(B) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

**(c) Health care industry cybersecurity task force****(1) In general**

Not later than 90 days after December 18, 2015, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing subchapter I of this chapter, so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

**(2) Termination**

The task force established under this subsection shall terminate on the date that is 1 year after the date on which such task force is established.

**(3) Dissemination**

Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

**(d) Aligning health care industry security approaches****(1) In general**

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 272(c)(15) of title 15;

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note); and

(iii) the provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111–5), and the amendments made by such Act; and

(D) are updated on a regular basis and applicable to a range of health care organizations.

**(2) Limitation**

Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase, on compliance with this subsection.

**(3) No liability for nonparticipation**

Nothing in this section shall be construed to subject a health care industry stakeholder to liability for choosing not to engage in the voluntary activities authorized or guidelines developed under this subsection.

**(e) Incorporating ongoing activities**

In carrying out the activities under this section, the Secretary may incorporate activities that are ongoing as of the day before December 18, 2015 and that are consistent with the objectives of this section.

**(f) Rule of construction**

Nothing in this section shall be construed to limit the antitrust exemption under section 1503(e) of this title or the protection from liability under section 1505 of this title.

(Pub. L. 114–113, div. N, title IV, § 405, Dec. 18, 2015, 129 Stat. 2981.)

## REFERENCES IN TEXT

Section 264(c) of the Health Insurance Portability and Accountability Act of 1996, referred to subsec. (d)(1)(C)(ii), is section 264(c) of Pub. L. 104–191, which is set out as a note under section 1320d–2 of Title 42, The Public Health and Welfare.

The Health Information Technology for Economic and Clinical Health Act, referred to in subsec. (d)(1)(C)(iii), is title XIII of div. A and title IV of div. B of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 226, 467, also known as the HITECH Act. For complete classification of this Act to the Code, see Short Title of 2009 Amendment note set out under section 201 of Title 42, The Public Health and Welfare, and Tables.