

114TH CONGRESS
2D SESSION

S. 2665

To amend the Homeland Security Act of 2002 to require State and local coordination on cybersecurity with the national cybersecurity and communications integration center, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 10, 2016

Mr. PETERS (for himself and Mr. PERDUE) 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 require State and local coordination on cybersecurity with the national cybersecurity and communications integration center, 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 Cyber
5 Protection Act of 2016”.

1 **SEC. 2. STATE AND LOCAL COORDINATION ON CYBERSECU-**
2 **RITY WITH THE NATIONAL CYBERSECURITY**
3 **AND COMMUNICATIONS INTEGRATION CEN-**
4 **TER.**

5 (a) IN GENERAL.—Section 227 of the Homeland Se-
6 curity Act of 2002 (6 U.S.C. 148) is amended by adding
7 at the end the following:

8 “(m) STATE AND LOCAL COORDINATION ON CYBER-
9 SECURITY.—

10 “(1) IN GENERAL.—The Center shall, to the ex-
11 tent practicable—

12 “(A) assist State and local governments,
13 upon request, in identifying information system
14 vulnerabilities;

15 “(B) assist State and local governments,
16 upon request, in identifying information secu-
17 rity protections commensurate with cybersecu-
18 rity risks and the magnitude of the potential
19 harm resulting from the unauthorized access,
20 use, disclosure, disruption, modification, or de-
21 struction of—

22 “(i) information collected or main-
23 tained by or on behalf of a State or local
24 government; or

25 “(ii) information systems used or op-
26 erated by an agency or by a contractor of

1 a State or local government or other orga-
2 nization on behalf of a State or local gov-
3 ernment;

4 “(C) in consultation with State and local
5 governments, provide and periodically update
6 via a web portal tools, products, resources, poli-
7 cies, guidelines, and procedures related to infor-
8 mation security;

9 “(D) work with senior State and local gov-
10 ernment officials, including State and local
11 Chief Information Officers, through national as-
12 sociations to coordinate a nationwide effort to
13 ensure effective implementation of tools, prod-
14 ucts, resources, policies, guidelines, and proce-
15 dures related to information security to secure
16 and ensure the resiliency of State and local in-
17 formation systems;

18 “(E) provide, upon request, operational
19 and technical cybersecurity training to State
20 and local government and fusion center analysts
21 and operators to address cybersecurity risks or
22 incidents;

23 “(F) provide, in coordination with the
24 Chief Privacy Officer and the Chief Civil Rights
25 and Civil Liberties Officer of the Department,

1 privacy and civil liberties training to State and
2 local governments related to cybersecurity;

3 “(G) provide, upon request, operational
4 and technical assistance to State and local gov-
5 ernments to implement tools, products, re-
6 sources, policies, guidelines, and procedures on
7 information security by—

8 “(i) deploying technology to assist
9 such State or local government to continu-
10 ously diagnose and mitigate against cyber
11 threats and vulnerabilities, with or without
12 reimbursement;

13 “(ii) compiling and analyzing data on
14 State and local information security; and

15 “(iii) developing and conducting tar-
16 geted operational evaluations, including
17 threat and vulnerability assessments, on
18 the information systems of State and local
19 governments;

20 “(H) assist State and local governments to
21 develop policies and procedures for coordinating
22 vulnerability disclosures, to the extent prac-
23 ticable, consistent with international and na-
24 tional standards in the information technology
25 industry, including standards developed by the

1 National Institute of Standards and Tech-
2 nology; and

3 “(I) ensure that State and local govern-
4 ments, as appropriate, are made aware of the
5 tools, products, resources, policies, guidelines,
6 and procedures on information security devel-
7 oped by the Department and other appropriate
8 Federal departments and agencies for ensuring
9 the security and resiliency of Federal civilian
10 information systems.

11 “(2) TRAINING.—Privacy and civil liberties
12 training provided pursuant to subparagraph (F) of
13 paragraph (1) shall include processes, methods, and
14 information that—

15 “(A) are consistent with the Department’s
16 Fair Information Practice Principles developed
17 pursuant to section 552a of title 5, United
18 States Code (commonly referred to as the ‘Pri-
19 vacy Act of 1974’ or the ‘Privacy Act’);

20 “(B) reasonably limit, to the greatest ex-
21 tent practicable, the receipt, retention, use, and
22 disclosure of information related to cybersecu-
23 rity risks and incidents associated with specific
24 persons that is not necessary, for cybersecurity
25 purposes, to protect an information system or

1 network of information systems from cybersecu-
2 rity risks or to mitigate cybersecurity risks and
3 incidents in a timely manner;

4 “(C) minimize any impact on privacy and
5 civil liberties;

6 “(D) provide data integrity through the
7 prompt removal and destruction of obsolete or
8 erroneous names and personal information that
9 is unrelated to the cybersecurity risk or incident
10 information shared and retained by the Center
11 in accordance with this section;

12 “(E) include requirements to safeguard
13 cyber threat indicators and defensive measures
14 retained by the Center, including information
15 that is proprietary or business-sensitive that
16 may be used to identify specific persons from
17 unauthorized access or acquisition;

18 “(F) protect the confidentiality of cyber
19 threat indicators and defensive measures associ-
20 ated with specific persons to the greatest extent
21 practicable; and

22 “(G) ensure all relevant constitutional,
23 legal, and privacy protections are observed, in-
24 cluding that information obtained from efforts
25 to address cybersecurity risks and incidents is

1 used only for such purposes, or as specifically
2 authorized by law.”.

3 (b) CONGRESSIONAL OVERSIGHT.—Not later than 2
4 years after the date of enactment of this Act, the national
5 cybersecurity and communications integration center of
6 the Department of Homeland Security shall provide to the
7 Committee on Homeland Security of the House of Rep-
8 resentatives and the Committee on Homeland Security
9 and Governmental Affairs of the Senate information on
10 the activities and effectiveness of such activities under
11 subsection (m) of section 227 of the Homeland Security
12 Act of 2002 (6 U.S.C. 148), as added by subsection (a)
13 of this section, on State and local information security.
14 The center shall seek feedback from State and local gov-
15 ernments regarding the effectiveness of such activities and
16 include such feedback in the information required to be
17 provided under this subsection.

○