

# 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.

1       *Be it enacted by the Senate and House of Representa-*

2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE.**

4       *This Act may be cited as the “State and Local Gov-*

5       *ernment Cybersecurity Act of 2021”.*

## 1 SEC. 2. AMENDMENTS TO THE HOMELAND SECURITY ACT

2 OF 2002.

3 Subtitle A of title XXII of the Homeland Security

4 Act of 2002 (6 U.S.C. 651 et seq.) is amended—

5 (1) in section 2201 (6 U.S.C. 651)—

6 (A) by redesignating paragraphs (4), (5),  
7 and (6) as paragraphs (5), (6), and (7), respec-  
8 tively; and9 (B) by inserting after paragraph (3) the  
10 following:11 “(4) ENTITY.—The term ‘entity’ shall in-  
12 clude—13 (A) an association, corporation, whether  
14 for-profit or nonprofit, partnership, proprietor-  
15 ship, organization, institution, establishment, or  
16 individual, whether domestic or foreign;17 (B) a governmental agency or other gov-  
18 ernmental entity, whether domestic or foreign,  
19 including State, local, Tribal, and territorial  
20 government entities; and

21 “(C) the general public.”;

22 (2) in section 2202 (6 U.S.C. 652)—

23 (A) in subsection (e)—

24 (i) in paragraph (11), by striking  
25 “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 redesigned, 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 (e)(1)(S); and”; and

14                         “(S) To make grants to and enter into co-  
15                         operative agreements or contracts with States,  
16                         local, Tribal, and territorial governments, and  
17                         other non-Federal entities as the Secretary de-  
18                         termines necessary to carry out the responsibil-  
19                         ties of the Secretary related to cybersecurity  
20                         and infrastructure security under this Act and  
21                         any other provision of law, including grants, co-  
22                         operative agreements, and contracts that pro-  
23                         vide assistance and education related to cyber-  
24                         threat indicators, defensive measures and cyber-

1 security technologies, cybersecurity risks, incidents, analysis, and warnings.”; and  
2

3 (3) in section 2209 (6 U.S.C. 659)—

4 (A) in subsection (e)(6), by inserting  
5 “operational and” before “timely”;

6 (B) in subsection (d)(1)(E), by inserting “,  
7 including an entity that collaborates with elec-  
8 tion officials,” after “governments”; and

9 (C) by adding at the end the following:

10 “(p) COORDINATION ON CYBERSECURITY FOR FED-  
11 ERAL AND NON-FEDERAL ENTITIES.—

12 “(1) COORDINATION.—The Center shall, to the  
13 extent practicable, and in coordination as appro-  
14 priate with Federal and non-Federal entities, such  
15 as the Multi-State Information Sharing and Analysis  
16 Center—

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

19 (B) provide operational and technical cy-  
20 bersecurity training related to cyber threat indi-  
21 cators, proactive and defensive measures, cyber-  
22 security risks and vulnerabilities, and incident  
23 response and management to Federal and non-  
24 Federal entities to address cybersecurity risks  
25 or incidents, with or without reimbursement;

1               “(C) assist Federal and non-Federal enti-  
2 ties, upon request, in sharing actionable and  
3 real time cyber threat indicators, defensive  
4 measures, cybersecurity risks, and incidents  
5 from and to the Federal Government as well as  
6 among Federal and non-Federal entities, in  
7 order to increase situational awareness and help  
8 prevent incidents;

9               “(D) provide notifications containing spe-  
10 cific incident and malware information that  
11 may affect them or their customers and resi-  
12 dents;

13               “(E) provide and periodically update via  
14 an easily accessible platform and other means  
15 tools, products, resources, policies, guidelines,  
16 controls, and other cybersecurity standards and  
17 best practices and procedures related to infor-  
18 mation security;

19               “(F) work with senior Federal and non-  
20 Federal officials, including State, local, Tribal,  
21 and territorial Chief Information Officers, sen-  
22 ior election officials, and through national asso-  
23 ciations, to coordinate a nationwide effort to en-  
24 sure effective implementation of tools, products,  
25 resources, policies, guidelines, controls, and pro-

1        cedures related to information security to se-  
2        cure and ensure the resiliency of Federal and  
3        non-Federal information systems, including  
4        election systems;

5           “(G) provide, upon request, operational  
6        and technical assistance to Federal and non-  
7        Federal entities to implement tools, products,  
8        resources, policies, guidelines, controls, and pro-  
9        cedures on information security, including by,  
10      as appropriate, deploying and sustaining cyber-  
11     security technologies, such as an intrusion and  
12     threat detection capability, to assist those Fed-  
13     eral and non-Federal entities in detecting cyber-  
14     security risks and incidents;

15           “(H) assist Federal and non-Federal enti-  
16       ties in developing policies and procedures for  
17       coordinating vulnerability disclosures, to the ex-  
18       tent practicable, consistent with international  
19       and national standards in the information tech-  
20       nology industry;

21           “(I) ensure that Federal and non-Federal  
22       entities, as appropriate, are made aware of the  
23       tools, products, resources, policies, guidelines,  
24       controls, and procedures on information secu-  
25       rity developed by the Department and other ap-

1 appropriate Federal departments and agencies for  
2 ensuring the security and resiliency of civilian  
3 information systems; and

4 “(J) promote cybersecurity education and  
5 awareness through engagements with Federal  
6 and non-Federal entities.

