Texas, Washington, and Florida, and Jewish cemeteries have been desecrated in the States of Missouri and Pennsylvania;

Whereas, in 2017, there has been harassment and hate-based violence against individuals who are perceived to be Muslim, including members of South Asian communities in the United States, and Hindu and Sikh Americans have been the target of hate-based violence targeting religious minorities; and

Whereas, on February 28, 2017, President Donald Trump, before a joint session of Congress, acknowledged threats targeting Jewish community centers and the vandalism of Jewish cemeteries, and stated that ''we are a country that stands united in condemning hate and evil in all of its very ugly forms'': Now, therefore, be it

Resolved, That the House of Representatives—

(1) affirms that the United States stands united in condemning hate and evil in all forms;

(2) rejects hate-motivated crime as an attack on the fabric of the society of the United States and the ideals of pluralism and respect;

(3) condemns hate crime and any other form of racism, religious or ethnic bias, discrimination, incitement to violence, or animus targeting a minority in the United States;

(4) calls on Federal law enforcement officials, working with State and local officials—

(A) to expeditiously investigate all credible reports of hate crimes and incidents and threats against minorities in the United States; and

(B) to hold the perpetrators of those crimes, incidents, or threats accountable and bring the perpetrators to justice;

(5) encourages the Department of Justice and other Federal agencies—

(A) to work to improve the reporting of hate crimes; and

(B) to emphasize the importance of the agencies' collection and reporting of data pursuant to Federal law;

(6) encourages the development of an interagency task force led by the Attorney General and bringing together the Department of Justice, the Department of Homeland Security, the Department of Education, the Department of State, the Federal Bureau of Investigation, and the Office of the Director of National Intelligence to collaborate on the development of effective strategies and efforts to detect and deter hate crime in order to protect minority communities; and

(7) calls on the executive branch—

(A) to offer Federal assistance that may be available for victims of hate crimes; and

(B) to enhance security measures and improve preparedness for religious institutions, places of worship, and other institutions that have been targeted because of the affiliation of the institutions with any particular religious, racial, or ethnic minority in the United States.

The resolution was agreed to.

A motion to reconsider was laid on the table.

MAKING AVAILABLE INFORMATION NOW TO STRENGTHEN TRUST AND RESILIENCE AND ENHANCE ENTERPRISE TECHNOLOGY CYBERSECURITY ACT OF 2017

Mr. WEBSTER of Florida. Mr. Speaker, I ask unanimous consent to take from the Speaker's table the bill (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, and ask for its immediate consideration in the House.

The Clerk read the title of the bill.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

The text of the bill is as follows:

S. 770

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.

(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 generally applicable and usable by a wide range of small business concerns;

(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 that promote awareness of simple, basic controls, a workplace cybersecurity culture, and third party stakeholder relationships, to assist small business concerns in mitigating 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) in accordance with the requirements under paragraph (2).

(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 and all updates to them 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.

AMENDMENT OFFERED BY MR. WEBSTER OF FLORIDA

Mr. WEBSTER of Florida. Mr. Speaker, I have an amendment at the desk.

The Clerk read as follows:

Amendment offered by Mr. WEBSTER of Florida:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''NIST Small Business Cybersecurity Act''.

SEC. 2. 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 other appropriate Federal agencies, shall disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks.

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

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

(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, that promote awareness of simple, basic controls, a workplace cybersecurity culture, and third-party stakeholder relationships, to assist small business concerns in mitigating common cybersecurity risks;

(D) include case studies of practical application;

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

(F) 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) in accordance with the requirements under paragraph (2).

(7) PUBLIC AVAILABILITY.—The Director and the head of each Federal agency that so elects shall make prominently available on the respective agency's public Internet website information about the resources and updates to 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) OTHER FEDERAL CYBERSECURITY REQUIREMENTS.—Nothing in this section may be construed to supersede, alter, or otherwise affect any cybersecurity requirements applicable to Federal agencies.

(e) FUNDING.—This Act shall be carried out using funds otherwise authorized to be appropriated or made available to the National Institute of Standards and Technology.

Mr. WEBSTER of Florida (during the reading). Mr. Speaker, I ask unanimous consent to dispense with the reading.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

The amendment was agreed to.

The bill was ordered to be read a third time, was read the third time, and passed.

The title of the bill was amended so as to read: ''An Act 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.''

A motion to reconsider was laid on the table.

CONFERENCE REPORT ON H.R. 5515, NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019

Mr. THORNBERRY submitted the following conference report and statement on the bill (H.R. 5515) to authorize appropriations for fiscal year 2019 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes:

CONFERENCE REPORT (H. REPT. 115–874)

The committee of conference on the disagreeing votes of the two Houses on the amendment of the Senate to the bill (H.R. 5515), to authorize appropriations for fiscal year 2019 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes, having met, after full and free conference, have agreed to recommend and do recommend to their respective Houses as follows:

That the House recede from its disagreement to the amendment of the Senate and agree to the same with an amendment as follows:

In lieu of the matter proposed to be inserted by the Senate amendment, insert the following:

SECTION 1. SHORT TITLE.

(a) IN GENERAL.—This Act may be cited as the ''John S. McCain National Defense Authorization Act for Fiscal Year 2019''.

(b) REFERENCES.—Any reference in this or any other Act to the ''National Defense Authorization Act for Fiscal Year 2019'' shall be deemed to be a reference to the ''John S. McCain National Defense Authorization Act for Fiscal Year 2019''.

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:

(1) Division A—Department of Defense Authorizations.

(2) Division B—Military Construction Authorizations.

(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.

(4) Division D—Funding Tables.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows: