Calendar No. 152

117TH CONGRESS
1ST SESSION

S. 2520

[Report No. 117–42]

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

JULY 28, 2021

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

OCTOBER 21, 2021

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause 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 2021".~~

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.'';

(2) in section 2202 (6 U.S.C. 652)—

(A) in subsection (c)—

(i) in paragraph (11), by striking ''and'' at the end;

(ii) in the first paragraph (12), by striking ''and'' at the end;

(iii) by redesignating the second and third paragraphs (12) as paragraphs (13) and (15), respectively;

(iv) in paragraph (13), as so redesignated, by striking ''and'' at the end; and

(v) by inserting after paragraph (13), as so redesignated, the following:

''(14) carry out the authority of the Secretary under subsection (c)(1)(S); and''; and

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

''(S) 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 cyber-

security 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'' before ''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:

''(p) 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, proactive and defensive measures, cybersecurity risks and vulnerabilities, and incident response and management 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 actionable and real time 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 an easily accessible platform 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, local, Tribal, and territorial 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 pro-~~

cedures related to information security to secure and ensure the resiliency of Federal and non-Federal information systems, 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 and threat 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 ap-

~~propriate 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.~~

~~"(q) 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—~~

~~"(1) 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;~~

~~"(2) the services and capabilities that the Agency directly provides to governmental agencies or other governmental entities; and~~

~~"(3) the services and capabilities that the Agency indirectly provides to governmental agencies or other governmental entities through an entity described in section 2201(4)(B).".~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "State and Local Government Cybersecurity Act of 2021".

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), by adding at the end the following:

"(7) SLTT ENTITY.—The term 'SLTT entity' means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof."; and

(2) in section 2209 (6 U.S.C. 659)—

(A) in subsection (c)(6), by inserting "operational and" before "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:

"(p) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.—

"(1) COORDINATION.—The Center shall, upon request and 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 SLTT entities;

"(B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

"(i) cyber threat indicators;

"(ii) defensive measures;

"(iii) cybersecurity risks;

"(iv) vulnerabilities; and

"(v) incident response and management;

"(C) in order to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable—

"(i) cyber threat indicators;

"(ii) defensive measures;

"(iii) information about cybersecurity risks; and

"(iv) information about incidents;

"(D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;

"(E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—

"(i) information about tools;

"(ii) information about products;

"(iii) resources;

"(iv) policies;

"(v) guidelines;

"(vi) controls; and

"(vii) other cybersecurity standards and best practices and procedures related to information security;

"(F) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;

"(G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;

"(H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and

"(I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

"(q) 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 services and capabilities that the Agency directly and indirectly provides to SLTT entities.".

Calendar No. 152

117TH CONGRESS
1ST SESSION

S. 2520

[Report No. 117–42]

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.

OCTOBER 21, 2021

Reported with an amendment