UPDATED
SESSION OF 2026

SUPPLEMENTAL NOTE ON HOUSE BILL NO. 2574

As Amended by House Committee on Legislative Modernization

Brief*

HB 2574, as amended, would create law and amend provisions concerning the administration and organization of information technology (IT) and cybersecurity services within each branch of state government and certain elected offices. The bill also would remove delayed versions of statutes to eliminate certain sunset provisions enacted in 2024 SB 291.

Information Technology Councils (New Sections 1 and 2, Sections 8 and 9)

Legislative and Judicial Branch Technology Oversight Councils (New Sections 1 and 2)

The bill would establish Branch Technology Oversight councils for the Legislative and Judicial branches. Membership for the councils would be determined by the Legislative Coordinating Council and the Chief Justice respectively. Duties of each Council would include:

- Setting IT standards;
- Establishing IT policies;
- Approving strategic IT plans;

---

*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 https://klrd.gov/

- Overseeing IT projects to ensure alignment with branch goals;
- Evaluating IT and cybersecurity programs; and
- Supporting the respective chief information technology officers (CITO) and the respective chief information security officers (CISO).

Information Technology Executive Council Membership (Section 8)

The bill would modify the membership and structure of the Information Technology Executive Council (ITEC). The number of voting members would increase from 13 to 17 by adding the executive CISO, removing the Network Manager for the Information Network of Kansas as a member, and converting the four legislative positions from non-voting members to voting members.

Information Technology Executive Council Duties (Section 9)

The bill would remove the ITEC's duty to develop a plan to integrate all IT services for the Executive Branch into the Office of Information Technology Services (OITS) and all cybersecurity services for state educational institutions into OITS and the Kansas Information Security Office (KISO). The related January 15, 2026, reporting requirement to the Senate Committee on Ways and Means and House Committee on Legislative Modernization would also be removed.

Cybersecurity Programs and Standards (Sections 3-7, 10-11, & 13)

The bill would require cybersecurity programs developed by CISOs for the Executive Branch, Legislative Branch, Judicial Branch, Attorney General, Commissioner of

Insurance, Secretary of State, State Treasurer, and the Director of the Kansas Bureau of Investigation (KBI) to be based on, rather than comply with, a nationally recognized standard for governmental entities. The requirement for the programs to achieve a specific National Institute for Standards and Technology Cyber Security Framework (NIST CSF) tier would be removed. Instead, beginning in 2027 and every two years thereafter, the appropriate CISO would be required to report to the Joint Committee on Information Technology (JCIT), the House Committee on Appropriations, and the Senate Committee on Ways and Means on the maturity level of the program.

Kansas Public Employee Retirement System (Section 5 and 15)

The bill would clarify that all cybersecurity services for the Kansas Public Employees Retirement System (KPERS) would be the responsibility of the Office of the State Treasurer's CISO. The bill would require all KPERS cybersecurity focused employees to work at the direction of the respective CISO and that all staff within the Office of the State Treasurer and KPERS complete annual cybersecurity awareness training or lose access to their state-issued system-related hardware.

Cybersecurity Audits and Vulnerability Assessments (Sections 3-7, 10-11, and 14)

The bill would amend the current requirements for CISOs to coordinate with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to perform annual audits to require coordination of periodic audits of departmental compliance with the respective cybersecurity program. Results of these audits would remain exempt from the Kansas Open Records act until July 1, 2030, unless reviewed and extended by the Legislature before that date.

The bill would remove provisions requiring the branch CISOs to report CISA audit failures to legislative leadership within 30 days and coordinate additional audits.

Executive Branch Chief Information Security Officer (Section 13)

In addition to the cybersecurity and program assessment duties required of all CISOs, the bill would modify the duties of the Executive Branch CISO. The bill would amend provisions regarding a duty to review all contracts to require the Executive Branch CISO to ensure that all contracts related to IT contain provisions to reduce the risk of security vulnerabilities within the supply chain or product.

