

113<sup>TH</sup> CONGRESS  
2<sup>D</sup> 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.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “American Digital Secu-  
5       rity and Commerce Act of 2014”.

6       **SEC. 2. FINDINGS.**

7       Congress makes the following findings:

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

3           (2) The United States Government, through the  
4 expert work of the National Institute of Standards  
5 and Technology (referred to in this section as  
6 “NIST”) and the Information Assurance Direc-  
7 torate of the National Security Agency, plays a vital  
8 role in developing the tools that keep global elec-  
9 tronic communications secure.

10          (3) The United States Government should ac-  
11 tively promote privacy and computer security. Alle-  
12 gations that entities within the United States Gov-  
13 ernment seek to undermine the security of encryp-  
14 tion standards or commercial products weaken pri-  
15 vacy and erode trust in the United States Govern-  
16 ment and in products from the United States.

17          (4) The actions described in paragraph (3) may  
18 take a serious toll on the United States economy.  
19 The Information Technology and Innovation Foun-  
20 dation has predicted that United States companies  
21 may lose 10 percent of the cloud computing market  
22 to overseas competitors due to surveillance and secu-  
23 rity concerns, a loss that could amount to not less  
24 than \$35,000,000,000 in lost sales by 2016.

1           (5) The cryptographic expertise of NIST is rec-  
2           ognized around the world, but widespread adoption  
3           of the robust encryption standards that NIST devel-  
4           ops depends on trust.

5           (6) To promote privacy protection and restore  
6           trust in the encryption standards of the United  
7           States and hardware and software from the United  
8           States, the United States Government should be pro-  
9           hibited from undermining the security of the United  
10          States technologies on which global commerce relies.

11 **SEC. 3. FEDERAL INFORMATION SECURITY MANAGEMENT.**

12          (a) **DIRECTOR OF OMB REQUIREMENT.**—Section  
13 3543(a)(3) of title 44, United States Code, is amended—

14           (1) by striking “assure, to the maximum extent  
15           feasible” and inserting the following: “assure—

16                   “(A) to the maximum extent feasible,”;

17           (2) by inserting “and” after the semicolon; and

18           (3) by adding at the end the following:

19                   “(B) that any agency or office described in  
20           subparagraph (A) does not intentionally weak-  
21           en, circumvent, undermine, or create any mech-  
22           anism through which any agency or office of the  
23           Federal Government may bypass, the privacy,  
24           security, or encryption protections included in  
25           any standard or guideline;”.

1 (b) REQUIREMENT FOR NIST CONSULTEES.—

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

5 (A) by redesignating subsection (e) as sub-  
6 section (f); and

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

9 “(e) Each agency or office that the Institute consults  
10 with under subsection (c)(1) may not intentionally weak-  
11 en, circumvent, undermine, or create any mechanism  
12 through which any agency or office of the Federal Govern-  
13 ment may bypass, the privacy, security, or encryption pro-  
14 tections included in any standard or guideline required  
15 under subsection (a) or (b).”.

16 (2) TECHNICAL AND CONFORMING AMEND-  
17 MENTS.—Section 22 of the National Institute of  
18 Standards and Technology Act (15 U.S.C. 278h) is  
19 amended—

20 (A) in subsection (a)(2), by striking “Com-  
21 puter System Security and Privacy Advisory  
22 Board under section 20(f)” and inserting “In-  
23 formation Security and Privacy Advisory Board  
24 under section 21”; and

1 (B) in subsection (e)(1), by striking “Com-  
2 puter System Security and Privacy Advisory  
3 Board” and inserting “Information Security  
4 and Privacy Advisory Board under section 21”.

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

7 (a) DEFINITIONS.—In this section—

8 (1) the terms “agent of a foreign power” and  
9 “foreign power” have the meaning given those terms  
10 in section 101(a) of the Foreign Intelligence Surveil-  
11 lance Act of 1978 (50 U.S.C. 1801);

12 (2) the term “covered person”—

13 (A) means an individual, partnership, asso-  
14 ciation, joint stock company, trust, or corpora-  
15 tion; and

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

18 (3) the term “covered product” means any com-  
19 puter hardware, computer software, or electronic de-  
20 vice that is made available to the general public; and

21 (4) the term “element of the intelligence com-  
22 munity” means an element of the intelligence com-  
23 munity specified in or designated under section 3(4)  
24 of the National Security Act of 1947 (50 U.S.C.  
25 3003(4)).

1 (b) SECURITY OF COVERED PRODUCTS.—

2 (1) PROHIBITIONS.—

3 (A) PROHIBITION ON INTERCEPTION.—EX-  
4 cept as provided in paragraph (2), an agency or  
5 department of the Federal Government may not  
6 intercept any shipment of covered products for  
7 the purpose of intentionally introducing into the  
8 covered products a mechanism or device that  
9 would allow an agency or department of the  
10 Federal Government to circumvent the privacy,  
11 security, or encryption protections of the cov-  
12 ered products.

13 (B) PROHIBITION ON REQUIRING OR CON-  
14 TRACTING FOR INSTALLATION OF DEVICES.—  
15 Except as provided in paragraph (2), an ele-  
16 ment of the intelligence community may not re-  
17 quire, or contract with, a manufacturer or de-  
18 veloper of covered products to place a mecha-  
19 nism or device into a covered product that  
20 would allow any agency or department of the  
21 Federal Government to circumvent any privacy,  
22 security, or encryption protections of the cov-  
23 ered product.

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

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

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

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

9 (c) ENFORCEMENT.—

10 (1) AUTHORIZATION OF CIVIL ACTION.—A cov-  
11 ered person that suffers an injury proximately  
12 caused by a violation of subsection (b) may bring a  
13 civil action against the United States in a district  
14 court of the United States to recover money dam-  
15 ages in accordance with paragraph (2) of this sub-  
16 section.

17 (2) AMOUNT OF DAMAGES.—A court, in award-  
18 ing money damages to a covered person in a civil ac-  
19 tion brought under this subsection, shall award—

20 (A) an amount that is the greater of—

21 (i) the amount of actual damages; or

22 (ii) \$10,000; and

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

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

5           (4) REIMBURSEMENT OF AWARD.—An agency  
6 or department of the United States, including an  
7 element of the intelligence community, shall deposit  
8 into the general fund of the Treasury of the United  
9 States an amount equal to any amount awarded  
10 under paragraph (2), for a violation of subsection  
11 (b) by the agency or department, out of any appro-  
12 priation, fund, or other account (excluding any part  
13 of such appropriation, fund, or account that is avail-  
14 able for the enforcement of any Federal law) that is  
15 available for the operating expenses of the agency or  
16 department.

17           (5) DEFENSE OF GOOD FAITH RELIANCE.—The  
18 United States shall not be liable to a covered person  
19 in a civil action brought under this subsection based  
20 on any action taken by an individual acting on be-  
21 half of an agency or department of the United  
22 States, including an element of the intelligence com-  
23 munity, if the individual acted in a good faith reli-  
24 ance on a court order, a grand jury subpoena, or a  
25 legislative authorization under—



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

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

○