S 412

State and Local Cyber Protection Act of 2017

Congress: 115 (2017–2019, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Feb 16, 2017
Current Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Latest Action: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Feb 16, 2017)
Official Text: https://www.congress.gov/bill/115th-congress/senate-bill/412

Sponsor

Name: Sen. Peters, Gary C. [D-MI]
Party: Democratic • **State:** MI • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Perdue, David [R-GA]	R · GA		Feb 16, 2017

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Feb 16, 2017

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Feb 16, 2017)

State and Local Cyber Protection Act of 2017

This bill amends the Homeland Security Act of 2002 to require the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to assist state and local governments with cybersecurity by:

- upon request, identifying system vulnerabilities and information security protections to address unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by, or information systems used or operated by, state or local governments or other organizations or contractors on their behalf;
- providing via a web portal updated resources and guidelines related to information security;
- coordinating through national associations to implement information security tools and policies to ensure the resiliency of state and local information systems;
- providing training on cybersecurity, privacy, and civil liberties;
- providing requested technical assistance to deploy technology that continuously diagnoses and mitigates cyber threats and to conduct threat and vulnerability assessments;
- coordinating vulnerability disclosures under standards developed by the National Institute of Standards and Technology; and
- ensuring that state and local governments are aware of DHS resources and other federal tools to ensure the security and resiliency of federal civilian information systems.

The NCCIC's privacy and civil liberties training must include: (1) reasonable limits on the receipt, retention, use, and disclosure of information associated with specific persons that is not necessary for cybersecurity purposes; (2) data integrity standards requiring the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the risk or incident information; (3) safeguards and confidentiality protections for cyber threat indicators and defensive measures, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition; and (4) methods to ensure that obtained information is used only to address cybersecurity risks and threats or as specifically authorized by law.

The NCCIC must seek feedback from state and local governments on the effectiveness of such activities and provide such information to Congress.

Actions Timeline

- **Feb 16, 2017:** Introduced in Senate
- **Feb 16, 2017:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.