Kansas Cybersecurity Act; House Sub. for SB 56

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

Definitions

The bill defines various terms used throughout the Act, including "cybersecurity," which means "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" does not include elected office agencies, the Kansas Public Employees Retirement System, Regents institutions, the Kansas Board of Regents (KBOR), or the Adjutant General's Department.

Chief Information Security Officer (CISO)

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

Duties of the CISO

Duties of the CISO 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 establishes the Kansas Information Security Office (KISO) within the Office of Information Technology Services to effect the provisions of the Act. For budgeting purposes, the KISO is a separate agency from the Department of Administration.

Under the direction of the CISO, the KISO is to 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 directs 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 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 are confidential and are not 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 excludes 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 Kansas. The entity head is 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 allows 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 allows 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 shall assist with

fingerprinting and background checks pursuant to the Act, and are 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) is considered confidential by the Executive Branch agency and KISO unless all information has been redacted that specifically identifies a target, vulnerability, or weakness that places the organization at risk. The provisions of this section expire on July 1, 2023, unless reviewed and reenacted by the Legislature.

Cybersecurity Fees

Executive Branch agencies are 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, are to be fixed by rules and regulations adopted by the agency and used only for cybersecurity. The bill allows 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 amends the membership of ITEC, as follows:

- Removes the Secretary of Administration;
- Adds language to allow each of the two cabinet agency heads to appoint a designee;
- Increases the number of non-cabinet agency heads from one to two, and allows each to appoint a designee;
- Removes the Director of the Budget;
- Removes the Judicial Administrator of the Kansas Supreme Court;
- Modifies the representation of KBOR from the Executive Director to the Chief Executive Officer, or the Officer's designee;
- Removes the Commissioner of Education;
- Reduces the number of representatives of cities from two to one;
- Reduces the number of representatives of counties from two to one;

- Adds 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;

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

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

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

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