NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

NCSL Executive Committee Task Force on Cybersecurity News
January 2018

NCSL staff is excited to announce that the Executive Committee Task Force on Cybersecurity has been approved by the NCSL Executive Committee to continue for the next two years! As we begin 2018, we look forward to hearing what topics all of our members want to discuss, and NCSL looks forward to providing the best resources, speakers and written products to further your efforts to securing state networks and becoming experts on cybersecurity policy in your state. This newsletter will focus on 2017 end-of-the year highlights, and what we have an eye on for the beginning of the new year.

But first:

Task Force Highlight: Louisiana Governor Edwards Establishes Cybersecurity Commission

Gov. John Bel Edwards issued an executive order on Dec. 7, establishing the Louisiana Cybersecurity Commission. The governor will appoint up to 15 commissioners who are tasked with developing various reports to the governor's office and the Louisiana Legislature. The goals of the Commission include:

- Identify, prioritize, and mitigate Louisiana's cyber risk;
- Grow Louisiana's cybersecurity workforce and educate the public/private sectors about cybersecurity;
- Enhance Louisiana cyber emergency preparedness and response capabilities;
- Monitor, understand, and share cyber threat information;
- Identify, prioritize, acquire, and establish funding mechanisms to enhance Louisiana's cybersecurity efforts; and
- Facilitate economic development by promoting a cyber-safe Louisiana for businesses and consumers.

Is your state looking at specific cybersecurity issues that you would like to feature in our newsletter? Are you working on cybersecurity legislation that you would like to highlight? Send us your cyber news and we will share it with the task force.

Welcome! New Sponsor Highlight: Consumer Data Industry Association

We are excited to announce the Consumer Data Industry Association (CDIA) has joined as a sponsor of the Cybersecurity Task Force. CDIA is an international trade association dedicated to the education of consumers, legislators, media and regulators about the benefits of the responsible use of consumer data. CDIA members provide businesses with the information and analytical tools necessary to manage risk and help ensure fair and safe transactions for consumers and facilitate competition to create opportunities for customers and the economy. Our contact will be Sarah M. Ohs, Manager of Government Relations.

NCSL Capitol Forum

Thank you to all who attended the Cybersecurity Task Force meeting during our annual Capitol Forum! We hope that you enjoyed the sessions and if you have any topics you'd like the task force to program for our next meeting, please let any of our NCSL team know. The next meeting will take place in conjunction with the Spring Executive Committee Meeting in Denver, May 10-12. For those who were unable to attend, but are interested in the resources from the sessions, here are a few highlights:

- The Intersection of Cybersecurity and Autonomous Vehicles
  - Presentation: Automated Driving Systems: A Vision for Safety, NHTSA
  - NHTSA Autonomous Vehicle Cybersecurity Guidance
- A New World: Blockchain
  - Presentation by Richard Morris, Department of Financial and Professional Regulation, Illinois
  - NCSL: Blockchain Technology: An Emerging Public Policy Issue, LegisBrief, Nov. 2017
- Defending Democracy Against Cybersecurity Attacks
  - NCSL Blog Post

All session materials and information on our upcoming task force meetings can be found on the Cybersecurity Task Force website.

Cyber Insurance Model Law

On Dec. 12, 2017, the National Association of Insurance Commissioners (NAIC) approved their Insurance Data Security Model Law for data security in the insurance industry. NAIC is a U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Complete with an analysis of the model law, here are some of the highlights:

- The model law would apply to all licensees;
- Licensee must identify and assess risks to nonpublic information;
- Licensees must implement and maintain a written information security program to mitigate identified risks;
- Requires annual compliance certification and five-year period of records retention;
- Requires cybersecurity event investigation, and
- Requires cybersecurity event reporting.

Federal Activity

New Law: The Strengthening State and Local Cyber Crime Fighting Act of 2017

The administration signed the Strengthening State and Local Cyber Crime Fighting Act of 2017 into law on Nov. 2017, which authorizes the National Computer Forensics Institute, within the U.S. Secret Service, to train, offer resources and provide timely actionable information related to cybercrime to state officers and prosecutors. Funding is allocated through FY 2022, and broadens the institute's functions to include:

- Educating officers, prosecutors and judges on current cyber and electronic crimes,
- Training officers to conduct investigations, and
- Ensure timely, actionable, and relevant expertise and information related to cybercrime and threats.

The law also authorizes the Department of Justice's Bureau of Justice Assistance to enter into cooperative agreements or grant disbursements for training and technical assistance to help law enforcement officers, investigators, auditors, and prosecutors identify, investigate and prosecute white collar crime. The list of offenses includes high-tech crime, and internet-based crime against children and child pornography.

House Passes the Cyber Vulnerability Disclosure Report Act

On Jan. 9, the House passed H.R. 3202, the Cyber Vulnerability Disclosure Report Act and the bill now awaits action in the Senate. H.R. 3202 requires the establishment of policies and procedures for coordinating cyber vulnerability disclosures across the federal government and other stakeholders. The bill also requires reporting on when such policies were used to disclose cyber vulnerabilities and how industry and other stakeholders acted upon this information. The full text of the bill can be found here.

Senator Introduces Bill on Cybersecurity Standards for Consumer Reporting Agencies

Senator Elizabeth Warren introduced S. 2289 on Jan. 11, which currently sits in the Senate Banking, Housing, and Urban Affairs committee. The bill would create an Office of Cybersecurity at the Federal Trade Commission to monitor data security at consumer reporting agencies. The office would also be required to promulgate cybersecurity standards for consumer reporting agencies to adhere to. The bill would also impose penalties on credit reporting agencies for data breaches that put sensitive consumer data at risk. A summary of the bill can be found here.

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)

Denver: 303-364-7700

Washington: 202-624-5400