

SESSION OF 2018

**SUPPLEMENTAL NOTE ON SUBSTITUTE FOR HOUSE
BILL NO. 2359**

As Recommended by House Committee on
Government, Technology and Security

Brief*

Sub. for HB 2359 would create the Kansas Cybersecurity Act (Act).

Definitions

The bill would define various terms used throughout the Act.

Chief Information Security Officer (CISO)

The bill would establish the position of Executive Branch Chief Information Security Officer (CISO). The CISO would be an unclassified employee appointed by the Governor.

Duties of the CISO

Duties of the CISO would include the following:

- Report to the Executive Branch Chief Information Technology Officer (CITO);
- Serve as the State's CISO;
- Serve as the Executive Branch chief cybersecurity strategist and authority on policies, compliance,

*Supplemental notes are prepared by the Legislative Research Department and do not express legislative intent. The supplemental note and fiscal note for this bill may be accessed on the Internet at <http://www.kslegislature.org>

procedures, guidance, and technologies impacting Executive Branch cybersecurity programs;

- Ensure resources assigned or provided to Executive Branch agencies are in compliance with applicable laws, rules, and regulations;
- Coordinate cybersecurity efforts among Executive Branch agencies;
- Provide guidance to Executive Branch agencies when compromise of personal information or computer resources has occurred or is likely to occur as the result of an identified high-risk vulnerability or threat; and
- Perform such other functions and duties as provided by law and as directed by the Executive Branch CITO.

Kansas Information Security Office (KISO)

The bill would establish the Kansas Information Security Office (KISO) to effect the provisions of the Act. For budgeting purposes, KISO would be a separate agency from the Department of Administration.

Under the direction of the CISO, the KISO would perform the following functions:

- Administer the Act;
- Assist the Executive Branch in developing, implementing, and monitoring strategic and comprehensive information security (IS) risk-management programs;
- Facilitate Executive Branch IS governance, including the consistent application of IS programs, plans, and procedures;

- Create and manage a unified and flexible framework to integrate and normalize requirements resulting from state and federal laws, rules, and regulations using standards adopted by the Information Technology Executive Council (ITEC);
- Facilitate a metrics, logging, and reporting framework to measure the efficiency and effectiveness of the state IS programs;
- Provide the Executive Branch with strategic risk guidance for Information Technology (IT) projects, including the evaluation and recommendation of technical controls;
- Assist in the development of Executive Branch agency cybersecurity programs that are in compliance with relevant laws, rules, regulations, and standards adopted by ITEC;
- Coordinate the use of external resources involved in IS programs, including, but not limited to, interviewing and negotiating contracts and fees;
- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;
- Assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;
- Assist Executive Branch agencies to create a framework for roles and responsibilities relating to information ownership, classification, accountability, and protection;
- Ensure a cybersecurity training program is provided to Executive Branch agencies;
- Provide cybersecurity threat briefings to ITEC;

- Provide an annual status report of Executive Branch cybersecurity programs to the Joint Committee on Information Technology and the House Committee on Government, Technology and Security; and
- Perform such other functions and duties as provided by law and as directed by the CISO.

Duties of Executive Branch Agency Heads

The Act would direct Executive Branch agency heads to do the following:

- Be solely responsible for security of all data and IT resources under such agency's purview, irrespective of the location of the data or resources (locations of data may include agency sites, agency real property, infrastructure in state data centers, third-party locations, and in transit between locations);
- Ensure an agency-wide IS program is in place;
- Designate an IS officer to administer the agency's IS program that reports directly to executive leadership;
- Participate in CISO-sponsored statewide cybersecurity program initiatives and services;
- Implement policies and standards to ensure all the agency's data and IT resources are maintained in compliance with applicable state and federal laws, rules, and regulations;
- Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data and IT resources;

- Include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and IT systems and services;
- Submit a cybersecurity assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to which of the agency's systems and devices specified in the Act are vulnerable to unauthorized access or harm and the extent to which electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use;
- Ensure the agency conducts annual internal assessments of its security programs. Such assessment results would be confidential and would not be subject to discovery or release to any person or agency outside of the KISO or CISO until July 1, 2023, unless the provision is reviewed and reenacted by the Legislature prior to that date;
- Prepare a summary of the cybersecurity assessment report, which would exclude information that might put data or information resources of the agency or its contractors at risks, to be made available to the public upon request;
- Participate in annual agency leadership training, which serves to ensure understanding of:
 - Information and information systems that support the operations and assets of the agency;
 - Potential impact of common types of cyberattacks and data breaches on the entity's operations and assets, and how such attacks could impact the operations and assets of other governmental entities on the state network;

- How cyberattacks and data breaches occur;
- Steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and
- Annual reporting requirements of the executive director or agency head; and
- Ensure, if an agency owns, licenses, or maintains computerized data that includes personal information, confidential information, or information that is regulated by law regarding its disclosure, it shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information, comply with the notification requirements as set by statute and federal law and rules and regulations to the same extent as a person who conducts business in the state of Kansas. The entity head would be required to notify the CISO and the Secretary of State (only if the breach involves election data) no later than 48 hours after the discovery of the breach or unauthorized exposure.

Protection of Confidential and Personal Information

The bill would allow an executive director or agency head, with input from the CISO, to require employees or contractors whose duties include collection, maintenance, or access to personal information to be fingerprinted and to submit to a state and national criminal history record check at least every five years. The bill would allow the information obtained from the background check to be used for purposes of verifying the person in question's identity and fitness to work in a position with access to personal information. Local and state law enforcement would assist with fingerprinting and background checks pursuant to the Act, and would be allowed to charge a fee as reimbursement for expenses incurred.

Any information collected pursuant to the Act (including system information logs, vulnerability reports, risk assessment reports, system security plans, detailed system design plans, network or system diagrams, and audit reports) would be considered confidential by the Executive Branch agency and KISO unless all information has been redacted which would specifically identify a target, vulnerability, or weakness that would place the organization at risk. The provisions of this section would expire on July 1, 2023, unless reviewed and reenacted by the Legislature.

Cybersecurity Fees

Executive Branch agencies would be able to pay for cybersecurity services from existing budgets, grants or other revenues, or through special assessments to offset costs; any increase in fees or charges due to the Act would be used only for cybersecurity. Services or transactions with an applied cybersecurity cost recovery fee could indicate the portion of the fee dedicated to cybersecurity on all receipts and transactions records.

Background

The original bill was introduced during the 2017 Legislative Session by the House Committee on Government, Technology and Security at the request of the Office of Information Technology Services (OITS). During the 2017 Legislative Session, the House Committee removed the contents of HB 2359, relating to the creation of the Kansas Information Technology Enterprise, and inserted those contents into Sub. for HB 2331.

The 2018 House Committee created a substitute bill for HB 2359 by incorporating proposed language suggested by OITS, based on language included in 2018 Sub. for HB 2560.

In the House Committee hearing on 2018 Sub. for HB 2560, representatives of OITS, the Department of Homeland Security, and the National Association of State Chief Information Officers testified in support of the bill. The representative of OITS stated the bill would codify in statute KISO and the position of CISO which were created by Executive Order. Representatives of the the Kansas Board of Healing Arts, the Kansas Board of Nursing, the Kansas Public Employees Retirement System, and the Kansas State Board of Pharmacy testified as neutral conferees. No opponent testimony was provided.

No fiscal note was available when the House Committee recommended the substitute bill be passed.