NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
Oct. 2018

October is National Cybersecurity Awareness Month (NCSAM)! The 15th annual national campaign NCSAM focuses on citizen awareness about the importance of cybersecurity, and promotes resources from government at all levels to ensure everyone has the resources they need to stay safe online. Every week has a new theme, and the initiative is jointly run by the National Cyber Security Alliance and the U.S. Department of Homeland Security. The state and local community also shares their work through the Multi-State Information Sharing and Analysis Center.

Week 1: Make Your Home a Haven for Online Safety.
Week 2: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity.
Week 3: It's Everyone's Job to Ensure Online Safety at Work.
Week 4: Safeguarding the Nation's Critical Infrastructure.

Read more information on NCSAM.

Also in Cyber Task Force news:

Task Force Highlights

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 to follow. If any task force member would like to suggest topics for this meeting, please email us at the referenced email address below. All ideas welcome!

California Signs Assemblymember Irwin's Cybersecurity Bill AB 1906 into Law
California's governor signed AB 1906 into law in late September. It mandates reasonable security features on the Internet of Things devices sold in California, in an aim to prevent future botnet attacks and minimize known vulnerabilities in our smart homes and cities. You can find the full press release on the task force website.

Louisiana Starts Cybersecurity Center at LSU Innovation Park
The Louisiana National Guard will build a Cyber Coordination Center in collaboration with Louisiana State University (LSU). The Cyber Coordination Center is currently in the approval process and would expand the National Guard's existing center at the LSU Innovation Park campus.

Still in its early stages, the center does not have a completion timeline or a budget just yet, but with Congress' approval, the Guard is hoping the project could get underway as soon as 2020.

Read the full news article.

Security Tip of the Month

Two-Factor Authentication

Have you enabled two-factor authentication for your iOS or Android devices, and for the programs and apps you use? It may seem like an annoying extra step, but it's a powerful way to keep others from taking over your accounts. PCmag.com explains. Two-Factor Authentication: Who Has It and How to Set It Up.

What We're Reading

North Dakota CIO Asks Lawmakers for 37 Additional Cybersecurity Staff

If the $12 million request is fulfilled, it would more than quadruple the size of the technology agency's cybersecurity team. North Dakota Chief Information Officer Shawn Riley reported that the state has received 34 million cyberattacks within the past six months and that the threat is rising. The request comes as Republican Gov. Doug Burgum is calling on agencies across the state government to identify ways to cut budgets between 5 and 10 percent, depending on the size of the agency. The Information Technology Department (ITD) itself already has plans to cut $77 million of its existing $245 million budget, a 31 percent reduction that will result in a loss of 17 of the agency's 344 employees. A revenue forecast released earlier this month could provide some hope for ITD that its request will be fulfilled, as the state is now projected to bring in $3.38 billion between 2019 and 2021, a 9.5 percent increase over a May 2017 forecast. Despite this, Burgum is persisting in his call for a "conservative" budgeting strategy.

More information.

Federal Activity

House Committee Approves Public-Private Cybersecurity Cooperation Act

The House Homeland Security Committee passed, under the suspension of the rules, **H.R. 6735,** sponsored by House Majority Leader Kevin McCarthy (R-Calif.). The Public-Private Cybersecurity Cooperation Act would require the Secretary of Homeland Security to establish a policy detailing how companies and other organizations or individuals can report security vulnerabilities to the Department of Homeland Security (DHS). The bill would also require DHS to create a remediation process to address the mitigation or remediation of security vulnerabilities that are reported, although consultation is only required with the attorney general, secretary of defense and "non-governmental security researchers." The bill now sits in the Senate Committee on Homeland Security and Governmental Affairs.

Read the full bill.

Department of Energy Hosts National Cyber Strategy Stakeholder Meeting

The Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response, Karen Evans announced the release of the administration's National Cybersecurity Strategy. This strategy explains how the administration will:

I. Defend the homeland by protecting networks, systems, functions, and data;
II. Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
III. Preserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
IV. Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet.

Department of Justice Hosts Cybersecurity Industry Roundtable

The Department of Justice's Criminal Division hosted a cybersecurity roundtable discussion with leaders in the private sector on the challenges in handling data breach investigations. At the event, the Cybersecurity Unit released revised guidance, which addresses new issues like working with incident response firms, cloud computing, ransomware, and information sharing. The goal is to help elevate cybersecurity efforts and build better channels of communication between law enforcement and industry.

Read more.

Secretary Kirstjen M. Nielsen Kicks Off National Cybersecurity Awareness Month

Department of Homeland Security (DHS) Secretary Kirstjen M. Nielsen kicked off National Cybersecurity Awareness Month with a conversation at the Washington Post's Cybersecurity Summit. Secretary Nielsen discussed DHS's continued efforts to secure our nation's election systems and combat the threats to our cyberspace.

Listen to the full conversation.

State Activity

Election Security

A key issue for states as they approach the November midterm elections is election security. Several states have enacted cybersecurity legislation aimed at protecting their election systems, with California passing a law that establishes an Office of Elections Cybersecurity to act as a coordinator between the secretary of state and local election officials on election security issues. For more information on election security, please visit NCSL's research page: http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx

Read the following article discussing state policy changes in cyber and elections: https://biglawbusiness.com/states-step-up-election-cybersecurity-as-federal-efforts-stall/

NCSL Cybersecurity and Security Breach Legislation
NCSL's 50-state web pages tracking 2018 cybersecurity legislation and security breach legislation are newly updated.

Cybersecurity Legislation: Thirty-five states, D.C. and Puerto Rico considered more than 265 bills or resolutions related to cybersecurity and at least 22 states enacted 51 bills so far in 2018. Some of the key issues the introduced legislation addressed include:

- Improving government security practices.
- Providing funding for cybersecurity programs and initiatives.
- Elections security.
- Targeting computer crimes.
- Restricting public disclosure of sensitive government cybersecurity information.
- Establishing cybersecurity studies, commissions or task forces.
- Promoting workforce, training, economic development.

Security Breach Legislation. The passage of bills in Alabama and South Dakota in March 2018 brought the number of states with security breach notification laws to 50. The laws require businesses or government to notify consumers or citizens if their personal information is breached. However, lawmakers in other states are still working to protect consumers in the face of continuing data breaches. At least 31 states, Puerto Rico and D.C. in 2018 considered measures that would amend existing security breach laws.

Some of the key issues in the legislation include:

- Providing for free credit freezes for victims of data breaches or that are otherwise aimed at credit bureaus or financial institutions.
- Expanding the definition of "personal information."
- Setting specific timeframes within which a breach must be reported.
- Requiring businesses to report breaches to the state's attorney general.
- Requiring notification to students, parents or guardians in the case of breaches of student information.

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