SESSION OF 2018

CONFERENCE COMMITTEE REPORT BRIEF
HOUSE SUBSTITUTE FOR SENATE BILL NO. 56

As Agreed to April 4, 2018

Brief*

House Sub. for SB 56 would create the Kansas Cybersecurity Act (Act) and would amend the membership and the frequency of required meetings for the Information Technology Executive Council (ITEC).

Definitions

The bill would define various terms used throughout the Act, including "cybersecurity," which would mean "the body of information technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access." The definition of "Executive Branch agency" would not include elected office agencies, the Kansas Public Employees Retirement System (KPERS), regents' institutions, the Kansas Board of Regents (KBOR), or the Adjutant General's Department (TAG).

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.

---

*Conference committee report briefs are prepared by the Legislative Research Department and do not express legislative intent. No summary is prepared when the report is an agreement to disagree. Conference committee report briefs may be accessed on the Internet at http://www.kslegislature.org/klrd

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, procedures, guidance, and technologies impacting Executive Branch cybersecurity programs;
- Ensure Kansas Information Security Office 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) within the Office of Information Technology Services (OITS) to effect the provisions of the Act. For budgeting purposes, the 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 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 at no cost;

- 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 who 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 risk and submit such report to the House Committee on Government, Technology and Security, or its successor committee, and the Senate Committee on Ways and Means;

- 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 that 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, from grants or other revenues, or through special assessments to offset costs. Any increase in fees or charges due to the Act, including cybersecurity fees charged by KISO, would be fixed

by rules and regulations adopted by the agency and would be used only for cybersecurity. The bill would allow services or transactions with an applied cybersecurity cost recovery fee to indicate the portion of the fee dedicated to cybersecurity on all receipts and transaction records.

Changes to ITEC

The bill would amend the membership of ITEC, as follows:

- Removing the Secretary of Administration;
- Adding language to allow each of the two cabinet agency heads to appoint a designee;
- Increasing the number of non-cabinet agency heads from one to two, and allowing each to appoint a designee;
- Removing the Director of the Budget;
- Removing the Judicial Administrator of the Kansas Supreme Court;
- Modifying the representation of KBOR from the Executive Director to the Chief Executive Officer, or the officer's designee;
- Removing the Commissioner of Education;
- Reducing the number of representatives of cities from two to one;
- Reducing the number of representatives of counties from two to one;
- Adding a representative from the private sector who has a background and knowledge in technology and cybersecurity and is not an IT or

cybersecurity vendor that does business with the State of Kansas;

- Adding one representative appointed by the Kansas Criminal Justice Information System Committee;

- Adding two members of the Senate Committee on Ways and Means, one of whom would be appointed by the President of the Senate or member's designee and the other would be appointed by the Minority Leader of the Senate or member's designee; and

- Adding two members of the House Committee on Government, Technology and Security, or its successor committee, one of whom would be appointed by the Speaker of the House of Representatives or member's designee and the other would be appointed by the Minority Leader of the House of Representatives or member's designee.

The bill would clarify that members could not appoint an individual to represent them on ITEC unless such individual is specified as a designee pursuant to the bill. The bill also would require ITEC to meet quarterly on call of the Executive Branch CITO, or as provided by continuing law.

Conference Committee Action

The Conference Committee agreed to the provisions of House Sub. for SB 56 relating to agency IT security, as amended by the Senate Committee on Ways and Means, and further agreed to amend the bill as follows:

- Added TAG to the list of entities excluded from the definition of "Executive Branch agency";

- Modified the definition of “cybersecurity”;
- Clarified KISO is a part of OITS;
- Clarified a provision related to cybersecurity training programs for Executive Branch agencies would be at no cost to the agencies;
- Removed a provision making the summary of cybersecurity assessment reports available to the public and replaced it with a requirement that Executive Branch agencies submit such summary to the House Committee on Government, Technology and Security and Senate Committee on Ways and Means; and
- Clarified a provision related to cybersecurity fees charged by KISO.

The Conference Committee also agreed to insert the provisions of Sub. for HB 2332, as amended by the Senate Committee on Ways and Means, and further agreed to insert language to add a representative of the private sector to ITEC.

Background

The House Committee on Government, Technology and Security created a substitute bill for SB 56 by removing its original contents related to filing requirements for campaign contribution reports and inserting the contents of Sub. for HB 2332 and Sub. HB 2359. [*Note:* The original contents of SB 56 were inserted into 2017 HB 2158 and became effective on July 1, 2017.] Background information for Sub. for HB 2332 and Sub. for HB 2359 is provided below.

Sub. for HB 2332 (ITEC Membership)

HB 2332 was introduced during the 2017 Legislative Session by the House Committee on Government, Technology and Security. The bill, as introduced, related to divulging contents of an electronic communication or storage in a legal proceeding. A hearing was held on the bill in March 2017, but no further action was taken by the House Committee.

On February 14, 2018, the House Committee adopted a substitute bill by removing the original contents of HB 2332 and inserting language proposed by OITS related to ITEC membership. A representative from OITS stated the changes to ITEC were being requested to increase its attendance and effectiveness.

In the Senate Committee on Ways and Means hearing, the Interim Executive Branch CITO testified in support of the bill. The CITO stated the ITEC had not met in the past three years and the changes in membership would make it easier for the ITEC to get a quorum for meetings. A representative of the Kansas Information Consortium (KIC) testified in opposition to the bill. The bill, as introduced, removed the Information Network of Kansas (INK) from the bill and the KIC representative requested that member be added back to the ITEC.

On March 22, 2018, the Senate Committee amended the bill to replace two members appointed from the Joint Committee on Information Technology to two members from the Senate Committee on Ways and Means or their designees, added back the Network Manager of INK, reduced the number of cabinet agency head members from two to one, and made the Executive Branch CITO responsible for setting the dates of the meetings. [*Note:* The Conference Committee agreed not to reduce the number of cabinet agency head members but retained all other amendments in its report.]

No fiscal note for Sub. for HB 2332 was available when the Senate Committee took action on the bill.

Sub. for HB 2359 (Agency IT Security)

The bill was introduced during the 2017 Legislative Session by the House Committee on Government, Technology and Security at the request of 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 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, KPERS, and the Kansas State Board of Pharmacy testified as neutral conferees. No opponent testimony was provided.

No fiscal note was available on Sub. for 2359 when the House Committee recommended the substitute bill be passed.

information technology; cybersecurity

ccrb_sb56_01_0000.odt