

Testimony for the Public Hearing before the Public Safety and Security Committee of the Connecticut General Assembly on HB 6317

Tuesday, February 17, 11:30 AM, Room 2B, Legislative Office Building

Good morning, Senator Larsan, Representative Dargan, and distinguished members of the Public Safety and Security Committee.

On behalf of the National Association of State Chief Information Officers (NASCIO), we thank you for the opportunity to provide public testimony in regards to House Bill #6317, "An Act Establishing Public-Private Partnerships To Provide Internet Security Training and Exercises."

Each year, states are facing greater numbers of evolving and sophisticated cyber-attacks. In addition to states serving as a repository of sensitive data about our citizens and homeland, states increasingly utilize the online environment to deliver vital services, maintain critical infrastructure such as public utilities, and ensure our first responders receive the data they need in crisis situations. While 90 percent of critical infrastructure is in private hands, state government IT facilities, networks and systems are a vital component of the nation's critical infrastructure and a disruption or failure due to a cyber-attack could be crippling to citizens and businesses alike.

Today, with this testimony, we want to provide the Committee information on the readiness of state governments to defend against and respond to major cyber-attacks, as well as opportunities to collaborate to minimize the risk to our nation through collaboration. We'll outline the threat landscape and how states, along with the private sector, can work together to better secure state government and reduce risks.

State governments are at risk from a host of new and aggressive security threats that require a formal strategy, adequate resources, and constant vigilance. Most state systems face cyber-attacks every day, ranging from a few thousand attempts to as many as 10 million per day—some domestic, many international. To win this ongoing battle, state IT experts have to be right every time, while hackers need to only be right once. For this reason, cybersecurity continues to be one of the major "hot button" issues for state CIOs like Connecticut's Mark Raymond, and one that receives increasing attention from governors and other elected officials throughout the states. As these attacks continue to grow more sophisticated, both public and private sector entities will need to develop better tools and increase collaboration to both deter attacks and plan a coordinated response to contain the damage from successful attacks. This ultimately requires a multi-sector approach, with all levels of government and private industry working together.

According to the 2014 Deloitte-NASCIO Cybersecurity Study, "State Governments at Risk: Time to Move Forward," state Chief Information Security Officers (CISOs) report insufficient funding remains the leading barrier to battling cyber threats. State governments spend far less on cybersecurity than comparable private sector organizations. Approximately 6 in 10 states cited an increase in sophistication of threats, up from roughly half in our 2012 survey, showing an increasingly difficult and risky threat environment. Finally, the number of states citing a shortage of qualified cybersecurity professionals jumped to 59 percent in 2014 from 46 percent in 2012. On a more positive note, the role

of the state CISO is becoming more formalized and standardized, with the CISO having enterprise-wide responsibilities over governance, risk management, and compliance functions becoming increasingly commonplace.

While funding is certainly an issue, it is not the *only* issue impacting state cybersecurity: it is also a policy and skilled personnel issue. On the latter two fronts, teaming with the private sector can be beneficial for state governments to improve preparedness and response to cyber-attacks.

On policy, perhaps the single key to ensuring a substantial attack does not blindside us is facilitating greater information sharing between the private sector and partners in government. Several states have created formal or informal commissions, committees and working groups to promote the exchange of information among key critical infrastructure partners, a wide range of experts in the cybersecurity field, and other important stakeholders.

For instance, the Texas Cybersecurity, Education and Economic Development Council (TCEEDC), was created to leverage public/private partnerships to examine the infrastructure of the state's cybersecurity operations. Its members are comprised of representatives from across Texas with backgrounds in cybersecurity and from government, academia, and industry. Its objectives include improving the infrastructure of the state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education. TCEEDC made recommendations in 2012 that created a framework for statewide action on cybersecurity that promoted better cybersecurity governance, as well as a stronger partnership between the state and its private sector and "non-government" partners over the long-term.

Michigan launched the "Michigan Cyber Initiative" in 2011, which helped create a focal point for the state, its localities, academic institutions, and the private sector to work together on cybersecurity. They recommitted to this effort in 2015, and are establishing a number of public private partnerships to improve state cybersecurity preparedness, mitigation, and response capabilities. These include cyber exercises between the state and its partners, education and awareness campaigns, a "Cyber Defense Response Team" to support state government and key stakeholders in Michigan during and after a cyber event, and developing better cybersecurity policies and governance across the state by working with private sector experts on best practices.

Virginia established a Virginia Cyber Security Commission by executive order approximately one year ago. Its objectives included identifying high risk cyber security issues facing the Commonwealth of Virginia, including, "advice and recommendations related to securing Virginia's state networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destruction of the Commonwealth's data."

As a whole, NASCIO sees the promotion of private-public partnerships on these type of efforts as providing tangible benefits to the state. First, it allows the state and private sector partners to create a knowledge network that they can tap. As a result, all parties become more apprised of the threats to their own networks and those of the entities in their region. Finally, both the private and public sector tend to walk away able to learn best practices, better governance models, and identify policies that will better secure their systems.

Cybersecurity is complex and multi-dimensional. Most importantly, it's not just a technology issue. For states, it's certainly about reducing business risk and maintaining citizen trust. With the diffuse threat and diverse actors, cybersecurity requires a many-to-many approach. Leveraging and collaborating with the private sector and finding ways to share information and resources among public and private sector entities will be crucial moving forward. From a state government perspective, NASCIO firmly believes cybersecurity is a "team sport". We applaud Connecticut State Representative Caroline Simmons for highlighting this issue and identifying ways to protect the state's digital assets.

Thank you for considering our testimony.

Doug Robinson
Executive Director
National Association of State Chief Information Officers (NASCIO)
201 East Main Street, Suite 1405, Lexington, KY 40507
859.514.9153; [drobinson@NASCIO.org](mailto:drobenson@NASCIO.org)

Mitch Herckis
Director of Government Affairs
National Association of State Chief Information Officers (NASCIO)
444 North Capitol Street NW, Suite 642, Washington, DC 20001
202.624.8477; mherckis@NASCIO.org