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

SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT

SUBCHAPTER III—OTHER CYBER MATTERS

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.