The bill would add a duty to require the CISO to adopt statewide cybersecurity standards, controls, directives, and maturity and tier expectations for the Executive Branch and continually evaluate standards and expectations to address evolving threats, federal requirements, technological changes, and statewide risk conditions.

Kansas Information Security Office Duties (Section 14)

The bill would require the KISO to conduct periodic cybersecurity assessments of each Executive Branch agency that could include a review of controls, processes, technologies, governance, incident preparedness, operational security, and compliance with statewide policies and standards. To accomplish the assessments, the Executive Branch CISO would be authorized to utilize KISO personnel, qualified third-party assessors, or a combination thereof.

The bill also would authorize the CISO to establish an assessment cycle that includes an initial baseline assessment for each agency and periodic assessments thereafter. After conducting an assessment, the Executive Branch CISO

would be required to issue written findings, recommendations, and a timeline for any corrective action needed based on the results. Agencies would be required to develop and maintain written plans of action and milestones that detail efforts to remediate any findings.

The bill also would remove the requirement for the Executive Branch CISO to report audit failures to certain legislative leadership officials within 30 days and coordinate additional audits.

Executive Branch Agency Head Responsibilities (Section 15)

The bill would require Executive Branch agency heads to:

- Continuously work toward improving cybersecurity maturity consistent with statewide standards and expectations adopted by the executive CISO; and
- Prior to acquiring any cybersecurity-related product, service, or platform that may materially affect state systems, data, or cybersecurity risks, work with the executive CISO and obtain a written certificate stating such acquisition does not create a cybersecurity risk.

Judicial Branch Chief Information Security Officer (Section 10)

The bill would require the Judicial Branch CISO to perform their duties in coordination with the Judicial Technology Oversight Council. Further, the Judicial Branch CISO duty to review all contracts related to IT would be changed to a requirement to ensure that all contracts contain provisions to reduce the risk of security vulnerabilities within the supply chain or product.

Legislative Branch Chief Information Security Officer (Section 11)

The bill would restructure the position and duties of the Legislative CISO and make the position an appointment of the Legislative CITO rather than the Legislative Coordinating Council. The bill would remove a list of specific duties of the Legislative CISO from statute. The bill would require the Legislative CISO to ensure all employees of each legislative agency and all legislators complete annual cybersecurity awareness training. The CISO would also be responsible for developing a cybersecurity program and coordinating periodic audits of such a program.

Cybersecurity Compliance and Budget Process (Section 17)

The bill would require, beginning October 1, 2028, the Executive Branch CISO, in consultation with the Director of the Budget, to report to the Senate Committee on Ways and Means, House Committee on Appropriations, and JCIT any Executive Branch agency that is not making progress on a written plan of action and milestones based on the cybersecurity assessment of such agency. Each such agency would be required to present to the aforementioned committees the agency's plan to make progress on the written plan of action and milestones.

The Executive Branch CISO would also be required to submit a detailed written report to the aforementioned committees on or before the first day of the regular legislative session concerning each agency that continues to fail to make progress on a written plan of action and milestones.

The bill would require, during the regular legislative session, the Senate Committee on Ways and Means and House Committee on Appropriations to consider whether to lapse amounts appropriated and reappropriated and decrease the expenditure limitations for IT and cybersecurity

expenditures for such state agencies by 10 percent during the budget process.

The bill would remove the sunset of July 1, 2026, for this section of the bill.

Definitions—Kansas Cybersecurity Act (Section 12)

The bill would modify the definition of “executive branch agency” to add the Kansas Public Employees Retirement System (KPERS) to the currently excluded entities (elected office agencies, Adjutant General's Department, State Board of Regents' institutions, and the State Board of Regents).

Technical Changes and Sunset Removal (Section 16 and 18)

The bill would remove a January 1, 2026, requirement for the Executive and Judicial branches to develop IT consolidation plans. [*Note:* These plans were delivered to the Legislature in January 2026.]

