Calendar No. 194

116TH CONGRESS
1ST SESSION

S. 1846

[Report No. 116–90]

To amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 13, 2019

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

SEPTEMBER 10, 2019

Reported by Mr. JOHNSON, with an amendment

[Omit the part struck through and insert the part printed in italic]

A BILL

To amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, 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 ''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 Sec-

retary 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.".

Calendar No. 194

116TH CONGRESS
1ST SESSION

S. 1846

[Report No. 116–90]

A BILL

To amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, and for other purposes.

SEPTEMBER 10, 2019

Reported with an amendment