

115TH CONGRESS
1ST SESSION

H. R. 2105

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

IN THE HOUSE OF REPRESENTATIVES

APRIL 20, 2017

Mr. WEBSTER of Florida (for himself, Mr. LIPINSKI, Mr. SMITH of Texas, Mrs. COMSTOCK, Ms. ROSEN, Mr. HULTGREN, Mr. KNIGHT, Mr. LAHOOD, Mr. MARSHALL, and Mr. POSEY) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

A BILL

To require the Director of the National Institute of Standards and Technology to disseminate guidance 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 “NIST Small Business
5 Cybersecurity Act of 2017”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

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

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

11 (3) The Cybersecurity Enhancement Act of
12 2014 (15 U.S.C. 7421 et seq.) calls on the National
13 Institute of Standards and Technology to facilitate
14 and support a voluntary public-private partnership
15 to reduce cybersecurity risks to critical infrastruc-
16 ture. Such a partnership continues to play a key role
17 in improving the cyber resilience of the United
18 States and making cyberspace safer.

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

23 **SEC. 3. IMPROVING CYBERSECURITY OF SMALL BUSI-**
24 **NESSES.**

25 (a) DEFINITIONS.—In this section:

1 (1) DIRECTOR.—The term “Director” means
2 the Director of the National Institute of Standards
3 and Technology.

4 (2) RESOURCES.—The term “resources” means
5 guidelines, tools, best practices, standards, meth-
6 odologies, and other ways of providing information.

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

11 (b) SMALL BUSINESS CYBERSECURITY.—Section
12 2(e)(1)(A) of the National Institute of Standards and
13 Technology Act (15 U.S.C. 272(e)(1)(A)) is amended—

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

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

16 and

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

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

21 (c) DISSEMINATION OF RESOURCES FOR SMALL
22 BUSINESSES.—

23 (1) IN GENERAL.—Not later than one year
24 after the date of the enactment of this Act, the Di-
25 rector, in carrying out section 2(e)(1)(A)(viii) of the

1 National Institute of Standards and Technology Act,
2 as added by subsection (b) of this Act, in consulta-
3 tion with the heads of other appropriate Federal
4 agencies, shall disseminate clear and concise re-
5 sources to help small business concerns identify, as-
6 sess, manage, and reduce their cybersecurity risks.

7 (2) REQUIREMENTS.—The Director shall en-
8 sure that the resources disseminated pursuant to
9 paragraph (1)—

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

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

17 (C) include elements, that promote aware-
18 ness of simple, basic controls, a workplace cy-
19 bersecurity culture, and third-party stakeholder
20 relationships, to assist small business concerns
21 in mitigating common cybersecurity risks;

22 (D) are technology-neutral and can be im-
23 plemented using technologies that are commer-
24 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) in accordance with the require-
25 ments under paragraph (2).

1 (7) PUBLIC AVAILABILITY.—The Director and
2 the head of each Federal agency that so elects shall
3 make prominently available on the respective agen-
4 cy’s public Internet website information about the
5 resources and updates to the resources disseminated
6 under paragraph (1). The Director and the heads
7 shall each ensure that the information they respec-
8 tively make prominently available is consistent, clear,
9 and concise.

10 (d) OTHER FEDERAL CYBERSECURITY REQUIRE-
11 MENTS.—Nothing in this section may be construed to su-
12 persede, alter, or otherwise affect any cybersecurity re-
13 quirements applicable to Federal agencies.

14 (e) FUNDING.—This Act shall be carried out using
15 funds otherwise authorized to be appropriated or made
16 available to the National Institute of Standards and Tech-
17 nology.

○