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

indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents;

''(D) provide notifications containing specific incident and malware information that may affect them or their customers and residents;

''(E) provide and periodically update via a web portal and other means tools, products, resources, policies, guidelines, controls, and other cybersecurity standards and best practices and procedures related to information security;

''(F) work with senior Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and through national associations, to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure and ensure the resiliency of Federal and non-Federal information systems and including election systems;

''(G) provide, upon request, operational and technical assistance to Federal and non-Federal entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist those Federal and non-Federal entities in detecting cybersecurity risks and incidents;

''(H) assist Federal and non-Federal entities in developing policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry;

''(I) ensure that Federal and non-Federal entities, as appropriate, are made aware of the tools, products, resources, policies, guidelines, controls, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of civilian information systems; and

''(J) promote cybersecurity education and awareness through engagements with Federal and non-Federal entities.

''(o) REPORT.—Not later than 1 year after the date of enactment of this subsection, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the status of cybersecurity measures that are in place, and any gaps that exist, in each State and in the largest urban areas of the United States.

[''(p) PILOT DEPLOYMENT OF SENSORS.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this subsection, the Secretary shall establish a pilot program to deploy network sensors capable of utilizing classified indicators for the purpose of identifying and filtering malicious network traffic.

''(2) VOLUNTARY PARTICIPATION.—Activities related to the pilot program established under this subsection may only be carried out on a voluntary basis in coordination with the owner of the impacted network.

''(3) EXPANSION AUTHORITY.—If, after 12 months of deployment, the Secretary determines that the network sensors deployed pursuant to this subsection would provide network security benefits to other critical infrastructure sectors, the Secretary may make additional network sensors available to those sectors on a voluntary basis at the request of critical infrastructure owners and operators.

''(4) REPORT.—Not later than 1 year after the date on which the Secretary establishes the pilot program under this subsection, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the pilot program, which shall include—

''(A) the status of the pilot program;

''(B) the rate of voluntary participation in the pilot program;

''(C) the effectiveness of the pilot program in detecting and blocking traffic that could not have been captured without the network sensors deployed under the pilot program; and

''(D) recommendations for expanding the use of classified threat indicators to protect United States critical infrastructure.''.]

''(p) DEPLOYMENT OF ENHANCED CAPABILITIES.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this subsection, the Secretary may establish an initiative to enhance efforts to deploy technical or analytic capabilities or services that utilize classified cyber threat indicators or intelligence for the purpose of detecting or preventing malicious network traffic on unclassified non-Federal information systems.

''(2) VOLUNTARY PARTICIPATION.—Activities conducted under this subsection may only be carried out on a voluntary basis upon request of the non-Federal entity.

''(3) REPORT.—Not later than 1 year after the date on which the Secretary establishes the initiative under this subsection, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the initiative, which shall include—

''(A) the status of the initiative;

''(B) the rate of voluntary participation in the initiative;

''(C) the effectiveness of the initiative; and

''(D) recommendations for expanding the use of classified cyber threat indicators to protect non-Federal entities.''.

Mrs. FISCHER. I further ask unanimous consent that the committee-reported amendment be withdrawn; that the Peters substitute amendment, which is at the desk, be considered and agreed to; that the bill, as amended, be considered read a third time and passed; and that the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

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

The committee-reported amendment was withdrawn.

The amendment (No. 1252) in the nature of a substitute is as follows:

(Purpose: In the nature of a substitute)

Strike all after the enacting clause and insert the following:

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 domestic or foreign;

''(B) a governmental agency or other governmental entity, whether domestic or foreign, 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, Tribal, and territorial 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 indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents;

''(D) provide notifications containing specific incident and malware information that may affect them or their customers and residents;

''(E) provide and periodically update via a web portal and other means tools, products, resources, policies, guidelines, controls, and other cybersecurity standards and best practices and procedures related to information security;

''(F) work with senior Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and through national associations, to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, controls, and

procedures related to information security to secure and ensure the resiliency of Federal and non-Federal information systems and including election systems;

''(G) provide, upon request, operational and technical assistance to Federal and non-Federal entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist those Federal and non-Federal entities in detecting cybersecurity risks and incidents;

''(H) assist Federal and non-Federal entities in developing policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry;

''(I) ensure that Federal and non-Federal entities, as appropriate, are made aware of the tools, products, resources, policies, guidelines, controls, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of civilian information systems; and

''(J) promote cybersecurity education and awareness through engagements with Federal and non-Federal entities.

''(o) REPORT.—Not later than 1 year after the date of enactment of this subsection, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the status of cybersecurity measures that are in place, and any gaps that exist, in each State and in the largest urban areas of the United States.''.

The bill (S. 1846), as amended, was ordered to be engrossed for a third reading, was read the third time, and passed.

REAFFIRMING THE IMPORTANCE OF THE GENERAL SECURITY OF MILITARY INFORMATION AGREEMENT BETWEEN THE REPUBLIC OF KOREA AND JAPAN

Mrs. FISCHER. Mr. President, I ask unanimous consent that the Foreign Relations Committee be discharged from further consideration and the Senate now proceed to S. Res. 435.

