NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
Sept. 2018

SAVE THE DATE to attend the next Cybersecurity Task Force meeting during NCSL's 2019 Executive Committee meeting January 17 -19 2019. If you have any topics you'd like us to program for our next meeting, please let any of our NCSL staff on the task force know.

Also in Cyber Task Force news:

Task Force Highlights

NASCIO Releases State Cybersecurity Governance Case Studies Report

NASCIO and DHS jointly released the "State Cybersecurity Governance Case Studies Cross Site Report" which examines six (6) areas regarding cybersecurity governance:

- Strategy and planning
- Budget and acquisition
- Risk identification and mitigation, trends include:
- Incident response
- Information sharing,
- Workforce and education

The cross-site report compares the five states across the aforementioned areas and also identifies trends. The five states are:

- Washington
- Virginia
- New Jersey
- Michigan
- Georgia

California Enacts New Cyber Legislation

At the end of August, California enacted CA AB 3075, a new cybersecurity law that officially created an Office of Elections Cybersecurity which is dedicated to combating cyberattacks on state voting

systems and includes a voter information campaign to correct targeted constituent disinformation. The new agency is housed under the secretary of state's office, was approved this week by both houses of the state legislature. A key component of the Office will include information sharing with county and city level elections officials as well, coordinating state and local efforts on cyber threats. The office will also be the point of contact for federal officials, be the overseer of local boards of election cybersecurity training. Secretary of State Alex Padilla announced earlier this year that the state would dedicate $134 million in new spending to modernize voting systems over the next few years.

Read about the Office of Election Cybersecurity.

Security Tip of the Month

Black Hat and Defcon cybersecurity experts share tips on how to protect yourself, cnet.com, Aug. 17, 2018

Here are a few of the tips from people at the annual "hacker summer camp":

- "Have a daily discipline of thinking, "What could go wrong?"
- "Set things to automatically patch. It would probably take care of 85 percent of your problems. That goes for your computers, your IoT devices -- anything that has a button."
- "Back up your phone, back up your computer, back up your tablet, then make a backup of your backup so you can restore them even if your house burns down."

Find more tips.

Federal Activity

States Oppose Federal Data Security Bill

House Financial Services Committee will vote on a bill, H.R. 6743 which was introduced by Rep. Blaine Luetkmeyer (R-Mo.) this week. The bill would preempt state data breach notification laws in favor of a federal uniform standard. Industry groups are in favor of a national standard that moves away from the state-by-state patchwork regulatory environment they are currently operate in. However some groups such as state banking and insurance regulators are gearing up to oppose the bill. The Conference of State Bank Supervisors wrote a letter against the federal legislation pointing to agreements already in place in many states with Equifax after its huge data breach last year

Read the full article.

DHS Hosts National Exercise on Election Security

State and county election officials participated in a 3-day exercise on election security in advance of the November elections. The table top exercises utilized realistic scenarios to identify best practices and areas for improvement in cyber incident planning, preparedness, identification, response and recovery. Participants also discussed the impact of a cyber incident on voter confidence, voting operations, and the integrity of elections. 44 States and the District of Columbia participated along with the Election Assistance Commission, department of Defense, Department of Justice and other Federal agency partners along with private sector vendors.

Read more here.

State Activity

Massachusetts report by the Special Senate Committee on Cyber Security Readiness, Aug. 15-18.
The Special Senate Committee on Cybersecurity Readiness, chaired by Senator Michael Moore, released a report on the State's cybersecurity readiness and response capabilities on August 15. In May of last year, the Senate created the special committee to "review and make recommendations for the state to improve its cyber security readiness, enhance technological responses to homeland security and public safety threats, and further protect financial, medical and other sensitive information." Some of the recommendations and findings included in the report are:

- To Create a joint standing committee on cybersecurity
- Cybersecurity Control and Review Board ("CCRB"), a five-person oversight committee that would be made up of private sector and cybersecurity representatives
- One of the greatest problems exacerbating the issue under discussion is that the government of Massachusetts has yet to determine a concrete definition for what types of actions fall under the realm of cybersecurity

Read the entire report

Ohio Enacts New Cybersecurity Law

Ohio enacted Senate Bill 220 which encourages businesses to voluntarily adopt strong cybersecurity controls to protect consumer data. The legislation identifies 10 different industry-recognized cybersecurity frameworks on which businesses can base their security. It also:

- Applies to a business or nonprofit entity, including a financial institution, that accesses, maintains, communicates, or handles personal information or restricted information.
- Requires a covered entity, to be eligible for the affirmative defense, to create, maintain, and comply with a written cybersecurity program that contains certain safeguards for the protection of personal information, restricted information, or both.

- Requires the cybersecurity program to meet the act's design, scale, and scope requirements and to reasonably conform to certain industry recognized cybersecurity frameworks.
- Creates an affirmative defense to a tort action against a covered entity because of a data breach, if the entity is accused of failing to implement reasonable information security controls and the entity has a cybersecurity program that meets the act's requirements programs.

NCSL Cybersecurity Staff: Susan Parnas Frederick (susan.frederick@ncsl.org), Danielle Dean (danielle.dean@ncsl.org), Pam Greenberg (pam.greenberg@ncsl.org.

Denver: 303-364-7700

Washington, D.C.: 202-624-5400