

114TH CONGRESS
1ST SESSION

H. R. 3869

IN THE SENATE OF THE UNITED STATES

DECEMBER 14, 2015

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

To amend the Homeland Security Act of 2002 to assist
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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “State and Local Cyber
3 Protection Act of 2015”.

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

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

13 “(g) STATE AND LOCAL COORDINATION ON CYBER-
14 SECURITY.—

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

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

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

1 “(i) information collected or main-
2 tained by or on behalf of a State or local
3 government; or

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

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

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

23 “(E) provide, upon request, operational
24 and technical cybersecurity training to State
25 and local government and fusion center analysts

1 and operators to address cybersecurity risks or
2 incidents;

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

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

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

18 “(ii) compiling and analyzing data on
19 State and local information security; and

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

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

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

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

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

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

10 “(C) minimize any impact on privacy and
11 civil liberties;

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

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

24 “(F) protect the confidentiality of cyber
25 threat indicators and defensive measures associ-

1 ated with specific persons to the greatest extent
2 practicable; and

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

5 (b) CONGRESSIONAL OVERSIGHT.—Not later than 2
6 years after the date of the enactment of this Act, the na-
7 tional cybersecurity and communications integration cen-
8 ter of the Department of Homeland Security shall provide
9 to the Committee on Homeland Security of the House of
10 Representatives and the Committee on Homeland Security
11 and Governmental Affairs of the Senate information on
12 the activities and effectiveness of such activities under
13 subsection (g) of the second section 226 of the Homeland
14 Security Act of 2002 (6 U.S.C. 148; relating to the na-
15 tional cybersecurity and communications integration cen-
16 ter), as added by subsection (a) of this section, on State
17 and local information security. The center shall seek feed-
18 back from State and local governments regarding the ef-
19 fectiveness of such activities and include such feedback in

1 the information required to be provided under this sub-
2 section.

Passed the House of Representatives December 10,
2015.

Attest:

KAREN L. HAAS,

Clerk.