NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

Cybersecurity Task Force Minneapolis MN Executive Committee Meeting

The NCSL Executive Committee Task Force on Cybersecurity held its first meeting in Minneapolis, MN Saturday May 21st, 2016. Rounding out a robust day of conversations from federal government, private sector and state government officials, the task force concluded the meeting with listing its top priorities for their next scheduled meeting. In conjunction with the Legislative Summit in August in Chicago, the Task Force will discuss cybersecurity issues related to workforce development and risk assessment of state systems through data analytics. The Task Force also will work with the NCSL Energy Supply Task Force going forward to address critical infrastructure issues. Below is a brief summary of the presentations and the speakers that guided legislator and legislative staff discussions.
The morning discussions delved into state cybersecurity postures and understanding existing state networks. Governing institute conducted a survey of state legislatures on their perception versus the reality of state network cyber readiness. The survey results indicated that there are gaps between perceptions of cyber readiness and actual preparedness. The first step to bridging that gap, is to ask the right questions to state CISOs and understanding what the current cybersecurity process is.

Instrumental to this process is talking to the state CIO and CISO. Legislatures should understand the governance structure of the CISOs and develop a relationship with leadership early. CISOs/CIOs have different levels of authority, with some having absolute control in a consolidated agency structure while others are decentralized. Conversations about state system weaknesses should not be the first time legislatures are meeting their CISO.

The good news is states should not assume that security state networks will require "throwing money" at the problem, but instead it was suggested that legislatures examine existing resources and channel support to successful programs. States should understand what strategic plans are in place, how to quickly detect breaches by talking to experts, and how to take advantage of existing resources such as the NIST framework and MS-ISAC services. Reaching students is also important. States should emphasize STEM education and offer internship programs to develop cyber professionals, as interns are more likely to fill open positions within the state.

Understanding that cyber is not just a technology issue, it is also a policy and risk management issue resonated with legislators. It is important to build and maintain partnerships between federal and private sector groups. A challenge to this perspective are continuing concerns around individual privacy and civil liberties. Federal-state relations will need to build trust if there is to be coordination around cybersecurity data sharing.

Under intense media scrutiny is the Apple v. FBI fight. Even after the case was dropped against Apple, the incident raises key concerns between law enforcement's public safety interests versus individuals' privacy and civil liberties concerns. Legislators delved into the key facts of the case, discussed background on encryption and will continue to discuss this issue going forward.

Cybersecurity Task Force Minneapolis MN Executive Committee Meeting

Top issues going forward:

- CISA – conference call briefing
- Workforce issues
- Risk assessment and data analytics
- Partnerships with National Guard and private sector companies
- Critical infrastructure (in conjunction with Energy Supply Task Force)