WRITTEN TESTIMONY OF

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

GOVERNMENT, TECHNOLOGY AND SECURITY COMMITTEE
KANSAS HOUSE OF REPRESENTATIVES

FEBRUARY 15, 2017

Chairman DeGraaf, Vice Chair Lewis, Ranking Member Curtis and members of the Government, Technology and Security Committee:

Thank you for the opportunity to testify before you today on issues related to House Bills 2359 (Creating the Kansas information technology enterprise agency) and 2331 (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 two bills, specifically, House Bills 2359 and 2331. While we will not comment on the merits of the specific bills before you, we would like to share with you the national perspective on the issues addressed in HB 2359 and HB 2331.

The Importance of IT and the Changing Role of the State CIO

In decades past, IT was viewed as one of many tools to support the mission of state executive branch agencies. Today, IT is not just a tool, IT is a part of the "fabric" of state government which enables innovative service delivery and provides the platform by which citizens interact with government. The changing and increasing value of IT also has implications for the state CIO whose responsibilities in the past were primarily to manage and provide infrastructure services and support. Now, the state CIO is viewed as a **change leader** who leads and facilitates government organizational transformation efforts in support of and in coordination with the agenda of the governor and state policy goals.

State CIOs now have a multifaceted, enterprise role which includes many of the following responsibilities:

- Enterprise strategic IT planning
- Enterprise policy and directives
- Investment management
- State IT governance bodies
- IT budget review and approval
- Enterprise Architecture and Standards
- Provision of the state IT infrastructure and shared application services
- Communications and networks
- Project Management oversight
- Disaster recovery and business continuity
- Procurement and contract management
- Service level management
- Risk management, security and privacy
- Digital government and portal services
- Geographic information systems
- Homeland security
- Business process improvement

- Heath information technology
- Multi-media production
- Electronic records management
- Customer relationship management
- Cross-boundary collaboration

From the collective experience of the states and NASCIO's research, three key elements emerge to foster a successful state IT management strategy: **governance, leadership, and organization**. This starts with an enterprise perspective of IT strategy, investments, authority, and policies. From the leadership perspective, the state CIO articulates the enterprise view and harnesses the power of IT in support of the policy goals of state government. In addition to managing the core IT infrastructure for the state, an overwhelming majority of state CIOs today have enterprise responsibilities for overall IT strategy, policies, budget review, and project oversight as well as managing the agency that provides a wide array of services to state agencies.

Common State CIO Priorities, Challenges, and Forces of Change

Every year since 2007, NASCIO has produced the "Top Ten" list which identifies the top ten priorities for state CIOs. The most frequently cited top three priorities over the last ten years were: consolidation/optimization, security, cloud services, and budget and cost control. For 2017, security topped the list, followed by consolidation/optimization, and cloud services. These priorities not surprising given the strained financial environment facing state governments. State IT costs are often driven by diversity and complexity and by reducing both factors through consolidation and optimization, state CIOs are attempting to recoup savings for the state.

While the priorities for state CIOs remain largely consistent over the years, state CIOs are operating in an environment that is affected by what we call the "forces of change" – these are broad trends that impact the way state governments and specifically, state CIOs, conduct business:

- Low revenue growth in many states, state CIOs are pressured to find cost savings, drive consolidation and optimization strategies, and cloud adoption
- Continued evolution from the owner-operator business model to one that focuses on services and hybrid models of delivery
- Regarding cybersecurity as a business risk
- Growing investments in cloud services, data analytics, and mobile services
- Continuing IT workforce challenges: retirements, skills gap, recruiting, talent management, workplace innovation
- Advocating for IT procurement reform, advancing agile approaches

Additionally, state CIOs across the country face similar challenges:

- Many state CIOs shoulder much of the responsibility for statewide IT governance, but do not possess the same level of authority
- Cybersecurity is an enterprise imperative and a top priority for state CIOs
- According to 2016 NASCIO data, almost half of state CIOs expect small increases or flat IT budgets through the 2016 year

It is possible to achieve the strategic goals and priorities of the state by harnessing the power of IT. In order to do so, it is critical that state CIOs operate in an environment that facilitates cost savings by

leveraging economies of scale, maximize cybersecurity through enforceable enterprise wide policies, and manage IT assets and investments in a manner that anticipates change.

