Calendar No. 152

117th Congress *1st Session*	SENATE	REPORT 117–42

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2520

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.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

29–007 WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
MICHAEL A. GARCIA, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
ANDREW C. DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*
CARA G. MUMFORD, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 152

117th Congress
1st Session

SENATE

REPORT
117–42

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2021

OCTOBER 21, 2021.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2520]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2520) to amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2520, the State and Local Government Cybersecurity Act of 2021, amends the Homeland Security Act of 2002 to help State, local, Tribal, and territorial (SLTT) entities enhance their cybersecurity. The bill codifies and strengthens the cybersecurity relationship between the Multi-State Information Sharing and Analysis Center (MS–ISAC) and the Department of Homeland Security (DHS). It authorizes DHS to work with MS–ISAC to assist SLTT

entities by conducting cybersecurity exercises, sharing information to increase situational awareness and prevent incidents, and coordinating effective implementation of cybersecurity tools, products, resources, policies, and guidelines. The bill also directs DHS to report to Congress on any services that the Cybersecurity and Infrastructure Security Agency (CISA), directly or indirectly through the MS–ISAC, provides to SLTT entities.

II. Background and Need for the Legislation

State and local governments oversee critical, daily services that Americans rely on, such as water utilities, schools, health care facilities, and other vital services. As these services increasingly become connected to the internet, malicious cyber actors have targeted them for criminal or other malicious purposes.[1] In 2020, cybercriminals targeted at least 2,350 government entities with ransomware attacks, including nearly 1,700 educational institutions and 560 healthcare facilities.[2] Many of these public entities lack the resources to prepare for and respond to ransomware and other cyber attacks. A 2020 survey of state chief information security officers found that 70% of respondents listed ransomware as a top concern for potential breaches in part due to inadequate funding and a lack of confidence in the ability of localities to protect state information assets.[3] While DHS operates disaster preparedness grant programs that SLTT entities can use for cybersecurity purposes, only 2.35% (roughly $40 million) of those grants were used for cybersecurity in fiscal year 2019.[4]

The MS–ISAC helps SLTT entities bolster their cybersecurity through focused cyber threat prevention, protection, response, and recovery offerings and assistance.[5] The MS–ISAC is a division within the nonprofit Center for Internet Security (CIS), which also manages the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC).[6] CIS is a 20-year old organization that develops and helps businesses and governments implement cybersecurity best practices and created the MS–ISAC in 2004 to help SLTT entities with cyber prevention, protection, response, and recovery.[7] The MS–ISAC maintains its own 24/7 watch and warning center and a computer emergency response team that can provide members with cyber incident response; malware, log, and forensics analysis; reverse engineering; and vulnerability assessments.[8] DHS s 24-hour watch floor, the National Cybersecurity and Communications Integration Center (NCCIC), coordinates with the MS–ISAC

---

[1] Michael Garcia, *The Underbelly of Ransomware Attacks: Local Governments*, Council on Foreign Relations: Net Politics (blog) (May 10, 2021) (https://www.cfr.org/blog/underbelly-ransomware-attacks-local-governments).

[2] Emisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2020*, Emisoft (blog) (Jan. 18, 2021) (https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/).

[3] Deloitte Insights, *2020 Deloitte-NASCIO Cybersecurity Study* 10, 28 (2020) (https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf).

[4] Department of Homeland Security, *2020 National Preparedness Report* 46 (Dec. 2020) (https://www.fema.gov/sites/default/files/documents/fema_2020-national-preparedness-report.pdf).

[5] Center for Internet Security, MS–ISAC (https://www.cisecurity.org/ms-isac/) (accessed Sept. 27, 2021).

[6] Center for Internet Security, Elections Infrastructure ISAC (https://www.cisecurity.org/ei-isac/) (accessed Sept. 27, 2021).

[7] Center for Internet Security, About Us (https://www.cisecurity.org/about-us/) (accessed Sept. 30, 2021).

[8] Center for Internet Security, Services (https://www.cisecurity.org/ms-isac/services/) (accessed Sept. 27, 2021).

to share information and help states and localities stay on top of emerging and evolving cyber threats.[9] MS–ISAC analysts are co-located on the NCCIC watch floor and work in tandem with NCCIC analysts to improve and support the nation's cybersecurity posture.[10] Today, the MS–ISAC has over 2,500 members including government, education, utility, and transportation entities.[11]

S. 2520 codifies and strengthens the cybersecurity relationship between the MS–ISAC and DHS which will provide additional cybersecurity services to SLTT entities. The bill authorizes DHS to work with the MS–ISAC to assist SLTT entities by conducting cybersecurity exercises with them; sharing cyber threat indicators, defensive measures, cybersecurity risks, and ongoing cyber incidents to increase situational awareness and help prevent incidents; and providing notifications with specific incident and malware information. This bill will also ensure MS–ISAC can continue enhancing and expanding its work with chief information officers, senior election officials, and others to coordinate effective implementation of tools, products, resources, policies, procedures, and guidelines to ensure the resiliency of systems, including election systems. In addition to these and other activities, S.2520 directs DHS to submit a report to Congress on the cybersecurity services and capabilities that CISA, directly or indirectly through the MS–ISAC, provides to SLTT entities.

