

Calendar No. 217

115TH CONGRESS
1ST SESSION

S. 770

[Report No. 115–153]

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, Mr. NELSON, Mr. GARDNER, Ms. CORTEZ MASTO, Ms. HASSAN, Mrs. MCCASKILL, and Mrs. GILLIBRAND) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

SEPTEMBER 11, 2017

Reported by Mr. THUNE, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italie*]

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Making Available In-
3 formation Now to Strengthen Trust and Resilience and
4 Enhance Enterprise Technology Cybersecurity Act of
5 2017” or the “MAIN STREET Cybersecurity Act of
6 2017”.

7 **SEC. 2. FINDINGS.**

8 Congress makes the following findings:

9 (1) Small businesses play a vital role in the
10 economy of the United States, accounting for 54
11 percent of all United States sales and 55 percent of
12 jobs in the United States.

13 (2) Attacks targeting small and medium busi-
14 nesses account for a high percentage of cyberattacks
15 in the United States. Sixty percent of small busi-
16 nesses that suffer a cyberattack are out of business
17 within 6 months, according to the National Cyber
18 Security Alliance.

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

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

5 **SEC. 3. IMPROVING CYBERSECURITY OF SMALL BUSI-**
 6 **NESSES.**

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

8 (1) **DIRECTOR.**—The term “Director” means
 9 the Director of the National Institute of Standards
 10 and Technology.

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

14 (3) **SMALL BUSINESS CONCERN.**—The term
 15 “small business concern” has the meaning given
 16 such term in section 3 of the Small Business Act
 17 (15 U.S.C. 632).

18 (b) **SMALL BUSINESS CYBERSECURITY.**—Section
 19 2(e)(1)(A) of the National Institute of Standards and
 20 Technology Act (15 U.S.C. 272(e)(1)(A)) is amended—

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

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

23 and

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

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

4 (c) DISSEMINATION OF RESOURCES FOR SMALL
 5 BUSINESSES.—

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

15 (2) REQUIREMENTS.—The Director shall en-
 16 sure that the resources disseminated pursuant to
 17 paragraph (1)—

18 (A) are effective and usable by small busi-
 19 ness concerns;

20 (B) vary with the nature and size of the
 21 implementing small business concern, and the
 22 nature and sensitivity of the data collected or
 23 stored on the information systems or devices of
 24 the implementing small business concern;

1 (C) include elements, such as simple, basic
 2 controls, to assist small business concerns in
 3 defending against common cybersecurity risks;

4 (D) are technology-neutral and can be im-
 5 plemented using technologies that are commer-
 6 cial and off-the-shelf; and

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

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

17 (4) SMALL BUSINESS DEVELOPMENT CENTER
 18 CYBER STRATEGY.—In carrying out paragraph (1),
 19 the Director, to the extent practicable, shall consider
 20 any methods included in the Small Business Devel-
 21 opment Center Cyber Strategy developed under sec-
 22 tion 1841(a)(3)(B) of the National Defense Author-
 23 ization Act for Fiscal Year 2017 (Public Law 114–
 24 328).

1 (5) ~~VOLUNTARY RESOURCES.~~—The use of the
 2 resources disseminated under paragraph (1) shall be
 3 considered voluntary.

4 (6) ~~UPDATES.~~—The Director shall review and,
 5 if necessary, update the resources disseminated
 6 under paragraph (1).

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

16 (d) ~~CONSISTENCY OF RESOURCES PUBLISHED BY~~
 17 ~~FEDERAL AGENCIES.~~—If a Federal agency publishes re-
 18 sources to help small business concerns reduce their cyber-
 19 security risks, the head of such Federal agency, to the de-
 20 gree practicable, shall make such resources consistent with
 21 the resources disseminated under subsection (c)(1).

22 (e) ~~OTHER FEDERAL CYBERSECURITY REQUIRE-~~
 23 ~~MENTS.~~—Nothing in this section may be construed to su-
 24 persede, alter, or otherwise affect any cybersecurity re-
 25 quirements applicable to Federal agencies.

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “Making Available Infor-*
 3 *mation Now to Strengthen Trust and Resilience and En-*
 4 *hance Enterprise Technology Cybersecurity Act of 2017” or*
 5 *the “MAIN STREET Cybersecurity Act of 2017”.*

6 **SEC. 2. FINDINGS.**

7 *Congress makes the following findings:*

8 *(1) Small businesses play a vital role in the*
 9 *economy of the United States, accounting for 54 per-*
 10 *cent of all United States sales and 55 percent of jobs*
 11 *in the United States.*

12 *(2) Attacks targeting small and medium busi-*
 13 *nesses account for a high percentage of cyberattacks in*
 14 *the United States. Sixty percent of small businesses*
 15 *that suffer a cyberattack are out of business within 6*
 16 *months, according to the National Cyber Security Al-*
 17 *liance.*

18 *(3) The Cybersecurity Enhancement Act of 2014*
 19 *(15 U.S.C. 7421 et seq.) calls on the National Insti-*
 20 *tute of Standards and Technology to facilitate and*
 21 *support a voluntary public-private partnership to re-*
 22 *duce cybersecurity risks to critical infrastructure.*
 23 *Such a partnership continues to play a key role in*
 24 *improving the cyber resilience of the United States*
 25 *and making cyberspace safer.*

