113TH CONGRESS
2D SESSION

S. 2500

To restrict the ability of the Federal Government to undermine privacy and encryption technology in commercial products and in NIST computer security and encryption standards.

IN THE SENATE OF THE UNITED STATES

JUNE 19, 2014

Mr. WALSH introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To restrict the ability of the Federal Government to undermine privacy and encryption technology in commercial products and in NIST computer security and encryption standards.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''American Digital Security and Commerce Act of 2014''.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The United States is the world leader in technology, encryption, and computer security.

(2) The United States Government, through the expert work of the National Institute of Standards and Technology (referred to in this section as ''NIST'') and the Information Assurance Directorate of the National Security Agency, plays a vital role in developing the tools that keep global electronic communications secure.

(3) The United States Government should actively promote privacy and computer security. Allegations that entities within the United States Government seek to undermine the security of encryption standards or commercial products weaken privacy and erode trust in the United States Government and in products from the United States.

(4) The actions described in paragraph (3) may take a serious toll on the United States economy. The Information Technology and Innovation Foundation has predicted that United States companies may lose 10 percent of the cloud computing market to overseas competitors due to surveillance and security concerns, a loss that could amount to not less than $35,000,000,000 in lost sales by 2016.

(5) The cryptographic expertise of NIST is recognized around the world, but widespread adoption of the robust encryption standards that NIST develops depends on trust.

(6) To promote privacy protection and restore trust in the encryption standards of the United States and hardware and software from the United States, the United States Government should be prohibited from undermining the security of the United States technologies on which global commerce relies.

SEC. 3. FEDERAL INFORMATION SECURITY MANAGEMENT.

(a) DIRECTOR OF OMB REQUIREMENT.—Section 3543(a)(3) of title 44, United States Code, is amended—

(1) by striking ''assure, to the maximum extent feasible'' and inserting the following: ''assure—

''(A) to the maximum extent feasible,'';

(2) by inserting ''and'' after the semicolon; and

(3) by adding at the end the following:

''(B) that any agency or office described in subparagraph (A) does not intentionally weaken, circumvent, undermine, or create any mechanism through which any agency or office of the Federal Government may bypass, the privacy, security, or encryption protections included in any standard or guideline;''.

(b) REQUIREMENT FOR NIST CONSULTEES.—

(1) IN GENERAL.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(A) by redesignating subsection (e) as subsection (f); and

(B) by inserting after subsection (d) the following:

''(e) Each agency or office that the Institute consults with under subsection (c)(1) may not intentionally weaken, circumvent, undermine, or create any mechanism through which any agency or office of the Federal Government may bypass, the privacy, security, or encryption protections included in any standard or guideline required under subsection (a) or (b).''.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Section 22 of the National Institute of Standards and Technology Act (15 U.S.C. 278h) is amended—

(A) in subsection (a)(2), by striking ''Computer System Security and Privacy Advisory Board under section 20(f)'' and inserting ''Information Security and Privacy Advisory Board under section 21''; and

(B) in subsection (e)(1), by striking ''Computer System Security and Privacy Advisory Board'' and inserting ''Information Security and Privacy Advisory Board under section 21''.

SEC. 4. SECURITY OF COMPUTER HARDWARE, COMPUTER SOFTWARE, AND ELECTRONIC DEVICES.

(a) DEFINITIONS.—In this section—

(1) the terms ''agent of a foreign power'' and ''foreign power'' have the meaning given those terms in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(2) the term ''covered person''—

(A) means an individual, partnership, association, joint stock company, trust, or corporation; and

(B) does not include a foreign power or an agent of a foreign power;

(3) the term ''covered product'' means any computer hardware, computer software, or electronic device that is made available to the general public; and

(4) the term ''element of the intelligence community'' means an element of the intelligence community specified in or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(b) SECURITY OF COVERED PRODUCTS.—

(1) PROHIBITIONS.—

(A) PROHIBITION ON INTERCEPTION.—Except as provided in paragraph (2), an agency or department of the Federal Government may not intercept any shipment of covered products for the purpose of intentionally introducing into the covered products a mechanism or device that would allow an agency or department of the Federal Government to circumvent the privacy, security, or encryption protections of the covered products.

(B) PROHIBITION ON REQUIRING OR CONTRACTING FOR INSTALLATION OF DEVICES.—Except as provided in paragraph (2), an element of the intelligence community may not require, or contract with, a manufacturer or developer of covered products to place a mechanism or device into a covered product that would allow any agency or department of the Federal Government to circumvent any privacy, security, or encryption protections of the covered product.

(2) EXCEPTION FOR LAWFUL SURVEILLANCE ACTIVITIES UNDER COURT ORDER.—The prohibi-

tions under paragraph (1) shall not apply to a lawful surveillance activity conducted pursuant to a court order issued under—

(A) chapter 119, 121, or 206 of title 18, United States Code; or

(B) the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), except section 702 of that Act (50 U.S.C. 1881a).

(c) ENFORCEMENT.—

(1) AUTHORIZATION OF CIVIL ACTION.—A covered person that suffers an injury proximately caused by a violation of subsection (b) may bring a civil action against the United States in a district court of the United States to recover money damages in accordance with paragraph (2) of this subsection.

(2) AMOUNT OF DAMAGES.—A court, in awarding money damages to a covered person in a civil action brought under this subsection, shall award—

(A) an amount that is the greater of—

(i) the amount of actual damages; or

(ii) $10,000; and

(B) reasonable costs, including reasonable attorney's fees.

(3) EXCLUSIVE REMEDY.—A civil action against the United States under this subsection shall be the exclusive remedy against the United States for a violation of subsection (b).

(4) REIMBURSEMENT OF AWARD.—An agency or department of the United States, including an element of the intelligence community, shall deposit into the general fund of the Treasury of the United States an amount equal to any amount awarded under paragraph (2), for a violation of subsection (b) by the agency or department, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the agency or department.

(5) DEFENSE OF GOOD FAITH RELIANCE.—The United States shall not be liable to a covered person in a civil action brought under this subsection based on any action taken by an individual acting on behalf of an agency or department of the United States, including an element of the intelligence community, if the individual acted in a good faith reliance on a court order, a grand jury subpoena, or a legislative authorization under—

(A) chapter 119, 121, or 206 of title 18, United States Code; or

(B) the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), except section 702 of that Act (50 U.S.C. 1881a).

○