Office of Information Technology Services
2800 SW Topeka Blvd.
Topeka, KS 66611 (785) 296-7440

Testimony of the Deputy Chief Information Security Officer
In Support of HB2506, Enacting the Kansas Cybersecurity Act
Before the Committee on Government, Technology and Security
January 31st, 2018

Mr. Chairman and members of the Committee. My name is Rod Blunt, I am the Deputy Chief Information Security Officer for the Executive Branch of the State of Kansas. Thank you for this opportunity to address the committee in support of HB2506. It is my hope to provide the committee with the information the committee needs to make a qualified decision regarding proposed legislation that is intended to reduce or mitigate significant risks to the information and information assets that citizens and businesses have entrusted to the State of Kansas.

Much of my testimony comes from the 2018 Kansas Cybersecurity Strategy. It is the same strategy provided to all members of the House to bring attention to, and hopefully continued support, in addressing cybersecurity risk, and cybersecurity legislation is vital to the success of this strategy.

## 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 illustrate the known data breaches and attacks against Kansas government, 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.

## 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 authority and more importantly responsibility. 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 responsibility 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 establish, under the leadership of the CISO, a new agency called the Kansas Information Security Office (KISO). Though the CISO would report to the Governor, the position would work closely with the executive branch Chief Information Technology Officer (CITO), 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 accurate and informed risk decisions.

One of the more important provisions of the proposed legislation is the assignment of agency responsibility 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.

As with all government services there is a cost and cybersecurity is no different. Presently, the cost of cybersecurity is a component of other service rates and must compete for portions of those charges. Complicating this further is the transformation of technology in Kansas government, and the uncertainty of those new service rates. To address these uncertainties, this legislation would provide the KISO with the authority to establish an independent cybersecurity rate. The intended rate would be based on staff count, which is by far a more consistent method. In moving these costs to an independent rate, the current cyber costs would be transferred from existing rates to the new rate essentially leaving the cost unchanged. However, it must be understood that current rate levels are not adequate to develop an efficient cybersecurity capability and an increase will be necessary. The intent is to publish a new rate in fiscal year 2019 and begins in fiscal year 2020; the initial rate will be roughly the same and then increase incrementally over three years until an adequate rate to sustain the program is reached. It is the hope that this incremental approach in addressing the cost of cybersecurity will be acceptable.

## The Strategy

For years the in 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 the 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 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 State Cybersecurity 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.

**Goal 1**, Protect State Information and Systems. Goal 1 concentrates on the foundational information security objectives of ensuring the confidentiality, integrity and availability of critical information and systems. The premise that attacks will happen and some will be successful accentuates the need to create and maintain cyber-resiliency, which is the ability to anticipate, withstand, recover and evolve from adversary attacks. This goal helps ensure that State information and systems are both resistant and resilient.

Under this goal, the State will utilize disciplined and formal processes to identify and classify the State's most critical as well as confidential information and digital assets and apply the most cost-effective security controls commensurate with those findings. Absent this important discipline, adequate protections will not be identified, placing the state at increased risk. These processes further prevent ad hoc security investments, resulting in waste and a poorly protected state. Proactive monitoring requirements for critical systems will also be identified and implemented, enabling the State to quickly focus on threats against its most crucial assets.

The objectives which support this goal further include establishing the processes and technologies to verify the validity of data and protect it from being inappropriately altered. Information and system availability will be provided based on the needs of the state and the criticality of the services provided. Significant action will also be taken to harden the State's systems to be more resistant to cyber-attacks and rapidly identify and remediate security vulnerabilities. Executable recovery plans will be established to minimize the impact to state operations should a system fail due to attack or other cyber event.

**Goal 2**, Reduce Cyber Risk. Goal 2 addresses the overall goal of information and cyber security programs which is to protect the enterprise by reducing information and cyber security risk to an acceptable level. The changing face of technology as well as the growing cyber-threat requires a proactive approach to risk identification, prioritization and remediation. In addition, the State must create a culture of cyber-risk awareness at all levels of government, from State employees to constitutional officers. Through this goal, the State will ensure decisions and investments are made based on sound risk management. The creation of a culture of cyber risk awareness further serves as a force-multiplier in keeping the State cyber-secure.

