NCSL Executive Task Force on Cybersecurity
December-January Newsletter

Task Force Highlights

The Task Force met at the 2019 Capitol Forum on Monday, December 9. We were fortunate to have Deputy Director of the Cybersecurity and Infrastructure Security Agency (CISA) Matthew Travis return to give us an update on CISA's recent projects and upcoming collaboration with states to further protect election security.

Members participated in a hands-on tabletop exercise on ransomware with the University of Maryland Center for Health and Homeland Security. The Task Force worked through a realistic ransomware scenario and had to make decisions to protect sensitive information and interact with the media.

We also discussed election security, cyber emergency declarations, and discussed topics for our next meeting this summer. If you would like to submit ideas for upcoming sessions, please contact NCSL staff.

The Task Force is also starting an exciting new project – the Privacy Working Group. This sub-group will examine consumer data privacy, government use of data, privacy models, and compliance issues. The first meeting of the Privacy Working Group will be this summer in Washington, D.C. Please let us know if you are interested in participating in the Privacy Working Group.

Also, NCSL staff presented our latest LegisBrief on State and Federal Efforts to Enhance Cybersecurity. Our agenda and resources are here.

Call for Elections Security Advocates

In April, NCSL will be leading a coalition to encourage Congress and the Administration to prioritize elections security. If interested, please contact Susan Frederick (susan.frederick@ncsl.org).

Federal Activity

The bipartisan Cybersecurity State Coordinator Act was introduced in the Senate last week, which would ensure that every state has a cybersecurity coordinator to prevent and respond to cyberattacks. CISA

would work with the coordinators to increase coordination on cyber issues and increase information sharing for cyber threats.

The FBI is expanding its notifications about cyber attacks on elections infrastructure. The agency will now notify state-level, local, and county authorities in the case of election hacking to better protect against interference. Although the FBI previously only notified affected counties, the agency recognized that because state election officials certify results it is essential to keep them informed on elections activity at the county level.

The National Institute of Standards and Technology released the final version of their landmark privacy framework, with some revisions to further stress the risk of emerging technologies in managing personal information. The guidance is intended to help companies and organizations comply with the expanding regulatory landscape and identify privacy outcomes. NIST laid out five "core" privacy functions based on public comment: identify, govern, control, communicate and protect and includes specific implementation recommendations. The framework also comes with a roadmap to support stakeholder engagement.

The Treasury Department is seeking public comment on a proposed request for information to financial institutions about cybersecurity and critical infrastructure. The Treasury's Office of Cybersecurity and Critical Infrastructure Protection is looking for more information about the cyber vulnerabilities of financial institutions, especially relating to their connection to other critical sectors like energy. The Treasury says this information will help the department work with agency and industry partners to develop risk management protocols.

State Activity

State Cyber Civilian Corps Now in Two States

Ohio's governor in October signed legislation (S.B. 2) allowing trained, civilian technical experts to volunteer to assist the state in the event of a critical cyber incident. Michigan was the first state to create a civilian corps, when the legislature passed H.B. 4508 in 2017.

Ohio's S.B. 52 creates a Civilian Cyber Security Reserve Force. The force will be trained to educate and protect state, county, and local government entities, critical infrastructure (including election systems), businesses, and citizens from cyber attacks. Reserve members may be paid when called to state active duty, but while performing any drill or training, they serve in an unpaid volunteer status. When called to state active duty by the governor, reserve members function as civilian members of the Ohio organized militia.

Michigan's Cyber Civilian Corps program "allows civilians with expertise in addressing cybersecurity incidents to volunteer and provide a rapid response and assistance to a municipal, educational, nonprofit, or business organization in need of expert assistance during a 'cybersecurity incident.'" The program, administered by the Department of Technology, Management and Budget (DTMB), provides training for volunteers, who may also be compensated for travel and subsistence expenses incurred during a deployment. The program has deployed volunteers for two cyber incidents at local governments.

The Michigan Office of the Auditor General in September completed a performance audit of the Michigan Cyber Civilian Corps to assess the effectiveness of DTMB's administration of the program. The

audit found the program to be moderately effective but made recommendations to address problems regarding training for volunteers and volunteers not meeting program requirements.

What We're Reading

Iowa paid a security firm to break into a courthouse, then arrested employees when they succeeded.
The state of Iowa contracted with two cyber security professionals from a prominent cybersecurity company to conduct "penetration tests" of certain municipal buildings in September, particularly courthouses. The workers were arrested in the course of doing their jobs. The charges still have not been dropped, despite admissions by the state of a miscommunication with county authorities. The incident has sparked concern across the cybersecurity industry, including worries that ramped-up efforts to test voting facilities in advance of the 2020 presidential election may put security professionals at risk.

The U.S. Conference of Mayors passed a resolution at its annual conference pledging not to pay ransoms. The resolution states that paying ransoms encourages others to conduct similar attacks by showing there could be a financial benefit, and that it benefits municipal governments to de-incentivize these attacks to prevent further harm. The Conference of Mayors is composed of mayors representing cities with more than 30,000 residents.

Government Technology Magazine rounds up the industry's cybersecurity predictions for 2020.

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