NCSL

NATIONAL CONFERENCE OF STATE LEGISLATURES

# NCSL Executive Task Force on Cybersecurity
# June-July 2019

## Task Force Highlights

The next meeting of the Cybersecurity Task Force will be held at NCSL's Legislative Summit in Nashville, Tenn., on Aug. 4 (register for the meeting here). Registration for the Summit is now open (register here for the Summit). PLEASE NOTE: THESE ARE TWO SEPARATE REGISTRATIONS!

A preliminary agenda is available here; we will send an updated link with the finalized agenda. Thank you to all the task force members who contributed session ideas.

**Recorded Webinar: Cybersecurity Inside State Legislatures**

State legislatures are vulnerable to many different types of cyberattacks—politically motivated cyber attackers and hacktivists, organized attackers, disgruntled employees or even benign computer trespassers. Legislative IT CIOs and managers are very familiar with these threats: They named cybersecurity as the No. 1 priority in recent NCSL surveys. In this webinar, sponsored by NCSL's National Association of Legislative Information Technology, find out how legislatures are dealing with cyber threats, including information about funding, staffing, training, preparation and policies. Jeff Ford, chief technical officer with Indiana's Legislative Services Agency, and Michael Norris, cybersecurity administrator with LEG-TECH in Washington, share their expertise. View the webinar here.

## Federal Activity

The U.S. Senate is moving quickly on S 315, a bill to authorize cyber hunt and incident response teams at the Department of Homeland Security (DHS). The legislation calls for the DHS to provide federal asset response activities and timely technical assistance to federal and non-federal entities (presumably states are included here) regarding actual or potential security incidents "as appropriate and on request." Areas of assistance include restoration of services after a cyberattack, analysis of cyber risk, and recommendations to improve network security.

Bipartisan congressional legislation, the Active Cyber Defense Certainty Act, will be introduced this week to provide a legal defense to hacking victims in the private sector who “strike back” at their attackers. The bill recognizes that “As a result of the unique nature of cybercrime, it is very difficult for law enforcement to respond to and prosecute cybercrime in a timely manner, leading to the existing low level of deterrence and a rapidly growing threat.” This legislation seeks to amend the 1986 Computer Fraud and Abuse Act to allow companies and entities to "hack back," letting them use defense measures to identify and stop digital assaults on their networks. FBI notice is required.

The U.S. House Intelligence Committee has begun to hold hearings on “deep fakes” which are video forgeries using artificial intelligence and video editing software to create forged videos of people doing or saying things they never did.

## State Activity

Susan Frederick and Pam Greenberg will testify on June 21 before the Vermont Joint Information Technology Committee on our task force’s Cybersecurity Conversation Guide and state activity in the cybersecurity space.

### State Cybersecurity Legislation

Forty-three states introduced more than 250 bills related to cybersecurity in 2019 (not including legislation related to security breach notification). Of the cybersecurity bills, 44 have been enacted so far this year.

A majority of the newly enacted laws are aimed at strengthening security practices within government. The other enactments fall into several main categories:

- Elections security.
- Workforce and cybersecurity education initiatives.
- Cybersecurity commissions and study groups (several are considering the use of distributed ledger technologies for cybersecurity).
- Insurance data security.
- Exemptions of cybersecurity information from public records laws.

## What We Are Reading

### DHS Needs Help Peeking into State and Local Networks, Cybersecurity Official Says

Rick Driggers, the deputy assistant director of the Cybersecurity and Infrastructure Security Agency, said more information-sharing agreements are needed. Read more here.

### Report: Ransomware Attacks Against State and Local Government on the Rise

Publicly acknowledged ransomware attacks against state and local governments jumped 39% in 2018, and the first few months of 2019 show no sign that trend is cooling. Read more here.

### Verizon’s Data Breach Investigations Report

This report is built upon analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches. Download the full report here.

**FBI Internet Crime Complaint Center (IC3) 2018 Annual Report**
The statistics gathered by the FBI's IC3 for 2018 show internet-enabled theft, fraud and exploitation remain pervasive and were responsible for a staggering $2.7 billion in financial losses in 2018. Read more here.

**Center for Long-Term Cybersecurity at the University of California, Berkeley New Report: Improving Cybersecurity Awareness in Underserved Populations**
This new report highlights how "underserved" residents in San Francisco—including low-income residents, seniors and foreign language speakers—face higher-than-average risks of being victims of cyberattacks. Download the report here.

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

Denver: 303-364-7700

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