

117TH CONGRESS
1ST SESSION

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.

IN THE SENATE OF THE UNITED STATES

JULY 28, 2021

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

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”.

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

7 **OF 2002.**

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

10 (1) in section 2201 (6 U.S.C. 651)—

1 (A) by redesignating paragraphs (4), (5),
2 and (6) as paragraphs (5), (6), and (7), respec-
3 tively; and

4 (B) by inserting after paragraph (3) the
5 following:

6 “(4) ENTITY.—The term ‘entity’ shall in-
7 clude—

8 “(A) an association, corporation, whether
9 for-profit or nonprofit, partnership, proprietor-
10 ship, organization, institution, establishment, or
11 individual, whether domestic or foreign;

12 “(B) a governmental agency or other gov-
13 ernmental entity, whether domestic or foreign,
14 including State, local, Tribal, and territorial
15 government entities; and

16 “(C) the general public.”;

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

18 (A) in subsection (c)—

19 (i) in paragraph (11), by striking
20 “and” at the end;

21 (ii) in the first paragraph (12), by
22 striking “and” at the end;

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

1 (iv) in paragraph (13), as so redesignated,
2 nated, by striking “and” at the end; and

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

5 “(14) carry out the authority of the Secretary
6 under subsection (e)(1)(S); and”; and

7 (B) in subsection (e)(1), by adding at the
8 end the following:

9 “(S) To make grants to and enter into co-
10 operative agreements or contracts with States,
11 local, Tribal, and territorial governments, and
12 other non-Federal entities as the Secretary de-
13 termines necessary to carry out the responsibil-
14 ities of the Secretary related to cybersecurity
15 and infrastructure security under this Act and
16 any other provision of law, including grants, co-
17 operative agreements, and contracts that pro-
18 vide assistance and education related to cyber
19 threat indicators, defensive measures and cyber-
20 security technologies, cybersecurity risks, inci-
21 dents, analysis, and warnings.”; and

22 (3) in section 2209 (6 U.S.C. 659)—

23 (A) in subsection (c)(6), by inserting
24 “operational and” before “timely”;

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

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

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

7 “(1) COORDINATION.—The Center shall, to the
8 extent practicable, and in coordination as appro-
9 priate with Federal and non-Federal entities, such
10 as the Multi-State Information Sharing and Analysis
11 Center—

12 “(A) conduct exercises with Federal and
13 non-Federal entities;

14 “(B) provide operational and technical cy-
15 bersecurity training related to cyber threat indi-
16 cators, proactive and defensive measures, cyber-
17 security risks and vulnerabilities, and incident
18 response and management to Federal and non-
19 Federal entities to address cybersecurity risks
20 or incidents, with or without reimbursement;

21 “(C) assist Federal and non-Federal enti-
22 ties, upon request, in sharing actionable and
23 real time cyber threat indicators, defensive
24 measures, cybersecurity risks, and incidents
25 from and to the Federal Government as well as

1 among Federal and non-Federal entities, in
2 order to increase situational awareness and help
3 prevent incidents;

4 “(D) provide notifications containing spe-
5 cific incident and malware information that
6 may affect them or their customers and resi-
7 dents;

8 “(E) provide and periodically update via
9 an easily accessible platform and other means
10 tools, products, resources, policies, guidelines,
11 controls, and other cybersecurity standards and
12 best practices and procedures related to infor-
13 mation security;

14 “(F) work with senior Federal and non-
15 Federal officials, including State, local, Tribal,
16 and territorial Chief Information Officers, sen-
17 ior election officials, and through national asso-
18 ciations, to coordinate a nationwide effort to en-
19 sure effective implementation of tools, products,
20 resources, policies, guidelines, controls, and pro-
21 cedures related to information security to se-
22 cure and ensure the resiliency of Federal and
23 non-Federal information systems, including
24 election systems;

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

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

17 “(I) ensure that Federal and non-Federal
18 entities, as appropriate, are made aware of the
19 tools, products, resources, policies, guidelines,
20 controls, and procedures on information secu-
21 rity developed by the Department and other ap-
22 propriate Federal departments and agencies for
23 ensuring the security and resiliency of civilian
24 information systems; and

1 “(J) promote cybersecurity education and
2 awareness through engagements with Federal
3 and non-Federal entities.

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

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

13 “(2) the services and capabilities that the Agen-
14 cy directly provides to governmental agencies or
15 other governmental entities; and

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

○