Office of Information Technology Services
900 SW Jackson
Topeka, KS 66612 (785) 296-3463

Testimony of the Office of Information Technology Services
IN SUPPORT OF HB 2509, STATE AGENCIES AND INFORMATION TECHNOLOGY PLANS
Before the House Vision 2020 Committee
February 3, 2016

I want to thank Chairman Campbell and members of the House Vision 2020 committee for the opportunity to speak to you today about House Bill 2509.

I am Phil Wittmer, the Chief Information Technology Officer for the Executive Branch of the State of Kansas, appointed by Governor Brownback on August 10th, 2015.

House Bill 2509 establishes a foundation in information technology leadership that will facilitate a more effective and efficient information technology service for state Executive Branch agencies and their customers. While this bill addresses a number of administrative duties and responsibilities necessary to improve information technology, the primary focus of my testimony will focus on the portion of the bill that addresses centralizing information security. Previous statutes from last session incorporate the other language detailing the new scope and scale of the Executive Branch Chief Information Technology Officer (CITO).

The proposed amendments contained in HB 2509 establish the official role, authority, responsibilities and duties of the Executive Chief Information Security Officer (CISO). The CISO reports to, and is selected / appointed by the CITO.

The reasons I support House Bill 2509 are as follows:

1) **Very real and present risks exist.**

As rapid technological developments make governments, business, and ordinary individuals increasingly dependent on electronic systems for information and communications, electronic systems become increasingly vulnerable to exploitation by malicious actors. Information systems have become a new domain for waging war and competition, with significant consequences for free trade and international relations. Ensuring the cybersecurity of citizens has thus become a crucial duty of governments, equal in importance to security in the "old", physical domains. Breaches in electronic networks that contain enormous amounts of personal and financial information have the potential to be much more destructive than physical theft.

As the Committee knows, cybersecurity is defined by rapid change. Technology is evolving at a much faster pace than ever before. Our adversaries are also changing rapidly, and are constantly developing new tools and attacks to compromise critical networks, steal data, and potentially damage our physical infrastructure. In this environment, it is essential for information security professionals to share information rapidly across organizational boundaries in the interest of collaborating on the next security solution or combating an emerging risk and the most efficient and effective way to accomplish this is to centralize the information security effort.

2) Increased diligence and rigor is needed.

Cyber attackers' primary strategic advantage is their rapidity of infiltration into information systems due to their evasion of legal boundaries. Thus, an equally rapid response is critical to network protection in the case of an information security incident. According to the National Governors Association, "several recent attacks reveal that states which fail to put in place a strong governance structure are at a distinct disadvantage." A decentralized governance structure hinders a rapid response by impeding the communication of the separate agencies, thus hampering their ability to share information regarding the incident and coordinate an effective response. The National Governors Association recommends establishing a consolidated governance structure for information security to promote efficient protection and suggests that governors grant their Chief Information Security Officers "the authority to develop and steer a coordinated governance structure that can greatly improve coordination and awareness across agencies", as well as the authority to "take actions to prevent or mitigate damage in the event of a cyber-breach."

I offer the following five areas of concern, which were previously expressed in the 2015 State of Kansas Information Security Strategic Plan. Increased and consistent rigor is needed in these areas to mitigate risk to the State:

Vulnerability and Patch Management: Information system vulnerabilities are the primary attack vector for external exploitation of protected information. As such, managing vulnerabilities on information systems is one of the most important defenses for an enterprise security function to perform. This service is performed by monitoring systems that collect information, record transactions, and provide border defenses. Operating these security technologies that have reach into systems across the State is a vitally important task to a central security function. In addition to operational necessity, the metrics these solutions provide are vital to evaluating organizational risk. That said, mitigating or patching vulnerabilities has been a recurring finding of most agencies year after year. While some vulnerabilities cannot be implemented without testing, most are routine and could be easily deployed using automated tools, however most medium and small agencies do not possess the necessary IT resources or skilled staff.

