NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
November/December 2018

This will be the last newsletter of the year!

The next meeting of the Cybersecurity Task Force will be Jan. 17-18, 2019 in New Orleans, La. Please save the date! Logistics and a draft agenda will follow soon.

In staffing news, our own Danielle Dean has taken a position with NCTA - The Internet & Television Association and is no longer with NCSL. We will miss her and wish her all the best in her new position! Abbie Gruwell is moving over from NCSL's Health and Human Services Committee and will now staff the Task Force as well as NCSL's Communications and Financial Services and Interstate Commerce Committee. She will be joining us in New Orleans in January. Welcome Abbie!

Also, in Cyber Task Force news:

Security Tip of the Month

Effective Methods for Removing Personal Data Before Disposing of Electronic Devices

At least 34 states and Puerto Rico have statutes that require either private or governmental entities, or both, to destroy, dispose, or otherwise make personal information on electronic devices unreadable or undecipherable (see NCSL's chart). It's also important for individuals to be sure all personal and sensitive information is removed before donating, recycling or disposing of electronic devices. U.S. CERT has detailed information on proper disposal of electronic devices.

Read more here.

What We're Reading

Which States Have the Best Cyber Hygiene?

An article in NCSL's *State Legislatures* magazine in October identifies the states whose residents are the most and the least prepared to prevent and respond to cyberattacks. All 50 states have data breach laws requiring entities that collect personal information to notify individuals if that information has been breached. Yet, the

risk of cyberattacks varies significantly by state, as cybercriminals take advantage of residents' risky online behavior.

Read the article here.

States at Risk: Bold Plays for Change

The National Association of State Chief Information Officers (NASCIO) and Deloitte recently released their fifth biennial cybersecurity report, States at Risk: Bold Plays for Change, about the role of the Chief Information Security Officer (CISO) and cybersecurity initiatives in the states.

All 50 states now have a statewide chief information security officer (CISO) or CISO equivalent. CISOs establish, oversee and facilitate statewide security management programs to ensure information is adequately protected.

This latest report surveyed the 50 state CISOs about funding and budgets, staffing, reporting requirements, cybersecurity strategy, operations and practices and threats. Two findings specifically related to legislatures include:

- The CISO role is firmly established, increasingly through legislation.
- CISOs are increasingly required to provide reports on cybersecurity status or posture of the enterprise to legislators–4 percent are required to report monthly, 14 percent quarterly, 35 percent annually, and 35 percent on an ad hoc basis.

The report notes that the top three issues impacting states' cybersecurity remain the same as in past surveys—budget, talent shortages and increasing cyber threats. To make progress in overcoming these and other challenges, the study calls for "bold action to disrupt the status quo," calling for CISOs to:

- Advocate for dedicated cyber program funding.
- Actively participate in shaping the state's innovation agenda.
- Team with the private sector and higher education to provide a pipeline of new talent.

Federal Activity

Federal Advisory Committee Approves "Cybersecurity Moonshot" Project

With the goal of securing the internet by 2028, a subcommittee of the National Security Telecommunications Advisory Committee sent its report to the president for approval. A primary focus of the report is on interdependencies in networked technology. The report also focuses on governance, stating that "The Cybersecurity Moonshot Initiative must engender a whole-of-nation approach, including a multi-tiered governance model spanning Government, industry, and academia that align their inherent capabilities and activities towards realizing a safe and secure Internet," and contains six strategic pillars: technology, human behavior, education, ecosystem roles and responsibilities, privacy and policy. Presidential approval is expected before Thanksgiving.

Director of National Intelligence Will Examine Whether There was Foreign Interference in the Midterms

Pursuant to a September 12 Executive Order, within 45 days after the conclusion of an election, the Director of National Intelligence, in consultation with other federal departments and agencies, is required to conduct an assessment to determine whether there was foreign interference in that election. A report on the findings of the assessment of foreign interference must be given to the president no later than 45 days after the assessment is concluded. This is the first review of its kind.

The Cybersecurity and Infrastructure Security Act of 2018 Becomes Law

On November 16, the president signed H.R. 3359 into law. This bill reorganizes the Department of Homeland Security's (DHS) cyber division and creates a new DHS agency that will be called the Cybersecurity and Infrastructure Security Agency (CISA). CISA will be a full-fledged DHS agency on par with FEMA and others. This new agency will be responsible for:

(A) Furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) Identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) Assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

Read the full text of the new law here.

State Activity

2018 Security Breach Enactments

In addition to new laws in Alabama and South Dakota, which brought the number of states with security breach notification laws to 50, several other states took action related to data breaches in 2018. For example:

Colorado H.B. 1128 amends the state's data breach notification law to require notice to affected Colorado residents and notice to the Colorado Attorney General within 30 days of determining that a security breach occurred. It also imposes requirements for specific content to appear in the notice to residents and expands the definition of personal information.

Arizona's H.B. 2154 requires government and businesses in the state to notify affected individuals within 45 days of a breach. The amended law also broadens the definition of personal information and requires notice to the Attorney General and to consumer reporting agencies under certain

circumstances. In addition, the Attorney General may impose up to $500,000 in civil penalties for knowing and willful violations of the law in relation to a breach or series of related breaches.

Louisiana S.B. 361 requires notice of breaches to affected individuals within 60 days and requires notification to the Attorney General. The law also expands the definition of personal information.

Lastly, Ohio's S.B. 220 provides a legal "safe harbor" from tort claims related to a data breach for entities that have implemented and comply with certain cybersecurity frameworks.

NCSL's full list of 2018 security breach legislation is available here.

NCSL Cybersecurity Staff: Susan Parnas Frederick (susan.frederick@ncsl.org), Pam Greenberg (pam.greenberg@ncsl.org), Heather Morton (Heather.Morton@ncsl.org, Abbie Gruwell (abbie.gruwell@ncsl.org)

Denver: 303-364-7700

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