

Calendar No. 194

116TH CONGRESS
1ST SESSION**S. 1846****[Report No. 116–90]**

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

JUNE 13, 2019

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

SEPTEMBER 10, 2019

Reported by Mr. JOHNSON, with an amendment

[Omit the part struck through 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 2019”.

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; and

9 (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 domestically or foreign
17 owned, that has the legal capacity to enter into
18 agreements or contracts, assume obligations,
19 incur and pay debts, sue and be sued in its own
20 right in a court of competent jurisdiction in the
21 United States, and to be held responsible for its
22 actions;

23 “(B) a governmental agency or other gov-
24 ernmental entity, including State, local, Tribal,
25 and territorial government entities; and

26 “(C) the general public.”; and

1 (2) in section 2202 (6 U.S.C. 652)—

2 (A) in subsection (c)—

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

5 (ii) by redesignating paragraph (11)
6 as paragraph (12); and

7 (iii) by inserting after paragraph (10)
8 the following:

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

11 (B) in subsection (e)(1), by adding at the
12 end the following:

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

1 (3) in section 2209 (6 U.S.C. 659)—

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

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

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

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

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

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

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

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

1 and incidents from and to the Federal Govern-
2 ment as well as among Federal and non-Fed-
3 eral entities, in order to increase situational
4 awareness and help prevent incidents;

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

9 “(E) provide and periodically update via a
10 web portal and other means tools, products, re-
11 sources, policies, guidelines, controls, and other
12 cybersecurity standards and best practices and
13 procedures related to information security;

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

24 “(G) provide, upon request, operational
25 and technical assistance to Federal and non-

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

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

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

23 “(J) promote cybersecurity education and
24 awareness through engagements with Federal
25 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 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.”

23 “(p) DEPLOYMENT OF ENHANCED CAPABILITIES.—

24 “(1) ESTABLISHMENT.—Not later than 180 days
 25 after the date of enactment of this subsection, the Sec-

1 *retary may establish an initiative to enhance efforts*
2 *to deploy technical or analytic capabilities or services*
3 *that utilize classified cyber threat indicators or intel-*
4 *ligence for the purpose of detecting or preventing ma-*
5 *licious network traffic on unclassified non-Federal in-*
6 *formation systems.*

7 “(2) *VOLUNTARY PARTICIPATION.—Activities*
8 *conducted under this subsection may only be carried*
9 *out on a voluntary basis upon request of the non-Fed-*
10 *eral entity.*

11 “(3) *REPORT.—Not later than 1 year after the*
12 *date on which the Secretary establishes the initiative*
13 *under this subsection, the Secretary shall submit to*
14 *the Committee on Homeland Security and Govern-*
15 *mental Affairs of the Senate and the Committee on*
16 *Homeland Security of the House of Representatives a*
17 *report on the initiative, which shall include—*

18 “(A) *the status of the initiative;*

19 “(B) *the rate of voluntary participation in*
20 *the initiative;*

21 “(C) *the effectiveness of the initiative; and*

22 “(D) *recommendations for expanding the*
23 *use of classified cyber threat indicators to protect*
24 *non-Federal entities.’’.*

Calendar No. 194

116TH CONGRESS
1ST Session

S. 1846

[Report No. 116-90]

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.

SEPTEMBER 10, 2019

Reported with an amendment