

116TH CONGRESS
1ST SESSION

S. _____

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

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

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 2019”.

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—

1 (1) in section 2201 (6 U.S.C. 651)—

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

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

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

9 “(A) an association, corporation, whether
10 for-profit or nonprofit, partnership, proprietor-
11 ship, organization, institution, establishment, or
12 individual, whether domestically or foreign
13 owned, that has the legal capacity to enter into
14 agreements or contracts, assume obligations,
15 incur and pay debts, sue and be sued in its own
16 right in a court of competent jurisdiction in the
17 United States, and to be held responsible for its
18 actions;

19 “(B) a governmental agency or other gov-
20 ernmental entity, including State, local, Tribal,
21 and territorial government entities; and

22 “(C) the general public.”; and

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

24 (A) in subsection (c)—

1 (i) in paragraph (10), by striking
2 “and” at the end;

3 (ii) by redesignating paragraph (11)
4 as paragraph (12); and

5 (iii) by inserting after paragraph (10)
6 the following:

7 “(11) carry out the authority of the Secretary
8 under subsection (e)(1)(R); and”;

9 (B) in subsection (e)(1), by adding at the
10 end the following:

11 “(R) To make grants to and enter into co-
12 operative agreements or contracts with States,
13 local governments, and other non-Federal enti-
14 ties as the Secretary determines necessary to
15 carry out the responsibilities of the Secretary
16 related to cybersecurity and infrastructure secu-
17 rity under this Act and any other provision of
18 law, including grants, cooperative agreements,
19 and contracts that provide assistance and edu-
20 cation related to cyber threat indicators, defen-
21 sive measures and cybersecurity technologies,
22 cybersecurity risks, incidents, analysis, and
23 warnings.”;

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

1 (A) in subsection (c)(6), by inserting
2 “operational and” after “timely”;

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

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

7 “(n) COORDINATION ON CYBERSECURITY FOR FED-
8 ERAL AND NON-FEDERAL ENTITIES.—

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

14 “(A) conduct exercises with Federal and
15 non-Federal entities;

16 “(B) provide operational and technical cy-
17 bersecurity training related to cyber threat indi-
18 cators, defensive measures, cybersecurity risks,
19 and incidents to Federal and non-Federal enti-
20 ties to address cybersecurity risks or incidents,
21 with or without reimbursement;

22 “(C) assist Federal and non-Federal enti-
23 ties, upon request, in sharing cyber threat indi-
24 cators, defensive measures, cybersecurity risks,
25 and incidents from and to the Federal Govern-

1 ment as well as among Federal and non-Fed-
2 eral entities, in order to increase situational
3 awareness and help 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 a
9 web portal and other means tools, products, re-
10 sources, policies, guidelines, controls, and other
11 cybersecurity standards and best practices and
12 procedures related to information security;

13 “(F) work with senior Federal and non-
14 Federal officials, including State and local Chief
15 Information Officers, senior election officials,
16 and through national associations, to coordinate
17 a nationwide effort to ensure effective imple-
18 mentation of tools, products, resources, policies,
19 guidelines, controls, and procedures related to
20 information security to secure and ensure the
21 resiliency of Federal and non-Federal informa-
22 tion systems and including election systems;

23 “(G) provide, upon request, operational
24 and technical assistance to Federal and non-
25 Federal entities to implement tools, products,

1 resources, policies, guidelines, controls, and pro-
2 cedures on information security, including by,
3 as appropriate, deploying and sustaining cyber-
4 security technologies, such as an intrusion de-
5 tection capability, to assist those Federal and
6 non-Federal entities in detecting cybersecurity
7 risks and incidents;

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

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

22 “(J) promote cybersecurity education and
23 awareness through engagements with Federal
24 and non-Federal entities.

1 “(o) REPORT.—Not later than 1 year after the date
2 of enactment of this subsection, and every 2 years there-
3 after, the Secretary shall submit to the Committee on
4 Homeland Security and Governmental Affairs of the Sen-
5 ate and the Committee on Homeland Security of the
6 House of Representatives a report on the status of cyber-
7 security measures that are in place, and any gaps that
8 exist, in each State and in the largest urban areas of the
9 United States.

10 “(p) PILOT DEPLOYMENT OF SENSORS.—

11 “(1) ESTABLISHMENT.—Not later than 180
12 days after the date of enactment of this subsection,
13 the Secretary shall establish a pilot program to de-
14 ploy network sensors capable of utilizing classified
15 indicators for the purpose of identifying and filtering
16 malicious network traffic.

17 “(2) VOLUNTARY PARTICIPATION.—Activities
18 related to the pilot program established under this
19 subsection may only be carried out on a voluntary
20 basis in coordination with the owner of the impacted
21 network.

22 “(3) EXPANSION AUTHORITY.—If, after 12
23 months of deployment, the Secretary determines
24 that the network sensors deployed pursuant to this
25 subsection would provide network security benefits

1 to other critical infrastructure sectors, the Secretary
2 may make additional network sensors available to
3 those sectors on a voluntary basis at the request of
4 critical infrastructure owners and operators.

5 “(4) REPORT.—Not later than 1 year after the
6 date on which the Secretary establishes the pilot
7 program under this subsection, the Secretary shall
8 submit to the Committee on Homeland Security and
9 Governmental Affairs of the Senate and the Com-
10 mittee on Homeland Security of the House of a Rep-
11 resentatives a report on the pilot program, which
12 shall include—

13 “(A) the status of the pilot program;

14 “(B) the rate of voluntary participation in
15 the pilot program;

16 “(C) the effectiveness of the pilot program
17 in detecting and blocking traffic that could not
18 have been captured without the network sensors
19 deployed under the pilot program; and

20 “(D) recommendations for expanding the
21 use of classified threat indicators to protect
22 United States critical infrastructure.”.