

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 entities 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.

Sec.
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.)

Statutory Notes and Related Subsidiaries

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.
1500. National Cyber Director.
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.
1532. Enhancement of emergency services.
1533. Improving cybersecurity in the health care industry.

Statutory Notes and Related Subsidiaries

LIMITATION RELATING TO ESTABLISHMENT OR SUPPORT OF CYBERSECURITY UNIT WITH THE RUSSIAN FEDERATION

Pub. L. 116-92, div. E, title LXVII, § 6701, Dec. 20, 2019, 133 Stat. 2221, provided that:

“(a) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ‘appropriate congressional committees’ means—

- “(1) the congressional intelligence committees;
- “(2) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and
- “(3) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

“(b) LIMITATION.—

“(1) IN GENERAL.—No amount may be expended by the Federal Government, other than the Department of Defense, to enter into or implement any bilateral agreement between the United States and the Russian Federation regarding cybersecurity, including the establishment or support of any cybersecurity unit, unless, at least 30 days prior to the conclusion of any such agreement, the Director of National Intelligence submits to the appropriate congressional committees a report on such agreement that includes the elements required by subsection (c).

“(2) DEPARTMENT OF DEFENSE AGREEMENTS.—Any agreement between the Department of Defense and

the Russian Federation regarding cybersecurity shall be conducted in accordance with section 1232 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) [130 Stat. 2488], as amended by section 1231 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91) [131 Stat. 1657].

“(c) ELEMENTS.—If the Director submits a report under subsection (b) with respect to an agreement, such report shall include a discussion of each of the following:

- “(1) The purpose of the agreement.
- “(2) The nature of any intelligence to be shared pursuant to the agreement.
- “(3) The expected value to national security resulting from the implementation of the agreement.
- “(4) Such counterintelligence concerns associated with the agreement as the Director may have and such measures as the Director expects to be taken to mitigate such concerns.

“(d) RULE OF CONSTRUCTION.—This section shall not be construed to affect any existing authority of the Director of National Intelligence, the Director of the Central Intelligence Agency, or another head of an element of the intelligence community, to share or receive foreign intelligence on a case-by-case basis.”

[For definitions of “congressional intelligence committees” and “intelligence community” as used in section 6701 of div. E of Pub. L. 116-92, set out above, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of Title 50, War and National Defense.]

Executive Documents

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.