Governance: State CIO Reporting Structures and Executive Branch Agency Organization

Across the nation, there are three general ways in which state CIOs are organized: report to the governor, report to agency head, and report to a board. Twenty-five states CIOs report to the governor, twenty-three state CIOs report to an agency head and two state CIOs report to a board. Ten years ago, twenty-one state CIOs reported to the governor and were a member of the governor's cabinet and twenty-seven state CIOs reported to an executive department head. In comparison to the reporting structure of 2007, the state CIO position seems to be moving toward a cabinet-level position. However, changes in administration and executive branch reorganizations result in constant fluctuations in these models.

While the reporting structure of state CIOs is generally split between reporting to the governor or to an agency head, the organizational structure of executive branch agencies is more difficult to determine as the answer to that question usually rests somewhere between very decentralized/federated at one end of the spectrum and very centralized at the other. However, we do know that the current trend is toward greater alignment and centralization of IT management due to the need to exercise a greater degree of control over IT direction and investments while delivering more efficient IT support to increasingly complex government organizations. Today, most states are in the midst of this movement, slowly maturing and adopting the characteristics of a more centralized approach with IT consolidation and shared application delivery initiatives. A major driver of the "enterprise view" of IT are the business risks associated with security threats or cybersecurity.

There is no "one right way" to organize the state executive branch because each state will define their approach that reflects the unique culture, politics, and decision making processes of the state. However, the lack of organizational stability contributes to greater challenges in execution, project oversight, and can be a barrier to implementing new strategies.

IT Service Delivery and Funding

With a couple of exceptions, almost all state CIO organizations operate on a chargeback basis. This means that state executive branch agencies sit in a customer relationship to the state CIO who is charged with providing IT services to those agencies. In other words, the agencies are "customers" that purchase data center, network, email or voice services under a published rate or pro-rated assessment method. The chargeback funding model presents a challenge to modernizing outdated or legacy systems which are known to be insecure and expensive to maintain. In 2016, NASCIO found that 90 percent of states consider at least 20 percent of their IT systems are due for replacement or modernization, while nearly two-thirds of state CIOs viewed more than 40 percent of IT systems as legacy.

Regarding *how* state CIOs deliver IT services to executive branch customer agencies, there are several business models but the most prevalent models are shared services (74%) and managed services (63%). The "shared services" model is typically defined as one part of an organization sourcing a product or service for the benefit of multiple parts of the organization or for the entire

organization/enterprise. This model incentivizes economies of scale which in turn can produce cost savings for the state.

Traditionally, state governments had owned and operated everything from infrastructure (e.g. broadband) to desktops. Now, 2016 NASCIO data indicate that two thirds of states outsource at least some IT infrastructure operations (e.g. running broadband services), almost two-thirds of states use a managed services model (e.g. managed services provider manages and assumes responsibility for providing some defined service) for some or all IT operations, and only one-third of states own and operate all state IT assets and operations. 79 percent of states outsource at least some IT applications and services (e.g. email, GIS), a significant increase from 42 percent reported just six years earlier in 2010.

The business of state government is conducted through IT but the speed at which technology advances outpaces the ability of government to adapt. This is one explanation as to why state governments are shifting from owning and operating IT assets and resources and shifting the adaptation responsibility to a managed service provider. A quote from a state CIO respondent accurately reflects the continued trend toward a managed service model: "We don't build or develop anything, we buy things that are SaaS (software as a service) or COTS (commercial off-the-shelf) services. Our CIO serves as an IT facilitator vs. provider." (NASCIO, Grant Thornton, CompTIA, 2016 State CIO Survey: The Adaptable State CIO, September 2016).

Cybersecurity

As a state CIO priority, cybersecurity has captured the number one position on the NASCIO Top Ten list for the past four 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. 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 7-9 percent of their IT budget on security and the health care sector spends between 4-6 percent (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.

Chairman DeGraaf, Vice Chair Lewis, Ranking Member Curtis 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 HB 2359 and HB 2331. I would be happy to answer any questions you may have at this time.