

114TH CONGRESS
1ST SESSION

H. R. 3869

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 HOUSE OF REPRESENTATIVES

NOVEMBER 2, 2015

Mr. HURD of Texas (for himself and Mr. RATCLIFFE) introduced the following bill; which was referred to the Committee on Homeland Security

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 2015”.

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.—The second section 226 of the
6 Homeland Security Act of 2002 (6 U.S.C. 148; relating
7 to the national cybersecurity and communications integra-
8 tion center) is amended by adding at the end the following
9 new subsection:

10 “(g) STATE AND LOCAL COORDINATION ON CYBER-
11 SECURITY.—

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

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

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

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

1 “(ii) information systems used or op-
2 erated by an agency or by a contractor of
3 a State or local government or other orga-
4 nization on behalf of a State or local gov-
5 ernment;

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

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

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

1 “(F) provide, in coordination with the
2 Chief Privacy Officer and the Chief Civil Rights
3 and Civil Liberties Officer of the Department,
4 privacy and civil liberties training to State and
5 local governments related to cybersecurity;

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

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

16 “(ii) compiling and analyzing data on
17 State and local information security; and

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

23 “(H) assist State and local governments to
24 develop policies and procedures for coordinating
25 vulnerability disclosures, to the extent prac-

1 ticable, consistent with international and na-
2 tional standards in the information technology
3 industry, including standards developed by the
4 National Institute of Standards and Tech-
5 nology; and

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

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

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

23 “(B) reasonably limit, to the greatest ex-
24 tent practicable, the receipt, retention, use, and
25 disclosure of information related to cybersecu-

1 rity risks and incidents associated with specific
2 persons that is not necessary, for cybersecurity
3 purposes, to protect an information system or
4 network of information systems from cybersecu-
5 rity risks or to mitigate cybersecurity risks and
6 incidents in a timely manner;

7 “(C) minimize any impact on privacy and
8 civil liberties;

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

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

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

1 “(G) ensure all relevant constitutional,
2 legal, and privacy protections are observed.”.

3 (b) CONGRESSIONAL OVERSIGHT.—Not later than
4 two years after the date of the enactment of this Act, the
5 national cybersecurity and communications integration
6 center of the Department of Homeland Security shall pro-
7 vide to the Committee on Homeland Security of the House
8 of Representatives and the Committee on Homeland Secu-
9 rity and Governmental Affairs of the Senate information
10 on the activities and effectiveness of such activities under
11 subsection (g) of the second section 226 of the Homeland
12 Security Act of 2002 (6 U.S.C. 148; relating to the na-
13 tional cybersecurity and communications integration cen-
14 ter), as added by subsection (a) of this section, on State
15 and local information security. The center shall seek feed-
16 back from State and local governments regarding the ef-
17 fectiveness of such activities and include such feedback in
18 the information required to be provided under this sub-
19 section.

○