115TH CONGRESS
1ST SESSION

S. 412

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

FEBRUARY 16, 2017

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "State and Local Cyber Protection Act of 2017".

SEC. 2. STATE AND LOCAL COORDINATION ON CYBERSECURITY WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

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

''(n) STATE AND LOCAL COORDINATION ON CYBERSECURITY.—

''(1) IN GENERAL.—The Center shall, to the extent practicable—

''(A) assist State and local governments, upon request, in identifying information system vulnerabilities;

''(B) assist State and local governments, upon request, in identifying information security protections commensurate with cybersecurity risks and the magnitude of the potential harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of a State or local government; or

''(ii) information systems used or operated by an agency or by a contractor of

a State or local government or other organization on behalf of a State or local government;

''(C) in consultation with State and local governments, provide and periodically update via a web portal tools, products, resources, policies, guidelines, and procedures related to information security;

''(D) work with senior State and local government officials, including State and local Chief Information Officers, through national associations to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, and procedures related to information security to secure and ensure the resiliency of State and local information systems;

''(E) provide, upon request, operational and technical cybersecurity training to State and local government and fusion center analysts and operators to address cybersecurity risks or incidents;

''(F) provide, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department,

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

''(G) provide, upon request, operational and technical assistance to State and local governments to implement tools, products, resources, policies, guidelines, and procedures on information security by—

''(i) deploying technology to assist such State or local government to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

''(ii) compiling and analyzing data on State and local information security; and

''(iii) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems of State and local governments;

''(H) assist State and local governments to develop policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry, including standards developed by the

National Institute of Standards and Technology; and

''(I) ensure that State and local governments, as appropriate, are made aware of the tools, products, resources, policies, guidelines, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of Federal civilian information systems.

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

''(A) are consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act of 1974' or the 'Privacy Act');

''(B) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of information related to cybersecurity risks and incidents associated with specific persons that is not necessary, for cybersecurity purposes, to protect an information system or

network of information systems from cybersecurity risks or to mitigate cybersecurity risks and incidents in a timely manner;

"(C) minimize any impact on privacy and civil liberties;

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

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

"(F) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

"(G) ensure all relevant constitutional, legal, and privacy protections are observed, including that information obtained from efforts to address cybersecurity risks and incidents is

used only for such purposes, or as specifically authorized by law.''.

(b) CONGRESSIONAL OVERSIGHT.—Not later than 2 years after the date of enactment of this Act, the national cybersecurity and communications integration center of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the activities and effectiveness of such activities under subsection (n) of section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148), as added by subsection (a) of this section, on State and local information security. The center shall seek feedback from State and local governments regarding the effectiveness of such activities and include such feedback in the information required to be provided under this subsection.

○