Security Architecture and Engineering: In the same manner that an enterprise information technology architecture is intended to establish a unified approach to technology implementations in the State, the establishment of common information security architecture is important to ensure that compatible security technologies are implemented in a consistent manner. Furthermore, security engineering professionals must research new technologies needed to meet expanding needs of the State. These technologies currently include:

- Identity management solutions that can be used to authenticate State personnel to the many State information systems,
- Single Sign On for Citizens to access State Resources,
- Multifactor authentication methods,
- Privileged account management and monitoring,
- Asset and user behavior analytics,

- Encryption technologies that protect data in transit and at rest.

These technologies must be integrated into the State security architecture. Security engineers must be included on technology projects across the State to determine the proper implementation of security controls, and compatibility with security architecture.

Risk Management: Building information security into any organization has as its goal to manage risks that face the organization. As such, recommendations for the managements of threats to the confidentiality, integrity, and availability of information assets should be the core mission of a centralized security activity. It's important to note that the goal of centralization in this context is to promote a governance structure that ensures security professionals report to and provide recommendations to agency leadership.

Security Operations: In large organizations, operational security, such as firewalls, intrusion prevention and log collection and review, are routinely managed and monitored by the information technology activity of the organization, however most State organizations either do not have information technology staff or their information technology staff are unqualified. By staffing a team of highly qualified security professionals, a centralized security activity would be able to meet the information security needs those agencies, as well as extend that support to local governments as security programs mature.

Compliance: There exists a multitude of requirements in various federal and state statutes, regulations, and industry mandates to which agencies must comply. In many cases like requirements exist for multiple agencies yet their levels of compliance vary widely as does their approach in reporting and meeting those requirements. History has proven that these requirements change, and likewise have the penalties for non-compliance. However, through a centralized effort and the collaboration of a qualified security team, meeting compliance would be far more effective, consistent, and efficient.

3) Centralizing Information Security is consistent with, and complementary to, other operating model initiatives currently underway in Executive Branch Information Technology (EBIT). It is also consistent with the Alvarez & Marsal Recommendation #5: Consolidate Project Management, Security, Management and "other" activities.

The absence of an effective single governing activity for information security management creates redundancies and causes the dispersal of useful information among many different agencies, preventing its effective utilization. Agencies' approaches to information security vary significantly, further preventing an organized interagency strategy. Greater interagency coordination is required to maximize the efficiency of security functions as well as the security budget.

Echoed by virtually all State Chief Information Security Officers, Renee Murphy, senior analyst of security and risk management for Forrester Research, also agrees that centralizing information technology security across departments or agencies brings several benefits. "It ensures they're purchasing with economies of scale, aligns the needs of stakeholders, and funds the security projects that reduce the greatest amount of risk," she says. "By collaborating across agencies, facilities can reduce costs through operational efficiencies."

As framed in this testimony, centralized governance for Information Security is generally the most efficient and provides the most benefits as resources can be leveraged in a cost effective manner across the organization. This model also offers sustainability in that stakeholders can be assured that the probability of an individual unit isn't likely to compromise the quality of the program. Should an incident occur, it can be handled in a uniform manner with full executive oversight.

In summary, a centralized Information Security organization yields the following operational benefits:

- Scale – Individual Agencies cannot fund sufficient resources to achieve the following goals.
- Focus – Ongoing diligence is needed in:
    - Risk Assessment – Having an ongoing picture of present vulnerabilities and their potential impacts
    - Predictive Analysis – Based on current cyber activity in our environment, we project where the next attack(s) may likely occur. Hence, we can proactively prepare and/or defend against such attack(s).
    - Compliance –The fundamental ongoing activities described in Section 2 above.
- Standardization – Of tools, methods and techniques
- Knowledge-sharing – Among Information Security professionals, which in turn drives higher levels of competency, and reduces diagnostic cycle times
- Diversity of skills and knowledge – Today's world requires many different skills to cover all of the issues present within a single agency. Covering all of these bases within any given Agency is financially infeasible.
- Efficiency – Pooling makes all of the above possible at a reasonable price point
- Mandatory, not optional – By not providing services for a fee, the CISO and staff can determine the proper "dosage" of Information Security required for any given Agency at any point in time or for any specific instance.

In conclusion, the benefits of centralizing information security present a clear benefit for the State of Kansas. I would like to thank the committee for their time and opportunity to present this testimony and I urge the committee to support HB 2509.