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

The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 435) reaffirming the importance of the General Security of Military Information Agreement between the Republic of Korea and Japan, and for other purposes.

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

There being no objection, the committee was discharged, and the Senate proceeded to consider the resolution.

Mrs. FISCHER. I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be considered made and laid upon the table.

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

The resolution (S. Res. 435) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in the RECORD of November 20, 2019, under ''Submitted Resolutions.'')

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mrs. FISCHER. Mr. President, I ask unanimous consent that the Senate proceed to executive session for the consideration of Calendar Nos. 510 through 517 and all nominations on the Secretary's desk in the Air Force, Army, Marine Corps, Navy, Foreign Service, and Coast Guard; that the nominations be confirmed, the motions to reconsider be considered made and laid upon the table with no intervening action or debate; that no further motions be in order; that any statements related to the nominations be printed in the Record; and that the President be immediately notified of the Senate's action.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The nominations considered and confirmed en bloc are as follows:

IN THE ARMY

The following named officers for appointment to the grade indicated in the United States Army under title 10, U.S.C., section 624:

To be brigadier general

Col. Patrick R. Michaelis

The following named officer for appointment in the United States Army to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., section 601:

To be lieutenant general

Maj. Gen Daniel L. Karbler

The following named Army National Guard of the United States officer for appointment in the Reserve of the Army to the grade indicated under title 10, U.S.C., sections 12203 and 12211:

To be brigadier general

Col. Stephanie A. Purgerson

IN THE AIR FORCE

The following named officers for appointment in the Reserve of the Air Force to the grade indicated under title 10, U.S.C., section 12203:

To be brigadier general

Col. Leslie A. Beavers
Col. Robert M. Blake
Col. Melissa A. Coburn
Col. Vanessa J. Dornhoefer
Col. Lynnette J. Hebert
Col. Jeffrey F. Hill
Col. Traci L. KuekerMurphy
Col. Preston F. McFarren
Col. William D. Murphy
Col. Dana N. Nelson
Col. Robert P. Palmer
Col. David A. Piffarerio
Col. Mitchell D. Richardson
Col. William A. Rock
Col. Mark V. Slominski
Col. Max J. Stitzer
Col. Robert W. VanHoy, II
Col. Adrian K. White

The following named officers for appointment in the Reserve of the Air Force to the grade indicated under title 10, U.S.C., section 12203:

To be major general

Brig. Gen. Lee Ann T. Bennett
Brig. Gen. Jay S. Goldstein
Brig. Gen. Jeffrey S. Hinrichs
Brig. Gen. Bret C. Larson
Brig. Gen. Bryan P. Radliff
Brig. Gen. Scott A. Sauter

The following named officer for appointment in the Reserve of the Air Force to the grade indicated under title 10, U.S.C., section 12203:

To be brigadier general

Col. Darrin D. Lambrigger

IN THE ARMY

The following named Army National Guard of the United States officer for appointment in the Reserve of the Army to the grade indicated under title 10, U.S.C., sections 12203 and 12211:

To be major general

Brig. Gen. John C. Boyd

The following named Army National Guard of the United States officer for appointment in the Reserve of the Army to the grade indicated under title 10, U.S.C., sections 12203 and 12211:

To be brigadier general

Col. Damon N. Cluck

NOMINATIONS PLACED ON THE SECRETARY'S DESK

IN THE AIR FORCE

PN1115 AIR FORCE nominations

(10) beginning JEFFREY J. AUTREY, and ending JENNIFER T. VECCHIONE, which nominations were received by the Senate and appeared in the Congressional Record of September 19, 2019.

PN1269 AIR FORCE nominations

(127) beginning THOMAS JASON ABELL, and ending LAWRENCE NAHNO YAZZIE, which nominations were received by the Senate and appeared in the Congressional Record of November 12, 2019.

PN1270 AIR FORCE nomination of Joshua B. Stierwalt, which was received by the Senate and appeared in the Congressional Record of November 12, 2019.

IN THE ARMY

PN1205 ARMY nomination of Michael W. Torre, which was received by the Senate and appeared in the Congressional Record of October 15, 2019.

PN1206 ARMY nomination of Austin C. Vann, which was received by the Senate and appeared in the Congressional Record of October 15, 2019.

PN1257 ARMY nomination of Michael J. Blanton, which was received by the Senate and appeared in the Congressional Record of October 30, 2019.

PN1258 ARMY nomination of Laina G. Cafego, which was received by the Senate and appeared in the Congressional Record of October 30, 2019.

PN1259 ARMY nomination of Lyle E. Bushong, which was received by the Senate and appeared in the Congressional Record of October 30, 2019.

PN1261 ARMY nomination of Garth E. Coke, which was received by the Senate and appeared in the Congressional Record of October 30, 2019.

PN1264 ARMY nomination of Brent R. Robertson, which was received by the Senate and appeared in the Congressional Record of October 30, 2019.

PN1271 ARMY nomination of Gerald J. Hall, which was received by the Senate and appeared in the Congressional Record of November 12, 2019.

PN1272 ARMY nomination of Nicole L. Kruse, which was received by the Senate and appeared in the Congressional Record of November 12, 2019.