NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

Michael Gronstal
Senate Majority Leader
Iowa
President, NCSL

Raúl E. Burciaga
Director
Legislative Council Service
New Mexico
Staff Chair, NCSL

William T. Pound
Executive Director

To: Nakia Grayson, National Institute of Standards & Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

From: National Conference of State Legislatures

Date: September 09, 2016

Subject: RFI on Current and Future States of Cybersecurity in the Digital Economy

Executive Summary

States are diverse and active participants in the security and resiliency of their state digital networks. It is crucial for legislators to balance the risk management and budget aspects of cybersecurity with the technological expertise required of the state implementers. Legislators are becoming more aware of the threats posed to their digital infrastructure and the evolving sophistication of criminal actors, which will help inform appropriations to protect those systems. However, states are diverse and need flexibility to implement strategies that address the unique challenges of their state. Critical to that process is the need to discuss different approaches and learn from experts that work in and out of state government.

In this request for information to the Commission on Enhancing National Cybersecurity, NCSL is responding to the topic of State government cybersecurity as it relates to: Critical Infrastructure Cybersecurity; Cybersecurity Insurance; Cybersecurity Workforce; Federal Governance; Identity and Access Management; and Public Awareness and Education. Cyber-attacks are evolving and will continue to present tangible challenges for state governments.

A universal challenge for states is how to keep up with the pace of change with a limited workforce and financial resources. States cannot guarantee requested funding levels from chief security officer's appropriation requests due to competing priorities. Critical infrastructure vulnerabilities pose public safety and homeland security concerns, and states are using emergency preparedness and response plans as a means for addressing this issue. Cyber insurance is too undeveloped to bridge the gap between the benefits of using insurance as a robust risk analysis tool against the potential high premium costs and low coverage amounts. As with the federal government, hiring a talented cybersecurity workforce is challenging, with some states experiencing high levels of vacant cybersecurity positions. Basic cyber awareness and training for state workers and contractors is also a high priority for legislators. They want to

understand how policy solutions can lower the risk of inside actors opening their networks up to attacks.

States are responding with solutions to better address the challenges facing their digital ecosystems. Accepting cybersecurity as part of its regular oversight and business culture is a valuable step for legislators and federal agencies. Cybersecurity policy is a risk management priority that will require continuous monitoring and updating to evolve with the ever-changing threat environment. Elevating legislative branch awareness about the necessity of having a resilient digital network and the cost of responding to preventable breaches are proactive ways to position funds towards addressing this issue continuously, thoughtfully and systematically. Legislators must be willing to talk to their executive branch counter parts including their Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) outside of public hearings, where agency leadership can share sensitive information on network vulnerabilities. State-Federal and public-private partnerships are also crucial, where outsourcing resources can help support data analytics and information sharing.

State Government Cybersecurity

States are diverse, complex and active participants in the security and resiliency of their state digital networks. As legislators become more aware of the threats posed to their digital infrastructure and the continually evolving sophistication of criminal actors, there is a move to increase resources available to protect those systems. Cyber security is a risk management issue and it will require both short-term solutions and long-term policy and financial resources allocated towards securing state networks. In order to combat this increasing threat, it is essential that all levels of government work together to develop appropriate and flexible solutions.

The National Conference of State Legislatures created its Executive Task Force on Cybersecurity in May of 2016 to address the challenges and discuss innovative solutions in the digital realm. By bringing together private sector experts, our colleagues at NASCIO, NGA and other public sector partners, the Task Force will explore how legislators can facilitate the work of their executive counterparts and support greater economic, educational and security growth. The purpose of the Task Force is to inform policy leaders on cybersecurity challenges and solutions by tapping into the resource of public partners and private sector leaders, in recognition of the fact that the private sector is a sophisticated actor in this space.

States are taking the initiative to introduce legislation in critical cyber policy areas. Legislators actively combat identity theft, security breaches, spyware, phishing and computer crime and have looked at internal data disposal policies. Given the ubiquity of cybersecurity, from financial sectors to law enforcement and energy sectors, state governments are in the best position to offer specialized, nuanced and targeted solutions tailored to their state needs and top threats.
For example, Washington enacted a comprehensive cybercrime law that addresses cyber-crime in that state, including computer trespass, electronic data service interference and spoofing. Wyoming requires agencies to adopt policies for data collection, access, security and use. The law directs the state chief information officer to develop guidelines for local governments for data collection, access, and security while also providing the necessary definitions.

In March of 2016, Florida enacted a law that broadens the scope of duties for their chief information security officer and creates computer security incident response teams. Florida enumerates training programs, risk assessments and notification requirements after data breaches. Georgia created a data security and privacy committee under the Senate to conduct studies to address the "conditions, needs, issues, and problems that may exist with existing security procedures, practices, and systems in place across the state and local government or related thereto and to recommend any action or legislation which the committee deems necessary or appropriate."

Last year alone 24 states considered cybersecurity bills, with at least nine (9) enacting legislation. The content of the bills range from authorizing studies, creating commissions, or even creating tax incentives for businesses. Additionally, executive and legislative branches are working together, promising an approach that acknowledges both branches as critical stakeholders in responding to cyber threats.

