

Union Calendar No.

114TH CONGRESS
1ST SESSION

H. R. 3869

[Report No. 114-]

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

NOVEMBER --, 2015

Committed to the Committee of the Whole House on the State of the Union,
and ordered to be printed

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”.

6 **SEC. 2. STATE AND LOCAL COORDINATION ON CYBERSECU-**
7 **RITY WITH THE NATIONAL CYBERSECURITY**
8 **AND COMMUNICATIONS INTEGRATION CEN-**
9 **TER.**

10 (a) IN GENERAL.—The second section 226 of the
11 Homeland Security Act of 2002 (6 U.S.C. 148; relating
12 to the national cybersecurity and communications integra-
13 tion center) is amended by adding at the end the following
14 new subsection:

15 “(g) STATE AND LOCAL COORDINATION ON CYBER-
16 SECURITY.—

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

19 “(A) assist State and local governments,
20 upon request, in identifying information system
21 vulnerabilities;

22 “(B) assist State and local governments,
23 upon request, in identifying information secu-
24 rity protections commensurate with cybersecu-
25 rity risks and the magnitude of the potential

1 harm resulting from the unauthorized access,
2 use, disclosure, disruption, modification, or de-
3 struction of—

4 “(i) information collected or main-
5 tained by or on behalf of a State or local
6 government; or

7 “(ii) information systems used or op-
8 erated by an agency or by a contractor of
9 a State or local government or other orga-
10 nization on behalf of a State or local gov-
11 ernment;

12 “(C) in consultation with State and local
13 governments, provide and periodically update
14 via a web portal tools, products, resources, poli-
15 cies, guidelines, and procedures related to infor-
16 mation security;

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

1 “(E) provide, upon request, operational
2 and technical cybersecurity training to State
3 and local government and fusion center analysts
4 and operators to address cybersecurity risks or
5 incidents;

6 “(F) provide, in coordination with the
7 Chief Privacy Officer and the Chief Civil Rights
8 and Civil Liberties Officer of the Department,
9 privacy and civil liberties training to State and
10 local governments related to cybersecurity;

11 “(G) provide, upon request, operational
12 and technical assistance to State and local gov-
13 ernments to implement tools, products, re-
14 sources, policies, guidelines, and procedures on
15 information security by—

16 “(i) deploying technology to assist
17 such State or local government to continu-
18 ously diagnose and mitigate against cyber
19 threats and vulnerabilities, with or without
20 reimbursement;

21 “(ii) compiling and analyzing data on
22 State and local information security; and

23 “(iii) developing and conducting tar-
24 geted operational evaluations, including
25 threat and vulnerability assessments, on

1 the information systems of State and local
2 governments;

3 “(H) assist State and local governments to
4 develop policies and procedures for coordinating
5 vulnerability disclosures, to the extent prac-
6 ticable, consistent with international and na-
7 tional standards in the information technology
8 industry, including standards developed by the
9 National Institute of Standards and Tech-
10 nology; and

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

19 “(2) TRAINING.—Privacy and civil liberties
20 training provided pursuant to subparagraph (F) of
21 paragraph (1) shall include processes, methods, and
22 information that—

23 “(A) are consistent with the Department’s
24 Fair Information Practice Principles developed
25 pursuant to section 552a of title 5, United

1 States Code (commonly referred to as the ‘Pri-
2 vacy Act of 1974’ or the ‘Privacy Act’);

3 “(B) reasonably limit, to the greatest ex-
4 tent practicable, the receipt, retention, use, and
5 disclosure of information related to cybersecu-
6 rity risks and incidents associated with specific
7 persons that is not necessary, for cybersecurity
8 purposes, to protect an information system or
9 network of information systems from cybersecu-
10 rity risks or to mitigate cybersecurity risks and
11 incidents in a timely manner;

12 “(C) minimize any impact on privacy and
13 civil liberties;

14 “(D) provide data integrity through the
15 prompt removal and destruction of obsolete or
16 erroneous names and personal information that
17 is unrelated to the cybersecurity risk or incident
18 information shared and retained by the Center
19 in accordance with this section;

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

1 “(F) protect the confidentiality of cyber
2 threat indicators and defensive measures associ-
3 ated with specific persons to the greatest extent
4 practicable; and

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

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