

115TH CONGRESS
1ST SESSION

S. 770

To require the Director of the National Institute of Standards and Technology to disseminate resources to help reduce small business cybersecurity risks, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 29, 2017

Mr. SCHATZ (for himself, Mr. RISCH, Mr. THUNE, Ms. CANTWELL, and Mr. NELSON) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To require the Director of the National Institute of Standards and Technology to disseminate resources to help reduce small business cybersecurity risks, and for other purposes.

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 “Making Available In-
5 formation Now to Strengthen Trust and Resilience and
6 Enhance Enterprise Technology Cybersecurity Act of
7 2017” or the “MAIN STREET Cybersecurity Act of
8 2017”.

1 **SEC. 2. FINDINGS.**

2 Congress makes the following findings:

3 (1) Small businesses play a vital role in the
4 economy of the United States, accounting for 54
5 percent of all United States sales and 55 percent of
6 jobs in the United States.

7 (2) Attacks targeting small and medium busi-
8 nesses account for a high percentage of cyberattacks
9 in the United States. Sixty percent of small busi-
10 nesses that suffer a cyberattack are out of business
11 within 6 months, according to the National Cyber
12 Security Alliance.

13 (3) The Cybersecurity Enhancement Act of
14 2014 (15 U.S.C. 7421 et seq.) calls on the National
15 Institute of Standards and Technology to facilitate
16 and support a voluntary public-private partnership
17 to reduce cybersecurity risks to critical infrastruc-
18 ture. Such a partnership continues to play a key role
19 in improving the cyber resilience of the United
20 States and making cyberspace safer.

21 (4) There is a need to develop simplified re-
22 sources that are consistent with the partnership de-
23 scribed in paragraph (3) that improves its use by
24 small businesses.

1 **SEC. 3. IMPROVING CYBERSECURITY OF SMALL BUSI-**
2 **NESSES.**

3 (a) **DEFINITIONS.**—In this section:

4 (1) **DIRECTOR.**—The term “Director” means
5 the Director of the National Institute of Standards
6 and Technology.

7 (2) **RESOURCES.**—The term “resources” means
8 guidelines, tools, best practices, standards, meth-
9 odologies, and other ways of providing information.

10 (3) **SMALL BUSINESS CONCERN.**—The term
11 “small business concern” has the meaning given
12 such term in section 3 of the Small Business Act
13 (15 U.S.C. 632).

14 (b) **SMALL BUSINESS CYBERSECURITY.**—Section
15 2(e)(1)(A) of the National Institute of Standards and
16 Technology Act (15 U.S.C. 272(e)(1)(A)) is amended—

17 (1) in clause (vii), by striking “and” at the end;

18 (2) by redesignating clause (viii) as clause (ix);

19 and

20 (3) by inserting after clause (vii) the following:

21 “(viii) consider small business con-
22 cerns (as defined in section 3 of the Small
23 Business Act (15 U.S.C. 632)); and”.

24 (c) **DISSEMINATION OF RESOURCES FOR SMALL**
25 **BUSINESSES.**—

1 (1) IN GENERAL.—Not later than one year
2 after the date of the enactment of this Act, the Di-
3 rector, in carrying out section 2(e)(1)(A)(viii) of the
4 National Institute of Standards and Technology Act,
5 as added by subsection (b) of this Act, in consulta-
6 tion with the heads of such other Federal agencies
7 as the Director considers appropriate, shall dissemi-
8 nate clear and concise resources for small business
9 concerns to help reduce their cybersecurity risks.

10 (2) REQUIREMENTS.—The Director shall en-
11 sure that the resources disseminated pursuant to
12 paragraph (1)—

13 (A) are effective and usable by small busi-
14 ness concerns;

15 (B) vary with the nature and size of the
16 implementing small business concern, and the
17 nature and sensitivity of the data collected or
18 stored on the information systems or devices of
19 the implementing small business concern;

20 (C) include elements, such as simple, basic
21 controls, to assist small business concerns in
22 defending against common cybersecurity risks;

23 (D) are technology-neutral and can be im-
24 plemented using technologies that are commer-
25 cial and off-the-shelf; and

1 (E) are based on international standards
2 to the extent possible, and are consistent with
3 the Stevenson-Wydler Technology Innovation
4 Act of 1980 (15 U.S.C. 3701 et seq.).

5 (3) NATIONAL CYBERSECURITY AWARENESS
6 AND EDUCATION PROGRAM.—The Director shall en-
7 sure that the resources disseminated under para-
8 graph (1) are consistent with the efforts of the Di-
9 rector under section 401 of the Cybersecurity En-
10 hancement Act of 2014 (15 U.S.C. 7451).

11 (4) SMALL BUSINESS DEVELOPMENT CENTER
12 CYBER STRATEGY.—In carrying out paragraph (1),
13 the Director, to the extent practicable, shall consider
14 any methods included in the Small Business Devel-
15 opment Center Cyber Strategy developed under sec-
16 tion 1841(a)(3)(B) of the National Defense Author-
17 ization Act for Fiscal Year 2017 (Public Law 114–
18 328).

19 (5) VOLUNTARY RESOURCES.—The use of the
20 resources disseminated under paragraph (1) shall be
21 considered voluntary.

22 (6) UPDATES.—The Director shall review and,
23 if necessary, update the resources disseminated
24 under paragraph (1).

1 (7) PUBLIC AVAILABILITY.—The Director and
2 such heads of other Federal agencies as the Director
3 considers appropriate shall each make prominently
4 available to the public on the Director’s or head’s
5 Internet website, as the case may be, information
6 about the resources disseminated under paragraph
7 (1). The Director and the heads shall each ensure
8 that the information they respectively make promi-
9 nently available is consistent, clear, and concise.

10 (d) CONSISTENCY OF RESOURCES PUBLISHED BY
11 FEDERAL AGENCIES.—If a Federal agency publishes re-
12 sources to help small business concerns reduce their cyber-
13 security risks, the head of such Federal agency, to the de-
14 gree practicable, shall make such resources consistent with
15 the resources disseminated under subsection (c)(1).

16 (e) OTHER FEDERAL CYBERSECURITY REQUIRE-
17 MENTS.—Nothing in this section may be construed to su-
18 persede, alter, or otherwise affect any cybersecurity re-
19 quirements applicable to Federal agencies.

○