State Cybersecurity; House Sub. for SB 291

House Sub. for SB 291 creates and amends law concerning the administration and organization of information technology (IT) and cybersecurity services within each branch of state government.

Cybersecurity Staff Reorganization; IT Services Consolidation and Judicial Branch IT Hardware Plans; Website Domains

Cybersecurity Staff Reorganization

The bill directs that, on and after July 1, 2027, all cybersecurity services for the legislative and executive branches are to be overseen by the Chief Information Technology Officer (CITO) and the Chief Information Security Officer (CISO) within each respective branch and all cybersecurity staff within each branch of state government be directed by the CITO of that branch.

IT Services Consolidation and Judicial Branch IT Hardware and Cybersecurity Program Plans

The bill requires the Information Technology Executive Council (ITEC), in consultation with cabinet agency heads, to formulate a plan to consolidate all Executive Branch IT services under the Office of Information Technology Services (OITS).

The bill requires the Judicial Branch CITO, in consultation with the Executive Branch CITO, to estimate project costs for providing IT to judicial agencies and employees, including state- and county-funded Judicial Branch district court employees. These employees are required to use state-issued hardware. The estimate must include a plan to allow each piece of IT hardware used to access Judicial Branch applications to become part of the Kansas Wide-area Information Network (KanWIN), and estimate the cost to develop a cybersecurity program for all judicial districts that complies with the requirements of the National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0, as they exist on July 1, 2024.

The bill requires the ITEC and the Executive Branch CITO to present these plans to the House Committee on Legislative Modernization and the Senate Committee on Ways and Means before January 15, 2026.

Website Domains

The bill requires all branch or agency websites to be migrated to a ".gov" domain by February 1, 2025.

Establishing Judicial Branch and Legislative Branch CISOs; Changes to Executive CISO Responsibilities

The bill establishes CISO positions for both the judicial and legislative branches. These officers will be placed in the unclassified service under the Kansas Civil Service Act. The Judicial Branch CITO is appointed by the Judicial Administrator, subject to approval by the Chief Justice of the Kansas Supreme Court. The Legislative Branch CISO is appointed by the Legislative Coordinating Council. The responsibilities of the CISOs will include:

- Reporting to the Judicial Administrator or the Legislative Branch CITO, respectively;

- Establishing security standards and policies to safeguard the branch's IT systems and infrastructure;

- Ensuring the confidentiality, availability, and integrity of information transacted, stored, or processed within the branch's IT systems;

- Developing a centralized cybersecurity protocol for protecting and managing the branch's IT assets and infrastructure;

- Detecting and responding to security incidents consistent with information security standards and policies;

- Being responsible for the cybersecurity of all branch data and information resources and, for the Legislative Branch CITO, obtaining approval from the Revisor of Statutes prior to taking any action on any matter that involves a legal issue related to IT security;

- Collaborating with the CISOs of the other branches to respond to cybersecurity incidents;

- Ensuring that all branch employees complete cybersecurity awareness training annually and revoking an employee's access to any state-issued hardware or the state network if the employee does not complete the required training;

- Reviewing all IT contracts entered into by a person or entity within the branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure they contain standard security language; and

- Coordinating with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to conduct annual audits of branch agencies for compliance with state and federal laws, rules, regulations, and branch policies. The bill requires the CISO to make such audit requests regardless of whether CISA has the capacity to perform the requested audit.

The bill also amends statutes for the Executive Branch CISO to make the position's responsibilities more consistent with the responsibilities of the Judicial Branch and Legislative Branch CISO positions and account for the creation of the new CISO positions.

Appointment of Elected Office CISOs

The bill requires the Attorney General, Commissioner of Insurance, Secretary of State, State Treasurer, and the Director of the Kansas Bureau of Investigation each to appoint a CISO for their respective office or agency. Each CISO is responsible for establishing security standards and policies to safeguard the office or agency's IT systems and infrastructure.

Cybersecurity Programs and National Institute of Standards and Technology Cybersecurity Framework

The bill requires all CISOs, in consultation with their respective agency heads, to develop cybersecurity programs for their respective agencies that comply with the CSF, ensuring agency achievement of specific tiers by July 1, 2028, and July 1, 2030. [*Note:* The CSF contains guidelines and best practices to reduce risk of a cyberattack and improve an organization's overall security posture.]

Cybersecurity Audits and Vulnerability Assessments

The bill requires, in the event of a CISA audit failure, the appropriate CISO to report the failure to the Speaker of the House, President of the Senate, House Minority Leader, and Senate Minority Leader within 30 days, with a plan to mitigate identified security risks. Results of audits and related reports remain confidential and exempt from disclosure under the Kansas Open Records Act.

The bill also allows the CITO for each branch of government to make a request to the Adjutant General for a National Guard active duty operations group to perform vulnerability assessments of the respective branch for the purposes of enhancing branch security. The operations group is required to limit harm to the system being assessed whenever possible.

