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 Repealed.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 Repealed.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

SUBCHAPTER II—FEDERAL CYBERSECURITY ENHANCEMENT

SUBCHAPTER III—OTHER CYBER MATTERS

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: