

Transportation, consistent with the Annex to the Memorandum of Understanding executed on August 9, 2006, shall promulgate such regulations and carry out necessary inspection and enforcement actions. Any regulations shall incorporate the guidance provided to pipeline operators by the September 5, 2002, Department of Transportation Research and Special Programs Administration's Pipeline Security Information Circular and contain additional requirements as necessary based upon the results of the inspections performed under subsection (b). The regulations shall include the imposition of civil penalties for noncompliance.

(e) Funding

From the amounts appropriated pursuant to section 114(w) of title 49, there shall be made available to the Secretary to carry out this section—

- (1) \$2,000,000 for fiscal year 2008;
- (2) \$2,000,000 for fiscal year 2009; and
- (3) \$2,000,000 for fiscal year 2010.

(Pub. L. 110-53, title XV, §1557, Aug. 3, 2007, 121 Stat. 475.)

§ 1208. Pipeline security and incident recovery plan

(a) In general

The Secretary, in consultation with the Secretary of Transportation and the Administrator of the Pipeline and Hazardous Materials Safety Administration, and in accordance with the Annex to the Memorandum of Understanding executed on August 9, 2006, the National Strategy for Transportation Security, and Homeland Security Presidential Directive-7, shall develop a pipeline security and incident recovery protocols plan. The plan shall include—

(1) for the Government to provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations as determined under section 1207 of this title when—

(A) under severe security threat levels of alert; or

(B) under specific security threat information relating to such pipeline infrastructure or operations exists; and

(2) an incident recovery protocol plan, developed in conjunction with interstate and intrastate transmission and distribution pipeline operators and terminals and facilities operators connected to pipelines, to develop protocols to ensure the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses in the event of an incident affecting the interstate and intrastate natural gas and hazardous liquid transmission and distribution pipeline system, which shall include protocols for restoring essential services supporting pipelines and granting access to pipeline operators for pipeline infrastructure repair, replacement, or bypass following an incident.

(b) Existing private and public sector efforts

The plan shall take into account actions taken or planned by both private and public en-

titles to address identified pipeline security issues and assess the effective integration of such actions.

(c) Consultation

In developing the plan under subsection (a), the Secretary shall consult with the Secretary of Transportation, interstate and intrastate transmission and distribution pipeline operators, nonprofit employee organizations representing pipeline employees, emergency responders, offerors, State pipeline safety agencies, public safety officials, and other relevant parties.

(d) Report

(1) Contents

Not later than 2 years after August 3, 2007, the Secretary shall transmit to the appropriate congressional committees a report containing the plan required by subsection (a), including an estimate of the private and public sector costs to implement any recommendations.

(2) Format

The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(Pub. L. 110-53, title XV, §1558, Aug. 3, 2007, 121 Stat. 476.)

CHAPTER 5—BORDER INFRASTRUCTURE AND TECHNOLOGY MODERNIZATION

Sec.

1401. Definitions.

1402 to 1404. Repealed.

1405. Authorization of appropriations.

§ 1401. Definitions

In this chapter:

(1) Commissioner

The term “Commissioner” means the Commissioner of U.S. Customs and Border Protection of the Department of Homeland Security.

(2) Maquiladora

The term “maquiladora” means an entity located in Mexico that assembles and produces goods from imported parts for export to the United States.

(3) Northern border

The term “northern border” means the international border between the United States and Canada.

(4) Secretary

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

(5) Southern border

The term “southern border” means the international border between the United States and Mexico.

(Pub. L. 110-161, div. E, title VI, §602, Dec. 26, 2007, 121 Stat. 2094.)

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.
- 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—