SESSION OF 2023

SUPPLEMENTAL NOTE ON SUBSTITUTE FOR HOUSE BILL NO. 2077

As Amended by Senate Committee on Ways and Means

Brief*

Sub. for HB 2077, as amended, would add requirements for reporting significant cybersecurity incidents by entities maintaining personal information provided by the State or using information systems operated by the State. Additionally, the bill would authorize the Executive Branch Chief Information Security Officer (CISO) to establish branch cybersecurity standards and policy, and make changes to the responsibilities of state agencies and agency heads with regard to cybersecurity training, assessment, and incident response.

The bill would make several changes to the powers and duties of the Joint Committee on Information Technology (JCIT) with regard to JCIT's role in information technology (IT) project proposals. Further, the bill would amend the existing definitions of "information technology project" and "IT project change or overrun."

Furthermore, the bill would make changes to membership requirements, membership terms, and quorum requirements for the Information Technology Executive Council (ITEC).

---

*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

Cybersecurity Provisions

Cybersecurity Incident Reporting (New Section 1 and Section 3)

The bill would require entities that handle personal information provided by the State, or utilize an information system operated by the State, to disclose significant cybersecurity incidents to the Kansas Information Security Office (KISO) within 48 hours of the discover of the incident. Additionally, if the incident involved election data, the entity would also be required to notify the Secretary of State. "Significant cybersecurity incident" would be defined as a cybersecurity event, incident, breach, suspected breach, or unauthorized disclosure that requires the entity to initiate a response or recovery.

The bill would also require entities connected to the Kansas Criminal Justice Information System (KCJIS) to report such incidents per the rules and regulations that would be adopted by the Kansas Criminal Justice Information System Committee (KCJIS Committee). Such entities would also be exempt from reporting incidents to the KISO if they are not connected to any other State of Kansas information system, and the Kansas Bureau of Investigation (KBI) would be required to notify the KISO of reports it receives per rules and regulations adopted by the KCJIS Committee within 48 hours of receiving such reports.

Furthermore, the bill would specify that information provided related to such an incident could only be shared with those responsible for response and defense activities in service of state information systems, or those requested to assist in such activities. The information pertaining to the incident would not be subject to the provisions of the Kansas Open Records Act through July 1, 2028.

CISO and KISO Requirements (Section 13 and 14)

The bill would modify the CISO's duties to include setting cybersecurity policy and standards for executive branch agencies, and make similar technical changes to provisions related to requirements of the KISO. Furthermore, the bill would require the KISO to perform audits of Executive Branch agencies for compliance with applicable laws, rules, policies, and standards adopted by ITEC. The audit results would not be subject to the provisions of the Kansas Open Records Act through July 1, 2028.

The bill would require the KISO to ensure a cybersecurity awareness training program is available to all branches of state government and remove the requirement that such a training be made available at no cost. [*Note:* Current law requires the KISO to ensure a cybersecurity training program is provided only to the Executive Branch.]

The bill would remove the requirements for KISO to provide cybersecurity threat briefings to ITEC and to provide an annual status report of Executive Branch cybersecurity programs to JCIT and the House Committee on Government, Technology, and Security.

Agency Head Cybersecurity Responsibilities (Section 15)

The bill would establish new requirements for executive agency heads with regard to cybersecurity. The requirements would include:

- Participation in annual leadership training to better understand;
    - The impact of common types of cyberattacks and data breaches on state operations and assets;
    - How cyberattacks occur; and

- The steps an agency head and their employees can take to protect information and IT systems;

- Disabling IT login credentials the same day any employee terminates their employment for the State; and

- Requiring all employees with access to IT systems to partake in at least one hour of IT security training each year.

Internal Cybersecurity Assessments

The bill would rename the agency cybersecurity reports that are submitted to the CISO by October 16 of even-numbered years. The bill would require the appropriate agency head to provide authorization prior to the release of the renamed cybersecurity self-assessment reports. Agency heads would also be required to prepare a financial summary of cybersecurity expenditures to address the findings of the self-assessment report and submit the report to the Senate Committee on Ways and Means (SWAM) and the House Committee on Appropriations (HAP) with any confidential information redacted.

The CISO, with input from JCIT and the Joint Committee on Kansas Security (Security Committee), would also be required to develop a self-assessment report template for agency use. The CISO would be required to provide a summary of the self-assessment reports to JCIT and the Security Committee. The self-assessment reports would not be subject to the provisions of the Kansas Open Records Act through July 1, 2028.

Confidentiality (Section 16)

The bill would require all units of state and local government to consider information collected under this act to

be confidential. [*Note:* Current law specifies only information collected by the Executive Branch and KISO should be considered confidential.]

JCIT and IT Project Provisions

JCIT Powers and Duties (Section 2)

The bill would require JCIT to advise and consult on state IT projects that have a significant business risk per ITEC policy. Furthermore, the bill would expand the items JCIT is required to make recommendations on to SWAM and HAP to include IT project requests for proposals (RFPs).

