NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
May 2018

Good afternoon Task Force members. With less than a week before our next NCSL Executive Task Force on Cybersecurity meeting in Denver, Colorado on Friday, May 11th, it is time to **SAVE THE DATE** for the Cyber Task Force meeting at the **NCSL Legislative Summit in Los Angeles**! The task force is meeting Monday, July 30th.

Also in Cyber Task Force news:

Task Force Highlights

Legislation by Cyber Task Force Member, Louisiana State Rep. Barry Ivey
Rep. Ivey introduced the Inmate Rehabilitation and Computer Technology Development Act earlier this year. The bill would create an inmate rehabilitation and computer technology development program and an advisory council responsible for administering resources, job training and the mentoring needed to direct successful program participants into the technology workforce. The bill has moved out of committee and now sits in the full House chamber. The legislative session ends June 4.

NCSL Staff Present to NASCIO D.C. Fly-In Delegation
Susan Frederick and Danielle Dean discussed the work of the Cyber Task Force before a full house of state CISOs last month. The discussion included information on upcoming Task Force programming as well as highlighting our most recent work product "Budgeting for Cybersecurity."

Cyber Task Force Meeting in Los Angeles is Monday, July 30!
Although we will see many of you next week at our meeting in Denver, we also hope to see you at our future meeting in L.A. on July 30. A registration link for this meeting will be sent to you soon so watch your inbox. We hope to provide you with programming on Cybersecurity and Disaster Response, Data Breach and the Entertainment Industry, and Responding to New Security Threats in Legislatures. We are happy to be partnering with NCSL's legislative technology staff section (NALIT) on the latter program.
If Task Force members have a session idea that they would like to see programming on at a future meeting, please let us know!

Partner Highlight

AT&T Public Sector Page on LinkedIn

AT&T is promoting the NCSL Cybersecurity Task Force-Budgeting for Cybersecurity Guide on their public-sector page on LinkedIn. The introduction states: "budgeting for state cybersecurity efforts is a challenging process. Check out the NCSL discussion guide for legislators, chief information security officers and chief information officers. *You can follow on LinkedIn here.*

Security Tip of the Month:

Malware

Does your computer seem sluggish? Are there new toolbars on your web browser that you don't remember downloading? Do you see pop-up ads as soon as you turn on your computer or when you're not even browsing the web? These symptoms could mean that your computer is infected with spyware or malicious software. Microsoft has hints about how to detect malware symptoms and how to prevent and remove viruses and other malware from your Windows computer.

Articles We Are Reading

Local Governments' Cybersecurity Crisis in Eight Charts

Baltimore and Atlanta are the latest cities hit with debilitating cyber-attacks that have forced essential government services offline. Atlanta experienced a ransomware attack that affected police files, the court system and even resident online bill paying portals for almost a week. Baltimore's 311 and 911 dispatch system was offline for over 17 hours. An NCSL "Big 7" coalition member, the International City/County Management Association (ICMA) teamed up with GovTech to create a local city government cybersecurity survey in 2016. This article summarizes the survey results and publishes several charts as visual representations of larger cybersecurity management themes. In summary, more work needs to be done.

Read the full article here.

Atlanta Recovering from a Multi-Million Dollar Ransomware Attack

A New York Times article on the Atlanta ransomware attack delves into how the city had been affected for almost a week with a wide-range of government services out of commission. Dell SecureWorks is the Atlanta-based security firm helping the city deal with the aftermath. Dell identified the attacker as SamSam, a group known for soliciting high ransoms—typically about $50,000 bitcoin—for unlocking systems.

The full article can be read on their website.

State Scoop Article–Arizona hires cybersecurity firm to manage risk across state government

RiskSense, a New Mexico-based firm, will be responsible for monitoring and managing all 133 state agencies' security activity on the state network. Arizona CISO Mike Letterman will oversee the program. The article highlights some high-profile vulnerabilities the state has been working to fix. It also mentions that Governor David Ducey formed the Arizona Cybersecurity Team, which includes Letterman, CIO Morgan Reed and other state and private sector members.

More information can be found here.

GovTech on the Cybersecurity Workforce

One of the biggest challenges that organizations face as they try to keep up with a growing number of cyberattacks is finding workers with the right skills. Some states are addressing this problem head on. Programs in Georgia, Virginia, and Ohio offer lessons for other states on how to increase the pool of cybersecurity professionals and encourage students to pursue the profession.

GovTech's full article is found here Boosting the Cyber workforce.

Federal Activity

Government Accountability Office to Study Federal Cyber Regulation Synchronization

Starting this month, the Government Accountability Office **(**GAO) will study how to coordinate and harmonize federal cyber regulations across agency jurisdictions. The decision was spurred by House Oversight and Government Reform Committee Chairman, Trey Gowdy's (R-S.C.) letter sent on October of last year. The National Association of State Chief Information Officers NASCIO wrote a letter to White House and sent a one-pager on federal audit processes.

Federal Agency "Turf War" on Cybersecurity

While the GAO researches how to coordinate and unify cybersecurity efforts across federal agencies, the Hill reports congressmembers are concerned that 'bureaucratic turf wars' are complicating the government's ability to effectively respond to cyber threats. The executive branch does not have a principle authority assigned to handle cyber, which also means "virtually every congressional committee has a say in the federal government's cybersecurity efforts." The article quotes Michael Sulmeyer, a former cyber policy official at the Pentagon stating: "responsibilities are so spread across so many parts of the federal government and across so many congressional jurisdictions…that [it] is very hard to get coherent policy government wide."

Read the full article here.

Office of Personnel Management Publishes Guidance on Hiring for Cyber Employee Skills Gaps

The Office of Personnel Management (OPM) published guidance on how to address the federal cybersecurity talent shortage, and gives agencies one year to report back to OPM about their cyber "work roles of critical need." Roles deemed as "critical need" are any positions that have the

'greatest skills shortages' and are critical to the agency's mission. OPM is also giving agencies a year to report on root causes of these shortages as well as what they plan to do to fill the gaps.

Read the full article here.

Election Security Included in 2018 Omnibus and More Funding Considered in 2019
Around $380 million in grant funding originally appropriated under the Help America Vote Act was finally authorized to be disbursed in the 2018 omnibus Consolidated Appropriations Act to assist states secure and improve elections systems.

Read the full list of funding by state and approved uses here.

State Activity

Ransomware Statutes
With the passage of H.B. 5257 and its companion H.B. 5258 in April, Michigan became the fifth state to enact legislation that expressly defines and criminalizes ransomware or computer extortion in statute. Ransomware is computer malware that is installed covertly on a victim's computer, denying access to the computer or data. Perpetrators then demand payment in exchange for returning access or not publishing or exposing data held on the computer. The other states with ransomware laws are:

- California: Calif. Penal Code § 523 (2016 S.B. 1137)
- Connecticut: CGS § 53a-262 2017 H.B. 7304, Public Act 17-223
- Texas: 2017 H.B. 9, Chap. 684
- Wyoming: Wyo. Stat. §§ 6-3-506, 6-3-507

NCSL Cybersecurity Staff: Susan Parnas Frederick (susan.frederick@ncsl.org), Danielle Dean (danielle.dean@ncsl.org), Pam Greenberg (pam.greenberg@ncsl.org, and Heather Morton (heather.morton@ncsl.org)