NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

S. 516
State Cyber Resiliency Act

Representatives Derek Kilmer (D-Wash.-06) & Barbara Comstock (R-Va.-10)
Senators Mark Warner (D-Va.) & Cory Gardner (R-Colo.)

The State Cyber Resiliency Act would establish a new grant program in the Department of Homeland Security (DHS) administered by FEMA, to assist state, local, and tribal governments in preventing, preparing for, protecting against and responding to cyber threats. Additionally, it authorizes DHS to run a state cyber grant program for five years. The State Cyber Resiliency Act, S. 516:

Sec. 1: **Short Title**

Sect. 2(a)-(c): **Establishment of Cyber Resiliency Grant Program**

The purpose is to assist state, local, and tribal governments in preventing, preparing for, protecting against and responding to cyber threats. The Federal Emergency Management Agency will manage the grant. Each state is eligible to apply for up to two planning grants and up to two implementation grants.

Sec. 2(d): **Approval of Cyber Resiliency Plans**

A resiliency plan submitted by a state shall be approved by the DHS secretary if:

- The plan incorporates any existing plans the state had to protect against cybersecurity threats or vulnerabilities, to the extent practicable.
- The plan is designed to achieve the following essential functions and objectives:
    - Enhance the security, response, and resiliency of cyber networks and systems.
    - Implement continuous cyber threat monitoring and mitigation practices.
    - Ensure entities performing cyber functions adopt recognized best practices.
    - Mitigate talent gaps in the cyber workforce.
    - Protect public safety and emergency management systems.
    - Mitigate cyber threats related to critical infrastructure.
    - Promote information sharing practices such as:
        - Ensuring continuity of communications and data networks between entities within the state enterprise responsible for data security.
        - Providing communications capabilities to ensure information sharing.
        - Developing and coordinating strategies in consultation with neighboring states; and neighboring countries.

The grant approval will be for a two-year term, subject to an annual evaluation that the state's plan continues to meet the objectives above and subject to the state making revisions as the secretary deems necessary.

The scope of the grant will include "essential functions" as defined as "state functions that enhance the cybersecurity posture of the state, local and tribal governments of the state, and the public services they provide."

Sec. 2(e): **Planning Grants**

A condition of awarding an initial planning grant will be to develop a cyber resiliency plan that meets the criteria described above, and the applicant state must submit an application including such information to the secretary. A state can receive up to two planning grants but on non-consecutive years.

Sec. 2(f): **Implementation Grants**

A condition of awarding an implementation grant will be for the state to submit an application with:

- A proposal, including a description and timeline, of the activities to be funded by the grant as described by an approved cyber resiliency plan.
- A description of how the activity would achieve one or more of the objectives outlined above.
- A description of how any prior implementation grants awarded under this section was spent and to what extent the objectives were met.
- The share of any amounts awarded to be distributed to local or tribal governments.
    - Distribution can be no later than 45 days after the award date.
    - The state must distribute no less than 50 percent of the grant award to local or tribal governments under most circumstances.
    - The state must consult with local and regional chief information officers (CIOs), emergency managers and senior public safety officials to determine how an implementation grant will be distributed.
- Other information as the secretary of DHS may determine necessary in consultation with CIOs, emergency managers and senior state public safety officials.

Sec. 2(g): **Use of Grant Funds**

Any grant award will supplement and not supplant state or local funds. Grant awards cannot be used to provide a federal cost-sharing contribution on behalf of a state or for any recreational or social purpose. Grant funds may be allowed for:

- Supporting or enhancing information sharing and analysis organizations.
- Implementing or coordinating systems and services that use cyber threat indicators as defined by the Cybersecurity Information Sharing Act of 2015 to address cyber threats or vulnerabilities.
- Supporting dedicated cyber and communications coordination planning including.
    - Emergency management elements.
    - National guard units.
    - Entities associated with critical infrastructure or key resources.
    - Information sharing and analysis organizations.
    - Public safety answering points.

    - Non-governmental organizations (NGOs) engaged in cyber research as a formally designated information analysis and sharing organization.
- Establishing programs such as scholarships or apprenticeships to provide financial assistance to state residents who:
    - Pursue formal education, training and industry-recognized certifications for cybersecurity careers and who commit to working for state government for a specified period of time.

Sec. 2(h): **Funding Allocations**

Excess funds not used to carry out this section shall be used by the secretary to allocate the entire amount among the states and the District of Columbia eligible for grants. Provides limitations and caps on amounts of funds that can be distributed. Distinguishes between the states and U.S. Territories. Funding allocations will consider:

- The degree of exposure the state and the protected government entities within the state is to threats, vulnerabilities or consequences resulting from cybersecurity risks or incidents.
- The level of effectiveness of data network protections and other secure communication capabilities.
- The extent to which the state is vulnerable to cyber threats because it has not implemented best practices.
- The extent to which a state government may face low cybersecurity workforce supply and high workforce demand.

Sec. 2(i): **Review Committee for Cyber Resiliency Grants**

Establishes a Review Committee (review committee) that will receive a copy of each cyber resiliency plan submitted to the secretary of DHS, and gives the review committee the ability to consider each application for (1) an additional planning grant and (2) each application for a biennial implementation grant. The review committee's duties include:

- Promulgate guidance for the development of applications for grants.
- Review any plan or application previously mentioned above. Provide to the state and the Secretary the recommendations regarding the approval or disapproval of the state plan or application and any suggestions on improvements to the application or plan.
- Provide the Secretary an evaluation of any progress made by a state in implementing an active cyber resiliency plan.
- Submit to Congress an annual report on progress made in implementing active cyber resiliency plans.

There will be 15 members appointed by the secretary. No more than nine individuals may be appointed who have educational and professional experience related to cybersecurity analysis or policy. It must include at least:

- Two National Governors Association members.
- One National Guard Bureau member.

- One representative from the National Association of Counties
- One National League of Cities member.

Sec. 2(j): **Funding**

Each member will have a one year term without pay. The bill also outlines certain vacancy filling rules for any member that terminates their association before their one year term is complete. Designates the Secretary or designee of the Secretary as chairperson of the Review Committee. The administrator of FEMA or the designee will serve as vice chairperson. Staff and experts may be appointed, with details outlined in the bill. The Federal Advisory Committee Act shall not apply to the Review Committee. The authority of the Review Committee shall terminate on the day after the end of the five fiscal year period.

For more information or questions, please contact Susan Parnas Frederick (susan.frederick@ncsl.org) or Danielle Dean (Danielle.dean@ncsl.org).