III. Legislative History

Chairman Gary Peters (D–MI) introduced S. 2520, the State and Local Government Cybersecurity Act of 2021, on July 28, 2021. Ranking Member Rob Portman (R–OH) joined as a cosponsor on August 4, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. The Committee considered S. 2520 at a business meeting on August 4, 2021. During the business meeting, a substitute amendment was offered by Chairman Peters and Ranking Member Portman. The Peters-Portman Substitute Amendment was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present. The Committee ordered the bill, as amended, reported favorably by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section designates the name of the bill as the "State and Local Government Cybersecurity Act of 2021."

---

[9] Department of Homeland Security, *NCIC Services for State, Local, Tribal, and Territorial Governments* (https://us-cert.cisa.gov/sites/default/files/publications/NCCIC%20Service%20Menu%20-%20SLTT.pdf) (accessed Sept. 27, 2021).

[10] Multi-State Information Sharing & Analysis *Center, Services Guide* 7 (Jan. 5, 2018) (https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf).

[11] Center for Internet Security, MS ISAC Membership FAQ (https://www.cisecurity.org/ms-isac/ms-isac-membership-faq/) (accessed Sept. 27, 2021).

Section 2. Amendments to the Homeland Security Act of 2002

This section amends Subtitle A of title XXII of the Homeland Security Act of 2002.

Paragraph (1) adds a definition of SLTT entity.

Paragraph (2), subparagraph (A) specifies that NCCIC will provide "operational" information on cyber threats, risks, and incidents to Federal and non-Federal entities.

Paragraph (2), subparagraph (B) adds a requirement that NCCIC will include an entity that collaborates with state and local election officials.

Paragraph (2), subparagraph (C) requires NCCIC to coordinate with Federal and non-Federal entities like the MS–ISAC to: conduct cybersecurity exercises with SLTT entities; offer operational and technical cybersecurity training for SLTT entities; assist SLTT entities with real-time information sharing; provide SLTT entities with notifications about specific incidents or malware information; provide to and periodically update SLTT entities on information about tools and products, resources, policies, guidelines, controls, and cybersecurity standards and best practices; work with senior SLTT officials to coordinate implementation of cybersecurity best practices and products; provide operational and technical assistance to help SLTT entities implement cybersecurity best practices and products; assist SLTT entities in developing their policies and procedures for coordinating vulnerability disclosures; and promote cybersecurity education and awareness. Subparagraph (C) also requires biannual reports by DHS to appropriate congressional committees on the services and capabilities that CISA directly and indirectly provides to SLTT entities.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, September 24, 2021.

Hon. Gary C. Peters,
Chairman Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2520, the State and Local Government Cybersecurity Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 2520, State and Local Government Cybersecurity Act of 2021
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on August 4, 2021

By Fiscal Year, Millions of Dollars	2021	2021-2026	2021-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	*	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 2520 would authorize the Department of Homeland Security (DHS) to coordinate with state, local, tribal, and territorial governments to enhance the cybersecurity of their information systems. Under the bill, DHS would continue to assist those governments by conducting cybersecurity exercises, providing training, and notifying them of cybersecurity threats. The bill also would require the department to report to the Congress on the effectiveness of its efforts.

DHS is already performing the coordination activities required by S. 2520; thus, the bill would codify those responsibilities but would not impose any new operating requirements on the department. CBO estimates that implementing S. 2520 would cost less than $500,000 over the 2021–2026 period to prepare and deliver the required reports; such spending would be subject to the availability of appropriations.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

* * * * * * *

Subchapter XVIII—Cybersecurity and Infrastructure Security Agency

* * * * * * *

Part A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 651. DEFINITIONS

In this part:

(1) * * *

* * * * * * *

(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.

* * * * * * *

SEC. 659. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

(a) * * *

(b) * * *

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) * * *

* * * * * * *

(6) upon request, providing *operational and timely* technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation;

* * * * * * *

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) * * *

* * * * * * *

(E) an entity that collaborates with State and local governments, *including an entity that collaborates with election officials*, on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

* * * * * * *

(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.

(p) 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.

* * * * * * *

○