114TH CONGRESS
2D SESSION

S. _____

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

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 _____

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.

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 ''Making Available Information Now to Strengthen Trust and Resilience and Enhance Enterprise Technology Cybersecurity Act of 2017'' or the ''MAIN STREET Cybersecurity Act of 2017''.

SEC. 2. FINDINGS.

Congress makes the following findings:

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

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

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

(4) There is a need to develop simplified resources that are consistent with the partnership described in paragraph (3) that improves its use by small businesses.

SEC. 3. IMPROVING CYBERSECURITY OF SMALL BUSINESSES.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) RESOURCES.—The term ''resources'' means guidelines, tools, best practices, standards, methodologies, and other ways of providing information.

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

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

(1) in clause (vii), by striking ''and'' at the end;

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

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

''(viii) consider small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)); and''.

(c) DISSEMINATION OF RESOURCES FOR SMALL BUSINESSES.—

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

(2) REQUIREMENTS.—The Director shall ensure that the resources disseminated pursuant to paragraph (1)—

(A) are effective and usable by small business concerns; and

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

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

(D) are technology-neutral and can be implemented using technologies that are commercial and off-the-shelf; and

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

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

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

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

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

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

(d) CONSISTENCY OF RESOURCES PUBLISHED BY FEDERAL AGENCIES.—If a Federal agency publishes resources to help small business concerns reduce their cybersecurity risks, the head of such Federal agency, to the degree practicable, shall make such resources consistent with the resources disseminated under subsection (c)(1).

(e) OTHER FEDERAL CYBERSECURITY REQUIREMENTS.—Nothing in this section may be construed to supersede, alter, or otherwise affect any cybersecurity requirements applicable to Federal agencies.