SESSION OF 2024

SUPPLEMENTAL NOTE ON HOUSE SUBSTITUTE FOR SENATE BILL NO. 291

As Recommended by House Committee on Legislative Modernization

Brief*

House Sub. for SB 291 would create and amend 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 (New Section 1)

Cybersecurity Staff Reorganization

On and after July 1, 2027, the bill would direct that all cybersecurity services for every branch of state government to be overseen by the Chief Information Technology Officer (CITO) and the Chief Information Security Officer (CISO) within each respective branch. Furthermore, it would require that all cybersecurity staff within each branch of state government to be directed by the CITO of that branch. The bill would exempt State Board of Regents' institutions from this reorganization.

---

*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

IT Services Consolidation and Judicial Branch IT Hardware Plans

The bill would require 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 would require the Judicial Branch CITO to estimate project costs for providing IT hardware to state and county employees in each judicial district accessing applications administered by the Judicial Branch. These employees would be required to use the state-issued hardware to access these applications. The bill would require the Judicial Branch CITO to consult with the Executive Branch CITO to develop a plan allowing each piece of IT hardware used to access Judicial Branch applications to become part of the KANWIN network before July 1, 2027.

The bill would require these plans to be presented to the House Committee on Legislative Modernization and the Senate Committee on Ways and Means before January 15, 2026.

Website Domains

The bill would also require all branch or agency websites be migrated to a ".Gov" domain by February 1, 2025.

Creation of Judicial Branch and Legislative Branch CISOs; Changes to Executive CISO Responsibilities (New Sections 2 and 3 and Section 23)

The bill would establish CISO positions for both the Judicial and Legislative branches. These officers would be placed in the unclassified service under the Kansas Civil Service Act. The Judicial Branch CITO would be appointed by the Judicial Administrator, subject to approval by the Chief

Justice of the Kansas Supreme Court. The Legislative Branch CISO would be appointed by the Legislative Coordinating Council. The responsibilities of the CISOs would 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 in order 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 contains 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 CISO would be required to make such audit requests regardless of whether CISA has the capacity to perform the requested audit.

The bill would also modify requirements in current law 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 (Sections 9–14)

The bill would require 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 would be 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 (New Sections 2–3; Sections 9, 11–14, and 23)

The bill would require all CISOs, in consultation with their respective agency heads, to develop cybersecurity programs for their respective agencies that would be in compliance with the National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0, 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 (New Sections 2 –3; Sections 9 –14, 18, and 24)

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

The bill would also allow 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 would be required to limit harm to the system being assessed whenever possible.

Appropriations and Compliance (New Sections 4–8)

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 would be allocated as separate line items. These appropriations would not 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, would assess each state agency's compliance with the provisions of the bill for the previous fiscal year. If found non-compliant, the Director would certify 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 would be required to establish a limitation that is 5.0 percent less than the total amount available in that fund. The bill would require 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 would review and consider a 5.0 percent lapse and decreased expenditure limitation for non-complying agencies during budget committee hearings.

The bill would also appropriate $15.0 million SGF in FY 2026 to the Kansas Information Technology Office. For the appropriation, the bill would require 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 that would be created by the bill.

The bill would appropriate $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 would also create, and appropriate in FY 2025 and 2026, a no-limit Information Technology Security Fund within the State Treasury, for use by the Kansas information Security Office 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 (Sections 16–17, 19, and 20)

The bill would modify 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. [*Note:* Current law provides that these members are voting members.] The bill would also add two IT employees, appointed by the State Board of Regents, as voting members of ITEC. The Executive Branch CITO would serve as the Chairperson of ITEC.

The bill would modify ITEC's responsibilities to make clear the polices it establishes would apply only to Executive Branch agencies. The bill would add 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 would remove 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 would require them to monitor and comply with policies set by their respective branches or offices.

Finally, the bill would require ITEC to meet monthly instead of quarterly.

CITO Requirements (Sections 18–22)

The bill would modify 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, KORA,

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 would specify IT and cybersecurity staff employed by OITS within branch agencies would be prohibited from disclosing confidential information of the agency. Violation of this prohibition would constitute a severity level 5 nonperson felony.

Agency Head Responsibilities (Section 25)

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

Definition Changes and Exemptions (Sections 15, 21–22)

The bill would modify the definition of "executive agency" in statutes governing IT in Chapter 75 of the *Kansas Statutes Annotated* to include the Judicial Council but not elected office agencies.

The bill would modify 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 would modify 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.

Background

SB 291, as passed by the Senate on March 28, 2023, contained provisions enacting the Kansas Public Investments and Contracts Protection Act and provisions concerning environmental, social, or governance (ESG) criteria.

On March 20, 2024, the House Committee on Legislative Modernization removed the contents of SB 291, inserted the contents of HB 2842, as amended by the House Committee, and recommended a substitute bill. The background of HB 2842 follows below.

HB 2842

The bill was introduced by the House Committee on Appropriations at the request of Representative B. Carpenter.

House Committee on Legislative Modernization

In the House Committee hearing, Representative B. Carpenter testified as a **proponent** of the bill, stating the bill contains comprehensive measures to strengthen cybersecurity infrastructure across all branches of state government.

The Executive CITO and representatives of the Office of Secretary of State and the Judicial Branch provided neutral

testimony on the bill, generally expressing the need for amendments and further consideration of the bill's impact on certain agency and branch operations before enacting the bill.

No other testimony was provided.

The House Committee amended the bill to clarify language regarding services and employees that would be transferred to OITS and which agencies or officers would be subject to the bill's provisions.

Fiscal Information

A fiscal note for HB 2842 was not available when the House Committee took action on House Sub. for SB 291.

Chief Information Security Officer; Chief Information Security Officer; cybersecurity; information technology; Information Technology Executive Council; state government