The PRESIDING OFFICER. Without objection, it is so ordered.

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2019

Mrs. FISCHER. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 36, S. 333.

The PRESIDING OFFICER. The clerk will report the bill by title.

The senior assistant legislative clerk read as follows:

A bill (S. 333) to authorize the Secretary of Homeland Security to work with cybersecurity consortia for training, and for other purposes.

There being no objection, the Senate proceeded to consider the bill, which had been reported from the Committee on Homeland Security and Governmental Affairs.

Mrs. FISCHER. I ask unanimous consent that the bill be considered read a third time and passed and that the motion to reconsider be considered made and laid upon the table.

The PRESIDING OFFICER. Without objection, it is so ordered.

The bill (S. 333) was ordered to be engrossed for a third reading, was read the third time, and passed, as follows:

S. 333

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 ''National Cybersecurity Preparedness Consortium Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''consortium'' means a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security;

(2) the terms ''cybersecurity risk'' and ''incident'' have the meanings given those terms in section 2209(a) of the Homeland Security Act of 2002 (6 U.S.C. 659(a));

(3) the term ''Department'' means the Department of Homeland Security; and

(4) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 3. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary may work with a consortium to support efforts to address cybersecurity risks and incidents.

(b) ASSISTANCE TO THE NCCIC.—The Secretary may work with a consortium to assist the national cybersecurity and communications integration center of the Department (established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659)) to—

(1) provide training to State and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, in accordance with applicable law;

(2) develop and update a curriculum utilizing existing programs and models in accordance with such section 2209, for State and local first responders and officials, related to cybersecurity risks and incidents;

(3) provide technical assistance services to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with such section 2209;

(4) conduct cross-sector cybersecurity training and simulation exercises for entities, including State and local governments, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, in accordance with section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c));

(5) help States and communities develop cybersecurity information sharing programs, in accordance with section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), for the dissemination of homeland security information related to cybersecurity risks and incidents; and

(6) help incorporate cybersecurity risk and incident prevention and response into existing State and local emergency plans, including continuity of operations plans.

(c) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this Act, the Secretary shall take into consideration the following:

(1) Any prior experience conducting cybersecurity training and exercises for State and local entities.

(2) Geographic diversity of the members of any such consortium so as to cover different regions throughout the United States.

(d) METRICS.—If the Secretary works with a consortium under subsection (a), the Secretary shall measure the effectiveness of the activities undertaken by the consortium under this Act.

(e) OUTREACH.—The Secretary shall conduct outreach to universities and colleges, including historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, and other minority-serving institutions, regarding opportunities to support efforts to address cybersecurity risks and incidents, by working with the Secretary under subsection (a).

SEC. 4. RULE OF CONSTRUCTION.

Nothing in this Act may be construed to authorize a consortium to control or direct any law enforcement agency in the exercise of the duties of the law enforcement agency.

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2019

Mrs. FISCHER. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 194, S. 1846.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the bill by title.

The senior assistant legislative clerk read as follows:

A bill (S. 1846) to amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, and for other purposes.

The PRESIDING OFFICER. Is there objection to proceeding to the measure?

There being no objection, the Senate proceeded to consider the bill, which had been reported from the Committee on Homeland Security and Governmental Affairs, with an amendment as follows:

(The part of the bill intended to be stricken is shown in boldfaced brackets.)

S. 1846

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 ''State and Local Government Cybersecurity Act of 2019''.

SEC. 2. AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.

Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2201 (6 U.S.C. 651)—

(A) by redesignating paragraphs (4), (5), and (6) as paragraphs (5), (6), and (7), respectively; and

(B) by inserting after paragraph (3) the following:

''(4) ENTITY.—The term 'entity' shall include—

''(A) an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestically or foreign owned, that has the legal capacity to enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued in its own right in a court of competent jurisdiction in the United States, and to be held responsible for its actions;

''(B) a governmental agency or other governmental entity, including State, local, Tribal, and territorial government entities; and

''(C) the general public.''; and

(2) in section 2202 (6 U.S.C. 652)—

(A) in subsection (c)—

(i) in paragraph (10), by striking ''and'' at the end;

(ii) by redesignating paragraph (11) as paragraph (12); and

(iii) by inserting after paragraph (10) the following:

''(11) carry out the authority of the Secretary under subsection (e)(1)(R); and''; and

(B) in subsection (e)(1), by adding at the end the following:

''(R) To make grants to and enter into cooperative agreements or contracts with States, local governments, and other non-Federal entities as the Secretary determines necessary to carry out the responsibilities of the Secretary related to cybersecurity and infrastructure security under this Act and any other provision of law, including grants, cooperative agreements, and contracts that provide assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings.''; and

(3) in section 2209 (6 U.S.C. 659)—

(A) in subsection (c)(6), by inserting ''operational and'' after ''timely'';

(B) in subsection (d)(1)(E), by inserting '', including an entity that collaborates with election officials,'' after ''governments''; and

(C) by adding at the end the following:

''(n) COORDINATION ON CYBERSECURITY FOR FEDERAL AND NON-FEDERAL ENTITIES.—

''(1) COORDINATION.—The Center shall, to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

''(A) conduct exercises with Federal and non-Federal entities;

''(B) provide operational and technical cybersecurity training related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents to Federal and non-Federal entities to address cybersecurity risks or incidents, with or without reimbursement;

''(C) assist Federal and non-Federal entities, upon request, in sharing cyber threat