7 “(q) REPORT.—Not later than 1 year after the date  
8 of enactment of this subsection, and every 2 years there-  
9 after, the Secretary shall submit to the Committee on  
10 Homeland Security and Governmental Affairs of the Sen-  
11 ate and the Committee on Homeland Security of the  
12 House of Representatives a report on—

13 “(1) the status of cybersecurity measures that  
14 are in place, and any gaps that exist, in each State  
15 and in the largest urban areas of the United States;

16 “(2) the services and capabilities that the Agen-  
17 cy directly provides to governmental agencies or  
18 other governmental entities; and

19 “(3) the services and capabilities that the Agen-  
20 cy indirectly provides to governmental agencies or  
21 other governmental entities through an entity de-  
22 scribed in section 2201(4)(B).”.

23 **SECTION 1. SHORT TITLE.**

24 *This Act may be cited as the “State and Local Govern-  
25 ment Cybersecurity Act of 2021”.*

1   **SEC. 2. AMENDMENTS TO THE HOMELAND SECURITY ACT**

2                   **OF 2002.**

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

5                 *(1) in section 2201 (6 U.S.C. 651), by adding at  
6         the end the following:*

7                 *“(7) SLTT ENTITY.—The term ‘SLTT entity’  
8         means a domestic government entity that is a State  
9         government, local government, Tribal government, ter-  
10         itorial government, or any subdivision thereof.”; and*

11                 *(2) in section 2209 (6 U.S.C. 659)—*

12                 *(A) in subsection (c)(6), by inserting “oper-  
13         ational and” before “timely”;*

14                 *(B) in subsection (d)(1)(E), by inserting “,  
15         including an entity that collaborates with elec-  
16         tion officials,” after “governments”; and*

17                 *(C) by adding at the end the following:*

18         *“(p) COORDINATION ON CYBERSECURITY FOR SLTT  
19         ENTITIES.—*

20                 *“(1) COORDINATION.—The Center shall, upon re-  
21         quest and to the extent practicable, and in coordina-  
22         tion as appropriate with Federal and non-Federal en-  
23         tities, such as the Multi-State Information Sharing  
24         and Analysis Center—*

25                 *“(A) conduct exercises with SLTT entities;*

1               “(B) provide operational and technical cy-  
2 bersecurity training to SLTT entities to address  
3 cybersecurity risks or incidents, with or without  
4 reimbursement, related to—

5               “(i) cyber threat indicators;  
6               “(ii) defensive measures;  
7               “(iii) cybersecurity risks;  
8               “(iv) vulnerabilities; and  
9               “(v) incident response and manage-  
10               ment;

11               “(C) in order to increase situational aware-  
12 ness and help prevent incidents, assist SLTT en-  
13 tities in sharing, in real time, with the Federal  
14 Government as well as among SLTT entities, ac-  
15 tionable—

16               “(i) cyber threat indicators;  
17               “(ii) defensive measures;  
18               “(iii) information about cybersecurity  
19               risks; and  
20               “(iv) information about incidents;

21               “(D) provide SLTT entities notifications  
22 containing specific incident and malware infor-  
23 mation that may affect them or their residents;

1               “(E) provide to, and periodically update,  
2               SLTT entities via an easily accessible platform  
3               and other means—

4               “(i) information about tools;  
5               “(ii) information about products;  
6               “(iii) resources;  
7               “(iv) policies;  
8               “(v) guidelines;  
9               “(vi) controls; and  
10              “(vii) other cybersecurity standards  
11              and best practices and procedures related to  
12              information security;

13              “(F) work with senior SLTT entity offi-  
14              cials, including chief information officers and  
15              senior election officials and through national as-  
16              sociations, to coordinate the effective implemen-  
17              tation by SLTT entities of tools, products, re-  
18              sources, policies, guidelines, controls, and proce-  
19              dures related to information security to secure  
20              the information systems, including election sys-  
21              tems, of SLTT entities;

22              “(G) provide operational and technical as-  
23              sistance to SLTT entities to implement tools,  
24              products, resources, policies, guidelines, controls,  
25              and procedures on information security;

1               “(H) assist SLTT entities in developing  
2               policies and procedures for coordinating vulner-  
3               ability disclosures consistent with international  
4               and national standards in the information tech-  
5               nology industry; and

6               “(I) promote cybersecurity education and  
7               awareness through engagements with Federal  
8               agencies and non-Federal entities.

9               “(q) REPORT.—Not later than 1 year after the date  
10      of enactment of this subsection, and every 2 years thereafter,  
11      the Secretary shall submit to the Committee on Homeland  
12      Security and Governmental Affairs of the Senate and the  
13      Committee on Homeland Security of the House of Rep-  
14      resentatives a report on the services and capabilities that  
15      the Agency directly and indirectly provides to SLTT enti-  
16      ties.”.

**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