

KANSAS OFFICE *of*
REVISOR *of* STATUTES

LEGISLATURE *of* THE STATE *of* KANSAS
Legislative Attorneys transforming ideas into legislation.

300 SW TENTH AVENUE ■ SUITE 24-E ■ TOPEKA, KS 66612 ■ (785) 296-2321

MEMORANDUM

To: House Committee on Appropriations

From: Office of Revisor of Statutes

Date: January 31, 2023

Subject: Bill Brief on HB 2077

HB 2077 implements additional reporting requirements for informational technology projects and state agencies and requires additional information technology security training and status reports.

Section 1 amends K.S.A. 46-2102 and would change the responsibilities of the JCIT. Under current law, the JCIT studies the use of information technology by state agencies, reviews and makes recommendations on information technology project budgets and implementation plans, and studies the results of implemented information technology projects. The draft would require the Joint Committee to advise and consult on all state agency information technology projects that pose a significant business risk as determined by the information technology executive council (ITEC) policies.

Section 2 amends K.S.A. 75-7201 and would make changes to the definitions used in information technology sections. Under current law, an information technology project is defined as a projected with an estimated cumulative cost of \$250,000 or more and includes any such project that has proposed expenditures for: (1) New or replacement equipment or software; (2) upgrade improvements to existing equipment and any computer systems, programs or software upgrades therefor; or (3) data or consulting or other professional services for such a project. The bill would instead define a project as an “information technology effort of defined and limited duration that implements, effects a change in or presents a risk to process, services, security, systems, records, data, human resources or architecture.” Additionally, the definition of a project change or overrun would change from an increase of \$1,000,000 or 10% to a threshold established by ITEC policies. The bill would also add a definition of business risk to mean “the overall level of risk determined by a business risk assessment that includes, but is not limited to,

cost, information security and other elements as determined by the information technology executive council policies.”

Section 3, 4, and 5 of the bill would make changes to reporting requirements for the Chief Information Technology Officers (CITO) of each branch of government concerning information technology projects. Under current law, the Executive CITO submits recommendations to the division of the budget, the Judicial CITO submits recommendations to the judicial administrator, and the Legislative CITO submits recommendations to the Legislative Coordinating Council for information technology projects. These recommendations concern the technical and management merit of information technology project estimates and project overruns based on a review with the corresponding agency regarding information technology plans, project estimates, and deviations from the state information technology architecture. The bill would change these recommendations to apply to all planned information technology projects that are reportable.

Section 6 of the bill would make changes to the reporting requirements for agencies concerning information technology projects. Under current law, an agency provides a project budget estimate and a written plan for the project that includes a description and need for the project, the tasks and schedule for the project, a financial plan and expenditures, and a cost-benefit statement for the project. The bill would remove these provisions and require an agency to submit a report for a project that includes documentation with a financial plan showing the proposed source of funding with cost estimates. It would also require the documentation to be consistent with information technology resource policies and procedures and project management methodologies, an information technology architecture, standards for data managements and a strategic information technology management plan. Any information technology project that, pursuant to ITEC policies, was determined to have significant business risk would be presented to the Joint Committee on Information Technology by the CITO for that agency.

Additionally, current law requires that before an agency can begin implementation of an information technology project, the project plan must be approved by the head of the agency and the CITO for that branch of government. The bill would require that prior to the release of any request for proposal, that all specifications for bids or proposals related to an approved information technology project of one or more state agencies be reviewed by the appropriate CITO for that agency. Projects that required CITO approval would also require the CITO's written approval on specifications for bids or proposals.

The state agency involved in the project would be required to submit the project, the project plan, including the architecture, and the cost-benefit analysis to their CITO. The CITO would then make the project plan summary available to the JCIT. Pursuant to ITEC policy, the CITO would facilitate coordination with JCIT on any questions, requests for additional information, and meeting requests from JCIT. If two or more members of the joint committee contact the director legislative research within seven days of the date specified in the summary description and request that the joint committee schedule a meeting, the director shall, within 24 hours, notify the CITO of the appropriate branch, the head of the state agency and the chairperson that a meeting has been requested. Upon receiving that notification, the chairperson shall call a meeting.

Additionally, the state agency could not approve the release of any request for proposal or other bid event for a high-risk information technology project without having first advised and consulted with JCIT. The agency shall be deemed to have advised and consulted with the joint committee if fewer than two members of the joint committee make a request for a meeting or a committee meeting is scheduled but does not occur within two calendar weeks.

Section 7 of the bill amends K.S.A. 75-7210 and concerns the submission of reports by the CITOs to the Joint Committee and other legislative committees. Under current law, the CITOs are required to submit all information technology project budget estimates, three-year plans, and deviations from the state information technology project architecture each year before October 1. The bill would move this date to November 1. It would also require the joint committee to review those estimates and make recommendations to House Appropriations and Senate Ways and Means regarding appropriations.

Section 8 of the bill amends K.S.A. 75-7211 and concerns information technology changes and the Joint Committee. Under current law, the head of an agency may authorize a change in an information technology project if such change would not result in increased project costs of more than \$1,000,000 or 10% of the currently authorized project cost. For project changes that would result in an increase of more than \$1,000,000 or 10% of the total project cost, the agency head must first consult with the Joint Committee on such project change. The bill would remove these provisions and require an agency head to report all project changes or overruns to the JCIT through the agency's CITO pursuant to ITEC policy.

Sections 9 through 12 would amend the Kansas Cybersecurity Act to require information technology security training and cybersecurity status reports from state agencies. Under current law, the Chief Information Security Officer is required to ensure a cybersecurity training

program is available to executive branch agencies at no cost. The bill would require the CISO to ensure a cybersecurity awareness training program is available to all agencies.

Currently the Cybersecurity Act requires all executive branch agency heads to submit a cybersecurity assessment report to the Chief Information Technology Officer and prepare a summary of the report for the Legislature. The bill would require the full report to instead be provided to the joint Committee on Information Technology and the summary of the report be provided to the House of Representatives Committee on Appropriations and the Senate Committee on Ways and Means. All information collected under the Act would be considered confidential unless all information that could compromise the security of an organization or information system was redacted.

The CISO, with input from the joint committee on information technology and the joint committee on Kansas security, would be required to develop a self-assessment report template and provide such template to state agencies. Self-assessment reports made to the CISO would be confidential and not subject to the Kansas open records act.

Lastly, the head of all state agencies would be required to:

- (1) Participate in annual agency leadership training to ensure understanding of how cyberattacks and data breaches occur, the potential impact of cyberattacks and data breaches on the agency and other governmental entities on the state enterprise network, and steps to take to protect their information systems;
- (2) ensure that all information technology login credentials are disabled the same day that any employee ends their employment with the state; and
- (3) require that all employees with access to information technology receive a minimum of one hour of information technology security training per year.