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

5 **SEC. 3. IMPROVING CYBERSECURITY OF SMALL BUSI-**
 6 **NESSES.**

7 (a) *DEFINITIONS.—In this section:*

8 (1) *DIRECTOR.—The term “Director” means the*
 9 *Director of the National Institute of Standards and*
 10 *Technology.*

11 (2) *RESOURCES.—The term “resources” means*
 12 *guidelines, tools, best practices, standards, methodolo-*
 13 *gies, and other ways of providing information.*

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

18 (b) *SMALL BUSINESS CYBERSECURITY.—Section*
 19 *2(e)(1)(A) of the National Institute of Standards and Tech-*
 20 *nology Act (15 U.S.C. 272(e)(1)(A)) is amended—*

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

22 (2) *by redesignating clause (viii) as clause (ix);*

23 *and*

24 (3) *by inserting after clause (vii) the following:*

1 “(viii) consider small business concerns
 2 (as defined in section 3 of the Small Busi-
 3 ness Act (15 U.S.C. 632)); and”.

4 (c) *DISSEMINATION OF RESOURCES FOR SMALL BUSI-*
 5 *NESSES.*—

6 (1) *IN GENERAL.*—Not later than one year after
 7 the date of the enactment of this Act, the Director, in
 8 carrying out section 2(e)(1)(A)(viii) of the National
 9 Institute of Standards and Technology Act, as added
 10 by subsection (b) of this Act, in consultation with the
 11 heads of such other Federal agencies as the Director
 12 considers appropriate, shall disseminate clear and
 13 concise resources for small business concerns to help
 14 reduce their cybersecurity risks.

15 (2) *REQUIREMENTS.*—The Director shall ensure
 16 that the resources disseminated pursuant to para-
 17 graph (1)—

18 (A) are generally applicable and usable by
 19 a wide range of small business concerns;

20 (B) vary with the nature and size of the im-
 21 plementing small business concern, and the na-
 22 ture and sensitivity of the data collected or
 23 stored on the information systems or devices of
 24 the implementing small business concern;

1 (C) include elements that promote aware-
 2 ness of simple, basic controls, a workplace cyber-
 3 security culture, and third party stakeholder re-
 4 lationships, to assist small business concerns in
 5 mitigating common cybersecurity risks;

6 (D) are technology-neutral and can be im-
 7 plemented using technologies that are commercial
 8 and off-the-shelf; and

9 (E) are based on international standards to
 10 the extent possible, and are consistent with the
 11 Stevenson-Wydler Technology Innovation Act of
 12 1980 (15 U.S.C. 3701 et seq.).

13 (3) NATIONAL CYBERSECURITY AWARENESS AND
 14 EDUCATION PROGRAM.—The Director shall ensure
 15 that the resources disseminated under paragraph (1)
 16 are consistent with the efforts of the Director under
 17 section 401 of the Cybersecurity Enhancement Act of
 18 2014 (15 U.S.C. 7451).

19 (4) SMALL BUSINESS DEVELOPMENT CENTER
 20 CYBER STRATEGY.—In carrying out paragraph (1),
 21 the Director, to the extent practicable, shall consider
 22 any methods included in the Small Business Develop-
 23 ment Center Cyber Strategy developed under section
 24 1841(a)(3)(B) of the National Defense Authorization
 25 Act for Fiscal Year 2017 (Public Law 114–328).

1 (5) *VOLUNTARY RESOURCES.*—*The use of the re-*
2 *sources disseminated under paragraph (1) shall be*
3 *considered voluntary.*

4 (6) *UPDATES.*—*The Director shall review and, if*
5 *necessary, update the resources disseminated under*
6 *paragraph (1) in accordance with the requirements*
7 *under paragraph (2).*

8 (7) *PUBLIC AVAILABILITY.*—*The Director and*
9 *such heads of other Federal agencies as the Director*
10 *considers appropriate shall each make prominently*
11 *available to the public on the Director's or head's*
12 *Internet website, as the case may be, information*
13 *about the resources and all updates to them dissemi-*
14 *nated under paragraph (1). The Director and the*
15 *heads shall each ensure that the information they re-*
16 *spectively make prominently available is consistent,*
17 *clear, and concise.*

18 (d) *CONSISTENCY OF RESOURCES PUBLISHED BY*
19 *FEDERAL AGENCIES.*—*If a Federal agency publishes re-*
20 *sources to help small business concerns reduce their cyberse-*
21 *curity risks, the head of such Federal agency, to the degree*
22 *practicable, shall make such resources consistent with the*
23 *resources disseminated under subsection (c)(1).*

24 (e) *OTHER FEDERAL CYBERSECURITY REQUIRE-*
25 *MENTS.*—*Nothing in this section may be construed to super-*

1 *sedes, alter, or otherwise affect any cybersecurity require-*
2 *ments applicable to Federal agencies.*

Calendar No. 217

115TH CONGRESS
1ST Session

S. 770

[Report No. 115–153]

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.

SEPTEMBER 11, 2017

Reported with an amendment