NCSL

NATIONAL CONFERENCE OF STATE LEGISLATURES

NCSL Executive Task Force on Cybersecurity
February - March 2020

Task Force Highlights

Webinar—Wed., March 18: Cybersecurity: Would You Like to Play a Game?

NCSL's National Association of Legislative Information Technology is sponsoring a cybersecurity webinar about preparing for cyber incidents on Wednesday, March 18. Hear legislative staff experts discuss how they built and trained computer emergency response teams, explore the key components and policies required to make them work, and learn how to simulate cyber incidents so your team can be prepared. Register or watch here.

Mark Your Calendar: Upcoming Meetings and Webinars

The Cybersecurity Task Force will meet this summer (exact date and location to be determined) and in Washington D.C. in conjunction with the NCSL Capitol Forum, Dec. 7-12. Additional information about the summer meeting will be available soon. Although the task force is not meeting with the NCSL Legislative Summit this year, task force members who attend the Summit will be interested in sessions on ransomware and elections security.

Federal Activity

The State and Local Cybersecurity Improvement Act (H.R. 5823)

In February, a bipartisan group of lawmakers introduced legislation to authorize a new grant program at the Department of Homeland Security (DHS) to address cybersecurity vulnerabilities on state and local

government networks. In recent years, state and local governments have been rich targets for cyber adversaries and the frequency of these attacks is accelerating. The act:

- Establishes a $400 million DHS grant program that incentivizes states to increase their own cybersecurity funding.
- Requires DHS's Cybersecurity and Infrastructure Security Agency (CISA) develop a strategy to improve the cybersecurity of state, local, tribal, and territorial governments.
- Requires state, local, tribal, and territorial governments develop comprehensive Cybersecurity Plans to guide use of grant dollars.
- Establishes a State and Local Cybersecurity Resiliency Committee so state, local, tribal, and territorial governments can advise CISA on their cybersecurity needs.

H.R. 4217, also titled "The State and Local Cybersecurity Improvement Act," was introduced in 2019. It would also provide for grants to state or local governments.

Cyberspace Solarium Commission Report

The Cyberspace Solarium Commission issued its final report this week. The commission is a bicameral, bipartisan, intergovernmental body created by the 2019 National Defense Authorization Act and charged with developing and articulating a comprehensive strategic approach to defending the United States in cyberspace. The commission is co-chaired by Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisc.), and its 14 commissioners include four members of Congress, four senior executive agency leaders, and six nationally recognized experts from outside of government. The report outlines a new cyber strategy called "layered cyber deterrence" and provides more than 75 recommendations for action across the public and private sectors. The strategy relies on a resilient economy, empowering CISA so that it "becomes so appealing to young professionals interested in national service that it competes with the NSA, the FBI, Google, and Facebook for top-level talent (and wins)", the creation of a new a National Cyber Director with oversight from new congressional Cybersecurity Committees, the recognition that the private sector needs to strengthen their security posture because most cyber infrastructure is owned by the private sector, and the prioritization of election security.

State Activity

Cybersecurity Legislation in 2020

Cybersecurity remains a focus in state legislatures, as many propose measures to address cyberthreats directed at governments and private businesses. At least 35 states, Washington, D.C., and Puerto Rico have introduced more than 365 bills or resolutions this year that deal significantly with cybersecurity. Some of the areas seeing the most legislative activity include measures:

- Requiring government agencies to implement training or specific types of security policies and practices and improving incidence response and preparedness.
- Increasing penalties for computer crime or addressing specific crimes, e.g., ransomware.
- Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.
- Supporting programs or incentives for cybersecurity training and education.

See NCSL's summary and list of 2020 Cybersecurity Legislation.

What We're Reading

Ransomware Attacks Prompt Tough Question for Local Officials: To Pay or Not to Pay? *(Task Force members Senator Susan Lee and Senator David Carlucci featured.)*

There were at least 113 successful ransomware attacks on state and local governments last year, according to global cybersecurity company Emsisoft, and in each case, officials had to figure out how to respond. Some states have passed laws to target cybercriminals who deploy ransomware, but prosecutors have rarely used them. And local officials often are left vulnerable. Read more here. *Stateline*

Ransomware Attacks Map chronicles a growing threat
An intelligence analyst at the cybersecurity firm Recorded Future, published research that caught the attention of security analysts and government officials everywhere. It included a list of 169 different ransomware attacks against state and local governments dating back to 2013, but that were now cropping up at an alarming rate. Read more and see the current ransomware map. *StateScoop*

Governments Are Paying Increasingly High Ransoms, Study Says
A new study by Deloitte shows that state and local governments are paying out more money to ransomware hackers than in previous years — sometimes more so than their private-sector equivalents. Read more. *Government Technology*

Live Coronavirus Map Used to Spread Malware
Cybercriminals constantly latch on to news items that captivate the public's attention, but usually they do so by sensationalizing the topic or spreading misinformation about it. Recently, however, cybercrooks have started disseminating real-time, accurate information about global infection rates tied to the Coronavirus/COVID-19 pandemic in a bid to infect computers with malicious software. Read more from here. *Krebs on Security*

Cyber planners should be carefully watching the coronavirus
Cyber experts across the globe should take note that COVID-19 is causing the same severe disruptions and tangible financial harm to manufacturing and transportation sectors predicted to accompany a large scale cyberattack. Read more. *The Hill*

Virginia builds new model for quantifying cybersecurity risk
A shortage of resources amid an uptick in ransomware attacks has prompted Virginia technology officials to develop a unique model for evaluating IT security threats and prioritizing their defenses. The new model, officials said, allows them to define cybersecurity risks in exact dollar amount, shifting away from a system in which policymakers relied on anecdotal information and estimates when allocating resources to the most sensitive government functions. Read more here. *StateScoop*

NCSL cybersecurity staff: Susan Parnas Frederick, Pam Greenberg and Abbie Gruwell.

Visit the Cybersecurity Task Force website for information on upcoming and past meetings and other cybersecurity resources.

Denver: 303-364-7700

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