NATIONAL CONFERENCE OF STATE LEGISLATURES

# NCSL Executive Task Force on Cybersecurity
# March - April 2019

## Task Force Highlights

The next meeting of the Cybersecurity Task Force will be at NCSL's Legislative Summit in Nashville, Tenn., on Sunday, Aug. 4. Registration for the Summit is now open, and our task force registration will be available soon.

We'll be sending a registration link and our agenda for the Cybersecurity Task Force meeting at the Summit soon. Thank you to all the task force members who contributed session ideas.

## Federal Activity

### Protect Our Elections Act of 2019

Senators Marco Rubio (R-Fla.), Chris Van Hollen (Md.), Susan Collins (Maine) and Ben Cardin (Md.) introduced the bipartisan bill S. 825, the "Protect Our Elections Act of 2019." This bill amends the Help America Vote Act of 2002 and would prohibit foreign nations or nationals from owning or controlling companies involved in the U.S. election infrastructure.

The bill would exclude the United Kingdom, Canada, Australia, and New Zealand from the ban on owning or controlling election system companies and would require state and local governments to conduct an annual evaluation of their election service providers to ensure none are under the control of a foreign nation or foreign citizen.

### New Bill Would Expand Children's Online Privacy Protection Act

Senators Markey (Maine) and Hawley (Mo.) introduced legislation that would amend the Children's Online Privacy Protection Act of 1998 to prohibit internet companies from collecting personal and location information from anyone under the age of 13 without parental consent and from anyone ages 13 to 15 without the user's consent.

The legislation also creates an "eraser button" so parents and kids can delete personal information, and a "Digital Marketing Bill of Rights for Minors" that limits the collection of personal information from teens. The bill additionally establishes a Youth Privacy and Marketing Division at the Federal Trade Commission, which will be responsible for addressing the privacy of children and minors and marketing directed at children and minors.

### Tightening Security of Sensitive Research at Universities

In the U.S. House, Republican members have introduced H.R. 1678 , the "Protect Our Universities Act of 2019." This bill seeks to protect sensitive research projects at U.S. universities by barring researchers who work on those projects from using any technology from companies such as Kaspersky or Huawei. It would also require background checks on students who work on those sensitive projects from Russia, China, Iran or North Korea.

## Security Tip of the Month

### IRS kicks off annual list of most prevalent tax scams with 'Dirty Dozen' campaign

Kicking off the annual "Dirty Dozen" list of tax scams, the Internal Revenue Service (IRS) in March warned taxpayers of the ongoing threat of internet phishing scams that lead to tax-related fraud and identity theft. The IRS reports on new variations of phishing schemes, such as one where taxpayers are victimized by a creative scheme that involves their own bank account. It also describes schemes aimed at tax professionals, payroll offices and human resources personnel. If a taxpayer receives an unsolicited email or social media attempt that appears to be from the IRS, they should report it by sending it to phishing@irs.gov. Read more here.

## State Activity

### 2019 State Legislation Related to IoT and Connected Devices Security

At least 11 states have introduced legislation related to the internet of things (IoT) this year, many following the lead of California's A.B. 1086, sponsored by Task Force co-chair Assemblymember Jacqui Irwin. The states considering bills this year include Illinois, Kentucky, Massachusetts, Maryland, New Jersey, New York, Oregon, Rhode Island, Vermont, Washington and additional proposals in California. Contact NCSL staff Pam Greenberg for details.

### 2019 Cybersecurity Legislation

At least 35 states and Puerto Rico have introduced more than 160 bills or resolutions this year related to cybersecurity. Some of the key areas of legislative activity include:

- Improving government security practices,
- Addressing the security of connected devices,
- Relating to cybersecurity insurance or standards for insurance data and information security,
- Addressing elections security, and
- Creating cybersecurity commissions, task forces or studies.

NCSL's summary of cybersecurity legislation for 2019 is available here.

## What We are Reading

### Microsoft's Takedown of Iranian Fake Sites Shows 'Creative Lawyering,' Experts Say

As foreign government-backed hackers increase their attacks against the private sector, companies are increasingly taking matters into their own hands and coming up with creative ways to shut them down. Microsoft used a novel legal strategy to get a court order to shut down 99 malicious websites that appeared to be sponsored by the Washington state tech giant but were actually phony—a ploy by an Iranian government-linked hacking group to steal information from Microsoft customers. Read more here.

### Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role

State governments collect more information about citizens than does the private sector, highlighting the importance of safeguarding the data. This new report from the National Association of State Chief Information Officers (NASCIO) provides a snapshot of the state chief privacy officer (CPO) position, the background of CPOs, what they do in their roles, how the role is administratively structured and their advice for states interested in creating the position. Download the report here.

### Tennessee, Virginia Among States to Launch Girls-only Cybersecurity Program

A national cybersecurity program to encourage more high school girls to go into the industry kicked off this month. The Girls Go CyberStart program is the result of a partnership between 27 state governors and the SANS Institute. The goal of the program is to encourage more girls into the cybersecurity sector and reduce the digital skills gap in America." Read more here.

### The 7 Biggest Cybersecurity Threats in an IoT World

The many connected devices now coming out are posing a huge challenge to cybersecurity professionals. Seven of the most significant cybersecurity threats the IoT poses today include:

1. Hidden, exploitable potential vulnerabilities,
2. Forgettable devices,
3. Recognizing an IoT attacker's goals,
4. Balancing security with user expectations,
5. Irresponsible manufacturers,
6. Insiders who take the bait, and
7. The battle for disused devices.

Read more here for recommendations on how to stay ahead of the challenges.

### Insurers Creating a Consumer Ratings Service for Cybersecurity Industry

Some of the world's biggest insurers plan to work together on an assessment of the best cybersecurity available to businesses, an unusual collaboration that highlights the rising dangers posed by digital hackers. The program, which was launched by the Marsh brokerage unit of Marsh & McLennan Co., will evaluate cybersecurity software and technology sold to businesses. Marsh will collate scores from participating insurers, which will individually size up the offerings, and identify the products and services considered effective in reducing cyber risk. The results will be available to the public on Marsh's U.S. website. Read more here.

NCSL Cybersecurity Staff: Susan Parnas Frederick, Pam Greenberg, Abbie Gruwell and Heather Morton.

Denver: 303-364-7700

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