STATE OF KANSAS

EXECUTIVE BRANCH INFORMATION TECHNOLOGY
OFFICE OF INFORMATION TECHNOLOGY SERVICES
2800 SW TOPEKA BLVD., BUILDING 100
TOPEKA, KS 66611

PHONE: (785) 296-3463
FAX: (785) 296-1168
oits.info@ks.gov

GOVERNOR JEFF COLYER, M.D.
DONNA R. SHELITE, INTERIM CHIEF INFORMATION TECHNOLOGY OFFICER

To: Chairwoman McGinn & Members of the Senate Ways and Means Committee
From: Rod Blunt, Deputy Chief Information Security Officer
Date: March 9th, 2018
Re: HB 2359, Enacting the Kansas Cybersecurity Act

Thank you for the opportunity to testify **in support** of House Bill 2359.

It is my hope that my testimony provides the committee with adequate information to make an informed decision regarding the proposed legislation. My testimony will draw largely from our Cybersecurity Strategy to address the threat, our strategy to mitigate our collective risk, and how this proposed legislation anchors our effort to safeguard the information and information assets that citizens and businesses have entrusted to the State of Kansas.

The Threat

Almost daily we read about another significant data breach and the millions of citizens and businesses that fall victim to criminal activity in the aftermath and yet across the country the response has simply not equaled the threat. In Kansas, millions of intrusion attempts are faced by the state on a daily basis. Attackers continually attempt to overwhelm the State's network to disrupt services. State employees face daily challenges as cyber-criminals pose as legitimate sources to gain trust, steal passwords and download malicious software. Criminals attempt to encrypt the State's data and hold it for ransom while nation-states attempt to steal personal information and insider threats are of continual concern.

In previous testimony, metrics were provided that illustrated our collective maturity as a State across several cybersecurity categories. Those metrics identified multiple weaknesses that leave the state vulnerable to attack, and it is clear from studies across virtually all industries that cyberattacks have been rising in both frequency and scale. Multiple publicly available reports examined the world-wide and regional impacts posed by threats such as the spread of infectious disease, the collapse of nation-states, food crises and weapons of mass destruction, and identified that cyberattacks rank as the number one risk facing the United States. Terrorist attacks rank third.

The challenges we face in protecting the privacy of our citizens, the confidentiality of our information and the ability to provide critical State services are vast. In addition, the State must lead efforts toward a more cyber-secure State as a whole by helping to protect the State's critical infrastructure, prepare the State for potential cyber disruption, and promote cybersecurity best-practices.

Today when we think of cybersecurity we think almost exclusively of the sensitive data we are entrusted with; however, the threat goes far beyond the criminality of stealing sensitive data. As we calculate the impact of cyber threats, we need to extend our understanding of the threat to include things that we rely upon every day such as medical equipment, water treatment facilities, and power grids. As cyber-dependence rises, the resulting interconnectivity and interdependence can dilute the ability of organizations to sufficiently protect government and business operations. The growth of the Internet of Things (IoT), which will result in more connections between people and machines, will exponentially increase cyber-dependency, which will raise the likelihood of a cyber-attack having serious if not devastating cascading effects. By including these additional targets in our calculations, perhaps our response in managing the risk will improve.

Our Strategy

The Office of Information Technology Services (OITS) central security team has promoted a widely accepted and common strategy that is anchored in an efficient, consistent, and collaborative approach in addressing cyber threats. Though the Kansas cybersecurity strategy has been modified over the years, the basic tenets remain and the goals, objectives and action plans continue to address gaps in cybersecurity with a focus on accelerating the State's progress toward establishment of a cooperative cybersecurity capability.

The comprehensive strategy maintains a focus on a Vision and a set of Strategic Guiding Principles which ensure a well-defined, deliberate and executable strategy. The strategy focuses on basic tenets of foundational cybersecurity concepts, processes and practices to protect the State while establishing a proactive approach to reducing risk and securing the technological capability of the State. The State's continuing digital transformation is moving the State into the mainstream of modern methods used to communicate and conduct business across the State and though it is vital that cybersecurity efforts are in concert with this transformation they must not be subordinate.

While the cybersecurity strategy must identify action plans to enable the secure use of advancing technologies, the strategy must also provide a roadmap or detailed plan for ensuring the State can face the ever-growing and evolving cybersecurity threat landscape. As proposed in the legislation, the continued development of a focused and efficient cybersecurity organization, the consistent use of best-practice frameworks with measurable maturity levels and a focus on building an industry-partnered cybersecurity workforce are key components of the strategy to ensure the cyber-readiness of the State for years to come.

The ever-growing reliance on technology solutions by state agencies, boards and commissions requires that cybersecurity programs align and support the business needs of the State. Our ability to deliver advanced and innovative technology capabilities which are secure is paramount to providing the high level of services that our citizens need and deserve. An effective and appropriate balance of nimble, innovative and secure solution delivery can be realized through sound cybersecurity risk management practices, secure solution engineering and effective cybersecurity governance, all of which are critical components of the strategy and well defined in the Kansas Cybersecurity Act.

Cyber-attacks are continuous and some will be successful. This realization exemplifies the importance that an effective cybersecurity strategy must include the development of robust cyber-defense and incident response and recovery capability. Proactive and deliberate cybersecurity monitoring and aggressive 'threat hunting' is required, as traditional network perimeter security alone can no longer protect the State from today's threat environment. The strategy includes significant focus on the critical areas of cyber-defense, threat intelligence, incident response and cyber-resiliency.