Federal Governance

NCSL appreciates the opportunity to respond to this Request for Information (RFI), and offers a critical perspective on the role of state government in the digital environment. The federal government should avoid preemption of state activity in this space. Due to the diversity of state structures and complexity of the risks involved, states need to be empowered to approach cybersecurity as individualized solutions that address the unique threats of their state. The federal government cannot operate in a vacuum, and assessing state laws and state executive pronouncements should be considered before federal action. NCSL urges Congress and the Obama Administration to:

- View state and local governments as critical stakeholders;
- Avoid unfunded federal mandates and preemptions on state and local partners;
- Collaborate with state and local governments to invest in securing state networks;
- Maintain the civil liberties and privacy of all citizens while sustaining the safety and stability of the internet and electronic communications; and
- Identify and share actionable information based on specific threats to allow states to respond effectively to known threats. Facilitate the communication of these threats from federal to state and state to state; and
- Provide timely and effective information sharing with the state as an essential tool for collaboration on emerging threats.

Federal resources can support state governments by providing technical experts with standardized definitions and straightforward language to effectively communicate with their policy counterparts.

Critical Infrastructure Cybersecurity

Managing critical systems online has created great opportunities for efficiency, increased accuracy and greater access of supply to the public. The complexity of managing the energy and critical resource supply is increasing, from operating the smart grid to managing financial resources and accessing medical information remotely, all of which increases bad actors' entry points into the system and therefore the systems' vulnerability to such attacks. Bad actors capabilities are also increasing, in both the number of actors engaged in cyber-attacks as well as the sophistication of those attacks. States are working to identify their cyber response plans and incident response capabilities in the event of a successful attack.

For example, California is considering legislation that would require their Office of Emergency Services to develop and disseminate an incident response plan in the event of a cyber-attack on their critical infrastructure system. New York is also considering legislation that would form a State Cyber Security Advisory board within their Homeland Security and Emergency Services Division. One of the outlined goals of the board would be to advise the governor and legislature on recommendations to protect critical infrastructure and information systems.

Cybersecurity Insurance

NCSL is cautious about the use of cybersecurity insurance as a way of buying down risk on state networks. Some states have limited cybersecurity insurance, such as Minnesota. Alabama is considering IT procurement legislation that would give preference to vendors that carry cyber insurance. Indiana, in January 2016, adopted legislation that requests a committee report on the use of commercial liability insurance. Insurance could be helpful in assisting states assess their assets and vulnerabilities in their state systems. However, cyber insurance is a new product with little actuarial data, making the costs on state budgets inconsistent and potentially expensive.

Cybersecurity Workforce

States are unable to meet the current demand for information security professionals, and this problem will only expand within the next three years. By investing in long-term solutions such as early age education and diversifying the demographics of potential cyber professionals, lawmakers hope to see more talented and diverse workforce eventually enter state government. Short-term solutions focus on the formation of public-private partnerships and outsourcing products and services, which lawmakers hope will boost the economy and increase stable attractive public sector jobs.

Lawmakers' role in enhancing cybersecurity for the private sector is an issue states consider addressing. Some solutions include scholarship for service, internship programs, tapping into the veteran workforce as well as the underemployed, and promising professionals a secure, yet challenging and outlined career path. One example of this is in Florida, where in 2014 legislation passed that created the Florida Center for Cybersecurity at the University of South Florida. The center plans to expand cybersecurity degree programs statewide and create partnerships among businesses, higher education communities and industry where cybersecurity is a major player in finance, health care, utilities and the military.

Identity and Access Management

At least eight (8) states have statutorily created executive agency Chief Information Security Officer (CISO) positions – Arizona, Colorado, Florida, Kentucky, Massachusetts, Ohio, Utah and Washington. Additional states have CISO positions created through executive order. Centralized agency structures that allow CISOs to manage state-wide information security and privacy issues across all agencies have had success in managing identity verification processes and access management. One approach does not fit all states, however, and larger states with decentralized agency structures are often left with each agency managing their IT infrastructure separately. Communication between agencies with IT management and security responsibilities is essential. The National Association of State Chief Information Officers (NASCIO) is comprised of state chief information officers, and NCSL is committed to working with them in developing tailored policy on this issue.

At least a dozen state legislatures have worked to limit access to secure data and impose specific security requirements for state agencies. For example, Utah passed a law in March of this year,

which penalizes individuals who violate unauthorized access to information technology rules including unauthorized access to a protected computer or causes the transmission of a program, code or command to a protected computer or traffics in a technological access barrier that could be used to access the protected computer. The Utah law is similar to a Florida law, the first of its kind, enacted in 2015. The law allows prosecution of former employees or others who may have at one time been authorized to access a computer, but later that permission was revoked. Other states require written security plans and policies, regular security assessments or requires agencies to adopt standards and reasonable security practices.

Internet of Things

There is continuous education for legislators on the future of *the internet of things*, and NCSL will continue to explore the impacts of digital connection to everyday items has for citizens and what role legislators play in this space.

Public Awareness and Education

NCSL's first priority is developing the awareness and understanding of legislators and staff on cyber issues, as to empower them to secure their state systems. Key to this process will be the development of secure policy and dissemination of information to others that utilize state systems such as contractors that access state data, vendors that supply products and services that store state information and citizens that access state resources online.

To get in touch with the NCSL Executive Committee on Cybersecurity team, please contact Susan Frederick, Danielle Jarchow and Danielle Dean