Kansas
Office of the Governor
Office of Information Technology Services

Office of Information Technology Services
900 SW Jackson St, Suite 804-N
Topeka, KS 66612

Phone: (785) 296-3463
Fax: (785) 296-1168
Email: oits.info@ks.gov

Phil Wittmer
Chief Information Technology Officer

Sam Brownback, Governor

To: Chairman Pete DeGraaf & Members of the Govt, Technology & Security Committee
Date: February 15, 2017
From: Joe Acosta, CISO
Re: HB2331 CyberSecurity or Information Security

Thank you for giving me the opportunity to speak before your committee as a **Proponent** regarding a very important piece of legislation. In an effort to easily identify specific sections of this testimony, I have numbered the paragraphs below.

1. House Bill 2331 pertains to information security, also known as cybersecurity which protects information systems from unauthorized access and/or malicious attacks. There are three pillars to cybersecurity:
   1. Availability – giving authorized individuals access to data
   2. Confidentiality – safeguarding from unauthorized access
   3. Integrity – ensuring data is accurate

2. By all measures, including investigations conducted by legislative oversight, the current state of cybersecurity in Kansas is inadequate. In December 2016, the Legislative Post-Audit Committee released a full report showing critical vulnerabilities at every level in Kansas.
   These include:
   * Inadequate structure and funding
   * Leadership and staffing gaps
   * Critical skills gaps*
   * Inconsistent or inexistent vulnerability management*
   * Inconsistent system patching*
   * Lack of centralized reporting or analysis
   * Inconsistent approach to securing software and systems
   * Lack of centralized incident tracking system*
   * Lack of Information Assurance Education training and continuing education*
   * No use of multi-factor authentication
   *Status: CRITICAL

3. Of the 100 State of Kansas agencies surveyed in a 2016 Legislative Post-Audit analysis, 75 maintain some form of confidential or sensitive information about the residents of Kansas and beyond. This includes 18 agencies that store credit card information. If any of these databases are exposed, it is projected to cost the State approximately $200 per record in fees and monitoring. As an example, if you multiply 50,000 records by $200 each it would cost Kansas taxpayers $10 million.

5. There have been several high-profile cases in recent years where government entities were hacked and confidential citizen data was exploited by hackers. Here are just three examples:
   * The U.S. Office of Personnel Management (OPM) was hacked in 2013-2014 and it's estimated more than 21 million employee records (including social security numbers and fingerprints) were exposed.
   * In 2016, hackers exposed vulnerabilities in the Illinois Board of Elections, compromising up to 200,000 personal voter records. Several states, including Kansas, reported evidence of attempts from unauthorized systems to penetrate election databases.
   * Millions of South Carolina Department of Revenue accounts were breached, costing the state more than $100 million.

6. Information Technology (IT) in general is currently decentralized within each State Agency, which leads in large part to an inability for the State of Kansas to identify vulnerabilities, monitor systems and avoid attacks. The current state of many of Kansas' IT systems render the State out of compliance with regulations and laws such as those for Personally Identifiable Information (PII) and the Health Insurance Portability and Accountability Act (HIPAA).

7. Across all Kansas agencies, we are budgeting only 1% for cybersecurity. Industry experts agree security should make up 10% of an organizations IT budget. A fully-funded, centralized Kansas Information Security Office (KISO) provides authorities, enterprise-wide risk management, a skilled cybersecurity workforce serving all agencies, and training and accountability for all agencies.

8. We propose to improve cybersecurity in Kansas by doing the following:
   * Increased monitoring and analysis
   * Vulnerability remediation
   * Centralized training
   * Improve compliance
   * No fees to the Agencies
   * Security Software
   * Security Hardware
   * Additional staff
   * Outsourcing and Third-Party Services

9. This approach will enable the KISO to identify, monitor and deliver service across function-specific security layers and across all Executive Branch agencies. The KISO and its goals can be achieved through passage of the Kansas Cybersecurity Act.

10. In addition to the aforementioned efforts, this new legislation will allow the KISO to:
    * Mitigate vulnerabilities and risk across all Executive Branch agencies.
    * Deliver critically needed standardization and accountability measures.
    * Recruit, train and retain the staff needed to rapidly respond to cyber threats.
    * Provide stable funding for the critical business need of cybersecurity in Kansas.
    * Become compliant with federal and state regulations.
    * Provide training to all State employees (not just IT people).
    * Most importantly, build trust with Kansas citizens, businesses and State employees when they know Kansas is doing everything we can to protect them and their personal data.

11. The Cybersecurity Act applies to Executive Branch agencies excluding elected offices and Regents universities. While the KISO will be centralized in the Kansas Information Technology Enterprise (KITE) office, team members will collaborate directly with individuals and teams in Cabinet and Non-Cabinet Agencies to assist in monitoring, improving and replacing systems as needed. Agencies will continue to require employees who are expert in agency-specific systems (ex: SHARP, SMART, KEES). The KISO will work with these employees to ensure the highest cybersecurity standards are being met. The KISO is also responsible for the critical task of increasing cybersecurity awareness and education for all State employees and contractors, not just those in IT roles.

12. In an effort to provide sustainable solutions to the issue of staff shortages in Kansas' government, as well as in public and private sectors, The Kansas Cybersecurity Act includes a fund to provide cooperative employment/internship experiences to students from Kansas Regents Universities in partnership with the KISO. When fully funded and implemented, this will provide a pipeline of trained cybersecurity professionals to the State of Kansas and other companies and organizations.

13. We believe the Kansas Cybersecurity Act is an aggressive, comprehensive approach to protect Kansas citizen's information. We apprecitate your continued interest and support of HB2331.

Thank you for your consideration and I stand to answer any questions you may have.