Appropriations and Compliance

Beginning on July 1, 2025, and annually thereafter, appropriations from the State General Fund (SGF) or any special revenue fund of any state agency for IT and cybersecurity expenditures must be appropriated as separate line items. These appropriations cannot be merged with other items of appropriation for the respective state agency.

Beginning on July 1, 2028, and annually thereafter, the Director of the Budget (Director), in consultation with relevant CITOs, is directed to assess each state agency's compliance with the provisions of the bill for the previous fiscal year. If found non-compliant, the Director certifies an amount equal to 5.0 percent of the appropriated and reappropriated SGF moneys and 5.0 percent of the funds credited to and available in each special revenue fund for that agency. If a special revenue fund lacks an expenditure limitation, the Director is required to establish a limitation that is 5.0 percent less than the total amount available in that fund. The bill requires a

detailed written report each year on these compliance determinations to be submitted to the Legislature prior to the regular session, outlining the amounts certified for each non-compliant state agency for the fiscal year. The Senate Committee on Ways and Means and the House Committee on Appropriations are directed to review and consider a 5.0 percent lapse and decreased expenditure limitation for non-complying agencies during budget committee hearings.

The bill appropriates $659,368 to the Judicial Branch in FY 2025.

The bill also appropriates $15.0 million SGF in FY 2026 to the Kansas Information Security Office (KISO). For the appropriation, the bill requires the Director, in consultation with the Executive Branch CITO and CISO, to determine the five-year average of each state agency's cybersecurity service cost financed with SGF and special revenue funds and lapse the certified SGF amount and transfer appropriate special revenues to a new fund created by the bill.

The bill appropriates $250,000 to the Adjutant General's Department for two full-time employees for the Intelligence Fusion Center for the purpose of monitoring state IT systems.

The bill also creates, and appropriates in FY 2025 and 2026, a no-limit Information Technology Security Fund within the State Treasury, for use by the KISO for receipt and expenditure of special revenue funds transferred from other state agencies for the purposes provided in the bill.

Information Technology Executive Council Changes

The bill modifies the composition of ITEC to make the Legislative Branch CITO, Judicial Branch CITO, and the appointees of the President of the Senate, Senate Minority Leader, Speaker of the House, and House Minority Leader non-voting members, changed from voting members. The bill also adds two IT employees, appointed by the State Board of Regents (Regents), as voting members of ITEC. The Executive Branch CITO will serve as the Chairperson of ITEC. The bill also requires ITEC to meet monthly instead of quarterly.

The bill modifies ITEC's responsibilities to make clear the polices it establishes apply only to Executive Branch agencies. The bill adds to the list of responsibilities the requirement to develop a plan to consolidate all Executive Branch IT services into OITS and report on such a plan to the Legislature.

The bill removes requirements for the Judicial Branch and Legislative Branch CITOs to monitor and determine whether their respective agencies are in compliance with ITEC policy, and instead requires them to monitor and comply with policies set by their respective branches or offices.

CITO Requirements

The bill modifies requirements of the Executive Branch, Judicial Branch, and Legislative Branch CITOs to add requirements to:

- Consult with appropriate legal counsel on matters pertaining to confidentiality of information, the Kansas Open Records Act, the Kansas Open Meetings Act, and any other legal issues related to IT;

- Ensure each agency has the necessary IT and cybersecurity staff embedded to fulfill its duties;

- Maintain all third-party data centers at locations within the United States or with companies that are based in the United States; and

- Create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged, and tagged within an inventory device.

The bill specifically prohibits IT and cybersecurity staff employed by OITS within branch agencies from disclosing confidential agency information.

The bill modifies the definition of "executive branch agency" in the Kansas Cybersecurity Act to include the Judicial Council and the Kansas Public Employees Retirement System. Additionally, the bill modifies the definitions of "business risk" and "information technology project change or overrun" to include policies or thresholds adopted by the Judicial Branch or Legislative Coordinating Council.

Agency Head Responsibilities

The bill removes certain requirements relating to an agency head's responsibility to ensure the agency's compliance with certain cybersecurity policies, but makes clear that an agency head is responsible for security of all data and IT resources under their purview, and the bill requires coordination with the respective CISO to implement security standards.

Definition Changes and Exemptions

The bill modifies the definition of "executive agency" in statutes governing IT in Chapter 75 of the *Kansas Statutes Annotated*, State Departments, Public Officers and Employees, to include the Judicial Council but not elected office agencies.

The bill also clarifies Regents institutions will be exempt from provisions relating to the delivery of cybersecurity staff reorganization, ".gov" website domain adoption, and requirements for appropriation requests and transfers.

Sunset and Re-codification

The bill sunsets all provisions of the bill, excluding those related to single-year appropriations, on July 1, 2026, and will re-codify certain statutes as they existed on June 30, 2024, where appropriate.