NASCIO
Representing Chief Information
Officers of the States

WRITTEN TESTIMONY OF

MR. ERIC SWEDEN
PROGRAM DIRECTOR
NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

WAYS AND MEANS COMMITTEE
KANSAS STATE SENATE

Senate Bill 342

FEBRUARY 1, 2018

Madam Chair McGinn, Vice Chair Billinger, Ranking Member Kelly and members of the Ways and Means Committee:

Thank you for the opportunity to testify before you today on issues related to Senate Bill 342 (Enacting the Kansas cybersecurity act). My name is Eric Sweden and I serve as the Program Director of the National Association of State Chief Information Officers or NASCIO, which is headquartered in Lexington, Kentucky.

My appearance before Committee today is in the capacity of an interested party to present information and insight about the general organizational models for state information technology functions and the role of state chief information officers (CIOs). My remarks will offer a generalized view of the states and cover the CIO roles, responsibilities, trends, and challenges. As background, NASCIO is a non-profit organization that represents state chief information officers and information technology executives and managers from the 50 states, U.S. territories, and the District of Columbia. The mission of the NASCIO is "to foster government excellence through quality business practices, information management, and technology policy." A key goal of NASCIO is to be the premier network and resource for state CIOs. To that end, we regularly publish surveys and studies on current business trends within the state CIO community which I plan to reference today.

We understand that you are currently considering a bill, Senate Bill 342. While we will not comment on the merits of this specific bill before you, we would like to share with you the national perspective on the issues addressed in Senate Bill 342.

Cybersecurity

As a state CIO priority, cybersecurity has captured the number one position on the NASCIO Top Ten list for the past five years. Cybersecurity protection, response, resiliency, and recovery dominate the agendas of state CIOs. Because of the massive amounts of personal information held in trust by state government agencies, states are attractive targets for hackers, cyber criminals, and foreign entities.

In the past few years, states have experienced a significant increase in cybersecurity threats. Attacks from activist groups or "hacktivists" with a political agenda have also become more prevalent. In fact, because of the increasing severity, volume, and sophistication of cyber threats, states are becoming more vulnerable to attacks. State governments are facing persistent challenges in cybersecurity risk reduction because of several factors, but most importantly these key issues: lack of sufficient funding (80%), inadequate availability of cybersecurity professionals (51%), lack of documented processes (45%), increasing sophistication of threats (45%), and lack of visibility and influence within the enterprise (33%). (See, 2016 NASCIO-Deloitte Cybersecurity Study, October 2016).

With these challenges in mind, NASCIO recommends states organize for success with a clear and authoritative governance structure that includes all appropriate stakeholders and not just technology leaders. Cybersecurity presents *business* risks to the states and must be understood in this context. States are attractive targets – specifically citizen data. Attacks have become much more aggressive and originate from organized crime that is highly budgeted and highly sophisticated. Cyber attacks are also launched from nation states and non-nation state organizations that specifically want to disrupt life in these United States.
With this in mind, NASCIO and the US Department of Justice, Bureau of Justice Assistance, collaborated on the publishing of NASCIO's Cyber Disruption Response Planning Guide. This guide presents principles, checklists and cross functional process descriptions to assist states and territories in preparing for the inevitable – a cyber disruption.

From our NASCIO 2016 Cybersecurity Survey, we present that executive awareness is growing. However, compared to state Chief Information Security Officers, state officials still overestimate how well they think states can handle security threats.

Security must become a normal operating discipline for state government. A significant contributor toward that end is the development of formal strategy. Top challenges for effective cybersecurity strategy implementation are funding and finding talent. States are moving more and more to enterprise-wide cybersecurity strategies, funding, and capability management.

Cybersecurity should be addressed as a significant business risk to state government and funded at a level commensurate with the risk. Based on NASCIO data, the percentage of information technology spending on security is much lower than recommended benchmarks for comparable organizations. According to SANS, those in the financial services sector spend roughly 10% to 12% percent of their IT budget on security; the health care sector spends between 4% and 6%; government spends between 4% and 6% in 2015 and 7% to 9% in 2016 (SANS, IT Security Spending Trends, 2015). In FY2016, the federal government spent 16 percent of the total federal IT budget on cybersecurity and still experienced very public and expensive cyber incidents that not only produced tangible harm to the affected victims but also damaged citizen trust in government (Christian Science Monitor, Despite billions spent, US Federal agencies struggle with cybersecurity, June 10, 2015).

There is no magic number or percentage that will always and sufficiently secure state governments against cybersecurity risk. Increased spending alone will not be enough to address evolving threats to the state's cyber environment. It is impossible to eliminate cybersecurity risk but state CIOs and CISOs can enhance the cybersecurity posture of their state with effective governance, leadership, and organizational structures.

There are patterns of success that we've seen from across the states and territories: enterprise leadership and governance; creating a cybersecurity culture; communicating the risks; statewide cybersecurity framework and controls; and investment in security technologies such as advanced cyber analytics. Enterprise-wide cybersecurity initiatives can achieve economies of scale, better use of resources, and provide a broader view of threats. A unification across agencies provides the ability to see and evaluate the full portfolio of threats. Without an enterprise-wide cybersecurity initiative there are isolated threats at the agency level that the Chief Information Security Officer team do not know about and therefore they cannot truly assess the full threat landscape.

Through our various publications, priorities and webinars we can generalize these key questions for state leaders:

- Does your state government support a "culture of information security" with a governance structure of state leadership and all key stakeholders?
- Has your state conducted a risk assessment? Is data classified by risk? Critical infrastructure reviewed? Are security metrics available?
- Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards, and compliance? Is the NIST Cybersecurity Framework a foundation?
- Has your state invested in enterprise solutions that provide continuous cyber threat detection, mitigation and vulnerability management? Has the state deployed advanced cyber threat analytics?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state's assets?
- Does your state have a cyber disruption response plan? A crisis communication plan focused on cybersecurity incidents?

Madam Chair McGinn, Vice Chair Billinger, Ranking Member Kelly and members of the committee, thank you for the opportunity to present the perspectives of NASCIO. I hope my comments have been beneficial as you consider Senate Bill 342. I would be happy to answer any questions you may have at this time.