Kansas Information Security Office
2800 SW Topeka Blvd.
Topeka, KS 66611 (785) 296-7440

Testimony of the Chief Information Security Officer
Implementation of the Kansas Cybersecurity Act
Before the Joint Committee on Kansas Security
December 12, 2018

Mr. Chairman and members of the Committee,

My name is Rod Blunt. I am the Chief Information Security Officer for the State of Kansas Executive Branch. Thank you for this opportunity to address the committee regarding the Implementation of the Kansas Cybersecurity Act (K.S.A. 2018 Supp. 75-7236 through 75-7243).

Legislation

Adopted in the 2018 legislative session, the Kansas Cybersecurity Act (KCA) established provisions for information security requirements and additional provisions that enable agencies to maintain successful information security programs. In today's business environment, information security is widely and incorrectly considered a technology issue, and though much of how we interact with information is accomplished through the use technology, the liability and associated risk acceptance remains with the business. The KCA enforces this premise by clearly assigning responsibility and authority.

The Chief Information Security Officer and the Kansas Information Security Office

To address an absence of oversight, the KCA establishes the position of the Chief Information Security Officer (CISO) and the position's authorities and responsibilities. The legislation also establishes, under the leadership of the CISO, the Kansas Information Security Office (KISO). The KCA promotes the KISO as the focal point of a collaborative and cooperative effort to efficiently enact the provisions and intent of the KCA. The organizational structure of the KISO provides technical cybersecurity capabilities and information assurance services, both of which provide executive leadership the information necessary to make more accurate and informed risk decisions.

Implementation of the KCA provisions for the CISO and the KISO are well underway as these are already included in rated services provided to agencies today. The KISO provides three rated services: Information Assurance Services, Technical Security Services, and Infrastructure Security Services. Through an assigned Information Security Officer, Information Assurance Services provide state organizations with a dedicated resource for governance and program development. Technical Security Services provide access to a team of highly skilled cybersecurity professionals to manage all technology-based security controls and activities. Infrastructure Security Services differ from Assurance and Technology Security Services in that this service provides information security controls and resources consumed by all that connect to the state data network. It is important to note the distinction in services to illustrate that though the KISO provides these services, they come at a cost and agencies that choose to participate may need to adjust their budgets to meet the provisions of the KCA.

Of note regarding the KISO provisions, I would like to mention a few solutions already available. First is cybersecurity awareness training. This solution was acquired in December of 2017 and first introduced in

January 2018 with a phishing campaign to establish a baseline. Since then, the KISO continues to enroll more agencies with the number of employees in the system being now more than thirteen thousand and growing. Another solution available to all connected to the state data network is a vulnerability scanning solution. This solution has been available since April of 2018 at no additional cost to agencies. This is particularly important because it identifies technical vulnerabilities, a key variable in effectively evaluating risk. A final service available is an intelligent central logging solution. Collecting and storing logs is vital for many technical reasons, but most importantly establishes a forensic capability that only an intelligent logging solution can provide and like the vulnerability scanner, this solution is also provided at no additional cost.

Of the provisions establishing the KISO, there is one provision that will need additional clarity (75-7239(c)(15)); paragraph fifteen requires the KISO to provide an annual status report regarding executive branch cybersecurity programs to select legislative committees, but this is problematic for two reasons. First, few agencies subscribe to the services provided by the KISO, nor are they required to, and second, agencies are only required to submit assessment reports to the KISO every other year. Since agencies are required to provide security assessment reports to the KISO in October of even numbered years, I would recommend changing the reporting cadence in this provision to odd numbered years. This would ensure committees receive the most up-to-date data.

Agencies

The more important provisions of the KCA are those addressing agency responsibility and the reporting requirements 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. To address this gap, the KCA requires each agency to appoint a designated information security officer to administer the agency's information security program. Though not required, the KISO will begin contacting all agencies to request contact information of their appointed Information Security Officers to establish a communication channel through which the state can collectively improve security programs.

Implementation of the provisions in the agency section of the KCA are solely the responsibility of the agency; however, not all agencies have the financial resources to immediately meet these requirements. To address this gap, the KISO has developed guides and templates that are published on the KISO website (kiso.ks.gov). Though not a substitute for qualified information security professionals, these resources will both help meet agency provisions of the KCA and to help identify potential gaps that would otherwise go unnoticed.

Of special mention in this section is the training requirement. To ensure agency executives meet their leadership training requirement, the KISO has developed a special curriculum for leaders in the learning management system previously mentioned; agencies only need request enrollment. Further, because executive sponsorship is so vital to this cause, the KISO will be sponsoring an annual seminar for executives to promote awareness and share ideas.

Summary

Though the KCA is comprised of other provisions, I believe those provided in my testimony are most relevant to implementation. 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.