Objectives and action plans to realize this goal help establish a mature and consistent Risk Management Framework to ensure the State understands the cyber-risks to the missions, information, assets, individuals and reputation of State agencies and the state as whole. The framework will combine risk assessments, risk communication, business executive-level risk ownership and the development of risk mitigation strategies into a comprehensive program which involves all levels of State government.

Creating a culture of cyber-risk awareness is key to the achievement of this goal. While annual cybersecurity awareness training is a component of the strategy, cybersecurity awareness must be continually developed and reinforced. Social engineering prevention programs and high-value target education are important components of this strategy.

**Goal 3**, An Effective and Efficient Cybersecurity Capability. Goal 3 focuses on establishing and continually improving effective and efficient cybersecurity practices, processes and workforce capabilities to ensure the state can effectively prepare, protect, defend, respond and recover in response to today's cyber-threat environment as well as prepare for tomorrow's cybersecurity challenges.

The State provides a myriad of services to support its citizens, many of which help ensure life, health and safety. Significant resources are expended every day to deliver these services to help maintain and improve the quality of life for citizens and visitors as well as provide a robust business environment critical to the State's economy. The growing reliance on information systems and other technology requires establishing and maintaining capabilities to protect the State from the threats posed by cyber-attacks which continue to increase both in volume and sophistication.

As the State executes its digital transformation in support of business needs, the State is rapidly advancing the use of cloud, mobility and data technologies. It is critical that cybersecurity functions and processes support the business needs of the State. This "business security alignment" priority is delivered through this goal while the state develops and continually improves effective and efficient cybersecurity capabilities in the areas of security engineering, incident response and cyber-defense.

**Goal 4**, Enterprise Approach to Cybersecurity. Goal 4 will enhance the cybersecurity posture of the state through the establishment of an enterprise-wide cybersecurity program. Disparate and inconsistent cybersecurity practices across state agencies, boards and commissions which place the state at increased risk will be replaced by enterprise security policies and standards, consistent, effective and protective technologies and formal information security processes based on best-practices.

The program will be driven by enterprise information and cyber security policies, standards, procedures and guidelines. Through an enterprise approach, executive support and management commitment to cybersecurity will be clearly established. Information security standards based on industry standard cybersecurity frameworks, federal regulations and best-practices will ensure security policy implementations and operations both protect the state and ensure regulatory compliance.

The State has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the anchor for the State's cybersecurity program. Embracing this framework enables the State to better manage and reduce cybersecurity risk and more easily align with regulatory requirements. The NIST framework also establishes a common language that provides a consistent cybersecurity maturity measurement capability to more easily communicate the state of cybersecurity to organizational leadership. While flexible, the adoption of the NIST Cybersecurity Framework as part of the enterprise approach to cybersecurity provides all agencies, boards and commissions with a common and widely-accepted roadmap.

**Goal 5**, A Cyber Secure State. Goal 5 seeks to address the borderless, interconnected, and global nature of today's cyber environment by recognizing the critical need to work collectively across the state, and the nation, to help protect the sensitive information of our citizens, our state and our nation.

The State and the critical infrastructure within the State are at risk from cyber-attacks that could disrupt government operations and negatively impact our citizens. The development of the Statewide Cyber Disruption Strategy will bring together partners across both the public and private sector, the National Guard and mission-critical State agencies. The development of this strategy will establish capabilities intended to eliminate or limit cyber events and the potential negative effects of such an event.

Action plans which support this goal also focus on establishing and nurturing partnerships across the State. Through outreach and collaboration with other State and local governmental entities, best-practices can be shared to help guide those entities which lack expertise and resources while learning from more cyber-advanced organizations. Through partnerships, the State will also identify opportunities for collaboration as well as identify potential funding for cybersecurity initiatives.

Through active participation with federal partners, the State will remain on the front lines of emerging programs and initiatives, developing standards and further help drive the national strategy. Aligning with the national vision also provides the potential for acquiring funding from federal initiatives. This goal further provides the action plans to be forward-leaning in the development of security practices which will enable the secure use of emerging technologies.

## Summary

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