Further, the bill would remove a February 1, 2025, deadline from a requirement that all branch or agency websites be hosted on a “.gov” domain.

The bill also would remove the July 1, 2026, sunset for the requirement that appropriations for IT and cybersecurity expenditures be separate line items, and that all branch or agency websites be hosted on a “.gov” domain.

The bill would repeal versions of statutes that would have taken effect on July 1, 2026, effectively sunsetting provisions enacted by 2024 SB 291 to recodify law as it existed on June 30, 2024. These provisions addressed topics that include, but are not limited to:

- IT project definitions;

- ITEC membership, powers, and duties;
- Branch CITO establishment and responsibilities;
- Branch and elected official CISO establishment and responsibilities;
- Agency head cybersecurity responsibilities; and
- KISO responsibilities.

Background

The bill was introduced by the House Committee on Legislative Modernization at the request of JCIT.

House Committee on Legislative Modernization

In the House Committee hearing, **proponent** testimony was provided by Representative Hoffman and the Executive Branch CITO. Both generally stated the bill would remove the sunset on certain provisions of 2024 SB 291 set to expire July 1, 2026, while amending others to strengthen state cybersecurity governance across all three governmental branches. Key changes include restructuring ITEC, refining the cybersecurity maturity assessment and accountability process, and mandating alignment to a recognized cybersecurity framework. Representative Hoffman also noted two potential amendments under consideration: creating a formal legislative technology oversight committee and replacing the specific NIST 2.0 reference with more generic statutory language.

Neutral testimony was provided by a representative of the Legislative Division of Post Audit, who raised several concerns, including ambiguous audit frequency requirements, audits being focused on cybersecurity programs rather than individual agency compliance, confidentiality gaps for agency-specific audits and assessments, a potential conflict of

interest in allowing the Executive CISO to conduct its own agency audits, and the budget penalty process lacking uniform criteria and clear definitions of progress, with such accountability measures applying only to the Executive Branch.

Additional neutral testimony was provided by the Executive Director of KPERS, who requested an amendment to exclude KPERS from the provisions that would consolidate its cybersecurity functions within the Executive Branch, citing concerns that such consolidation would weaken the Board of Trustees' ability to exercise direct oversight over a critical fiduciary risk area.

No other testimony was provided.

The House Committee amended the bill to:

- Create a Legislative Branch Information Technology Oversight Council;
- Make cybersecurity programs based on nationally recognized standards for government instead of specifically basing them on NIST CSF;
- Clarify audits would be conducted on an agency's compliance with a respective cybersecurity program instead of an audit of the cybersecurity program itself;
- Add JCIT to the list of committees that would receive a report pertaining to an agencies continued failed progress on written cybersecurity action plans; and
- Make technical and conforming changes throughout.

Fiscal Information

According to the fiscal note prepared by the Division of the Budget on the bill, as introduced, the Secretary of State estimates an increase in State General Fund (SGF) expenditures of $120,000 in FY 2026 for an additional IT staff person.

Legislative Administrative Services indicates the bill could increase expenditures but could not provide an estimate, and additional resources may be needed depending on the cybersecurity program.

The State Treasurer's Office indicates increased expenditures resulting form enactment of the bill could be handled with existing resources.

The Office of Judicial Administration indicates enactment of the bill could increase expenditures for establishing the Judicial Branch Technology Oversight Council and conducting cybersecurity audits. An initial audit could be absorbed within existing resources, but future audits could require additional SGF depending on cost and frequency of audits.

The Department of Insurance, Office of the Attorney General, OITS, and KBI indicate enactment of the bill would have no fiscal effect.

KPERS indicates the bill would not result in a significant change to the agency's cybersecurity expenditures, and enactment of the bill could be handled with existing resources.

Any fiscal effect associated with enactment of the bill is not reflected in *The FY 2027 Governor's Budget Report*.

Chief information security officer; chief information technology officer; cybersecurity; information technology; technology councils; state government