A collective and enterprise-wide approach to cybersecurity is crucial to help protect the State from the impacts of cyberattacks. Historically, state agencies, boards and commissions have operated in cybersecurity silos, each with its own security policies, practices and protections. While some state agencies have maintained pace with the growing sophistication of attacks and increasing risk, most agencies lack the resources, expertise or focus to adequately protect their data and systems. The entire, interconnected network is placed at risk due to inconsistent, or sometimes, non-existent cybersecurity controls. The strategy addresses this critical issue through the establishment of a specific goal to ensure the State addresses the cybersecurity challenge through an enterprise approach.

Providing cybersecurity leadership across the State leads to a more cyber-secure State in both private and public sectors. A key component to the vision of a cyber-secure State includes a focus on public and private sector partnerships to help secure the State's critical infrastructure. The development of a comprehensive cyber disruption plan to help protect our citizens is a key deliverable of this strategy. Nurturing partnerships at all levels across government and private sector entities will provide leadership and facilitate continuous growth. Alignment with federal efforts ensures the State is contributing to the overall improvement of the

cybersecurity posture of the nation, but is also providing key visibility to funding and joint cybersecurity initiatives which can benefit the State.

Critical to the success of this strategy is a focus on executive involvement, effective communication and continual improvement that provides the State with the ability to reduce cyber-risk as the State continues to transform into a digital State with a positive impact on service delivery to citizens, businesses, and our economy.

Development of the strategic outcomes of the State Cybersecurity Strategy included an analysis of state cybersecurity and the identification of desired end-states. Cybersecurity goals, objectives and action plans were developed with a continuous eye toward desired end-state characteristics and here again the strategy and proposed legislation are aligned. These characteristics have been translated into specific strategic outcomes.

Proposed Legislation

Establishing a cornerstone from which to build an effective cybersecurity program is vital and I believe that cornerstone is legislation dedicated to cybersecurity. Through carefully crafted legislation we can clearly assign cybersecurity responsibility and more importantly accountability. In today's business environment, cybersecurity is widely and incorrectly considered a technology issue, and though much of how we interact with information is accomplished through the use technology the accountability for the associated risk remains with the business.

To address an absence of oversight, the proposed legislation would establish the position of the Chief Information Security Officer (CISO) and the position's authorities and responsibilities. The legislation would also officially recognize, under the leadership of the CISO, the Kansas Information Security Office (KISO). Though the CISO would report to the Executive Chief Information Technology Officer, and work closely with department heads and agency executives.

Under the legislation the KISO would become the focal point of a collaborative and cooperative effort that directly impacts every objective of the cybersecurity strategy. The organizational structure of the KISO would provide technical cybersecurity capabilities and information assurance services, both of which would provide executive leadership throughout the executive branch with the information necessary to more accurately make informed risk decisions.

One of the more important provisions of the proposed legislation is the assignment of agency responsibilities and accountability and the reporting requirements that frame what is necessary to construct and sustain a sound information security program. Although these critical elements are not new and exist in various security frameworks, the absence of qualified security professionals to socialize and promote them within the organizations continue to hinder program development.

Progress!

It's clear that the State has some challenges with cybersecurity, however it's important to note that there has been a significant increase in awareness of the risks cyber-attacks pose to the State and that interest has provided some much-needed attention. In June of 2017, Budget Amendment HB 2000 appropriated funds for cybersecurity enhancement. This enabled us to initiate implementation of several desperately needed measures identified in our strategic plan. We also identified crucially needed tools and services for initiation in Fiscal Year 2018 including:

- A central logging solution. In any well-constructed security program, logs detect anomalous activity both in real-time, as well as reactively during an incident-response event. Centralized logging provides two important benefits. First, it places all log records in a single location, greatly simplifying log analysis

and correlation tasks. Second, it provides a secure storage for log data; in the event a device is compromised the intruder will not be able to tamper with the logs.

- A Central User and Endpoint Behavior Analytics (UEBA) solution to identify anomalous activity, insider threats, fraud, and other criminal behavior. UEBA enables security analysts to track individual data and activities. These identity-based technologies focus on individuals first, monitoring their interactions and building baseline profiles to compare with historical behaviors and that of their peer groups.

- An Enterprise Security Information and Event Management (SIEM) solution to improve efficiencies in incident detection and response. A SIEM solution provides quicker identification, analysis and recovery from security events.

- A Web Application Firewall (WAF) solution. WAFs protect against unauthorized data exposure, theft or fraud on a website or application. A firewall blocks suspicious activity and inspects every web request for attack, ensuring that data remains secure.

- Denial of Service (DoS) protection. DoS attacks impact citizen services by overloading technology resources rendering them, and the services they provide, unusable. Preventing or mitigating DoS attacks is necessary to ensure citizen services remain available.

- Security assessments for sensitive, publicly accessible applications. While necessary, applications increase security and compliance risks such as hacking, unauthorized access and data loss. Testing the state of applications, whether developed in-house or by a third-party is critical to strengthening the overall security posture and meeting compliance requirements.

Those tasked with cybersecurity for the State are certainly grateful for these funds as the 2017 appropriation does help address dire deficiencies, but the central security office will have to absorb ongoing maintenance and support costs associated with resources acquired with that one-time appropriation. We look forward to working with the members of this Committee to perhaps translate growing concern for cybersecurity into a long-term fiscal solution.

Summary

In summary, it is my hope that the committee has found my testimony compelling in addressing how cyber legislation is needed to address cyber risks in state government. I would like to thank the Chair and members of the committee for allowing me to present this testimony, subject to your questions, this concludes my testimony.