

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 Repealed.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 Repealed.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.
- 1524. Assessment; reports.
- 1525. Termination.

**SUBCHAPTER III—OTHER CYBER MATTERS**

- 1531. Apprehension and prosecution of international cyber criminals.

- Sec. 1532. Enhancement of emergency services.
- 1533. Improving cybersecurity in the health care industry.

**SUBCHAPTER I—CYBERSECURITY INFORMATION SHARING**

**§ 1501. Definitions**

In this subchapter:

**(1) Agency**

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

**(2) Antitrust laws**

The term “antitrust laws”—

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

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

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

**(3) Appropriate Federal entities**

The term “appropriate Federal entities” means the following:

- (A) The Department of Commerce.
- (B) The Department of Defense.
- (C) The Department of Energy.
- (D) The Department of Homeland Security.
- (E) The Department of Justice.
- (F) The Department of the Treasury.
- (G) The Office of the Director of National Intelligence.

**(4) Cybersecurity purpose**

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

**(5) Cybersecurity threat**

**(A) In general**

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

**(B) Exclusion**

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

**(6) Cyber threat indicator**

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

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

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

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

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

(E) malicious cyber command and control;

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

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

(H) any combination thereof.

**(7) Defensive measure**

**(A) In general**

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

**(B) Exclusion**

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

(i) the private entity operating the measure; or

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

**(8) Federal entity**

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

**(9) Information system**

The term “information system”—

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

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

**(10) Local government**

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

village, or other political subdivision of a State.

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

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

**(12) Malicious reconnaissance**

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

**(13) Monitor**

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

**(14) Non-Federal entity**

**(A) In general**

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

**(B) Inclusions**

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

**(C) Exclusion**

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

**(15) Private entity**

**(A) In general**

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

**(B) Inclusion**

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

**(C) Exclusion**

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

**(16) Security control**

The term “security control” means the management, operational, and technical controls used to protect against an unauthorized effort

to adversely affect the confidentiality, integrity, and availability of an information system or its information.

**(17) Security vulnerability**

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

**(18) Tribal**

The term “tribal” has the meaning given the term “Indian tribe” in section 450b 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 individ-