[*Note:* Current law requires JCIT to make recommendations on implementation plans, budget estimates, and three-year IT plans.]

Definitions (Section 4)

The bill would amend the definitions of "business risk," "information technology project," and "information technology project change or overrun."

The term "business risk" would be defined as an overall level of risk that is determined through a business risk assessment and would include, but not be limited to, the cost of the project, information security of the project, and other elements determined by ITEC policy.

The bill would define "information technology project" as an effort by a state agency 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 IT architecture.

The bill would amend the definition for "information technology project change or overrun" by replacing the

existing $1.0 million threshold with regard to project expenditures to a threshold established per ITEC policy. The definition would also include any IT project that has experienced a change to its presented scope or timeline of more than 10 percent or a change that is significant as determined by ITEC policy.

IT Project Process (Section 9)

Submission of Project Documentation

The bill would require an agency to prepare and submit IT project documentation to the Chief Information Technology Officer (CITO) of their respective branch of state government. The IT project documentation would be required to:

- Include a financial plan that shows funding sources and expenditures for each project phase;
- Include cost estimates for needs analysis, other investigations, consulting and professional services, data, equipment, buildings, and associated costs;
- Include other items necessary for the project; and
- Be consistent with:
    - ITEC policy, procedures, and project planning methodology;
    - IT architecture for state agencies;
    - State agency data management standards; and
    - The State's Strategic IT Management Plan.

The bill would require any IT project with significant business risk, as determined by ITEC policy, to be presented to JCIT by the appropriate CITO.

Prior to Release of RFPs or Bids

Prior to the release of any IT project proposals with a significant business risk, an agency would be required to:

- Submit plans for such project to the appropriate CITO of the branch of government in which their office resides;

- Receive approval on the bid specifications if a project requires the CITO's approval; and

- Submit a project plan summary to members of JCIT, for consultation on the project, and to the Director of Legislative Research.

The project plan summary would be required to include the project, project plan, IT architecture information, cost benefit analysis, and date the summary was mailed or emailed.

The bill would allow JCIT members to communicate with the appropriate branch CITO to seek any additional information regarding the project.

Request for a JCIT Meeting for Review

The bill would authorize JCIT members to request a presentation and review of the proposed IT project to be presented to JCIT in a meeting. To request a meeting, members would contact the Director of Legislative Research within seven business days from the specified project submission date (included in the project summary information) and request a meeting for the purpose of receiving such a presentation.

If at least two committee members make a request, the Director of Legislative Research would have until the next business day after the second request to notify the appropriate CITO, head of the respective agency, and the

chairperson of JCIT. Upon receipt of the communication, the chairperson would be required to call a meeting as soon as practicable for such a presentation and provide the appropriate CITO and respective agency head with notice of the time, date, and place of the meeting.

The bill would prohibit the agency from releasing any RFPs or bids for IT projects with significant business risk, without having first advised and consulted with JCIT at a meeting.

Advise and Consult Criteria

The bill would deem the "advise and consult" requirement to have been met if fewer than two members notify the Director of Legislative Research with a request for a JCIT meeting within the specified time frame, or the requested meeting does not occur within two calendar weeks of the chairperson receiving the communication from the Director of Legislative Research.

Reporting Requirement Changes (Section 10)

The bill would change the submission date of three-year IT plans from October 1 to November 1 of each year.

The bill would also change, from the Legislative Branch CITO to JCIT, the entity responsible for reviewing all (Legislative, Judicial, and Executive branches) IT project budget estimates and revisions, three-year IT plans, and changes from the state IT architecture. JCIT would be responsible for making recommendations on the merit of associated appropriations to HAP and SWAM.

Legislative CITO and JCIT Direction (Section 11)

The bill would change the entity responsible for monitoring execution of reported IT projects from the

Legislative Branch CITO to JCIT. The bill would require, under the direction of JCIT, the CITO of each branch of government to provide a report on the implementation of all such projects. The report would be required to include proposed expenditures or any revisions for the current and subsequent fiscal years.

The bill would authorize JCIT to require the head of any agency to advise and consult on the status of IT projects for their respective agency, including any revisions to expenditures for the current or ensuing fiscal years. The bill would also authorize JCIT to provide updates to HAP and SWAM.

The bill would require agency heads to report all IT project changes or overruns to JCIT through the appropriate CITO pursuant to established ITEC policy, prior to the approval of any such change.

ITEC Membership and Quorum Requirements (Section 5)

The bill would remove the requirement that certain legislative members appointed to serve on ITEC by the President of the Senate, Minority Leader of the Senate, Speaker of the House, and the Minority Leader of the House, or their designees, be members of the SWAM or the House Committee on Government, Technology and Security or its successor committee.

The bill would further clarify that legislative members of ITEC must remain members of the Legislature in order to retain ITEC membership, and such members would serve until replaced. The appointing authority could remove, reappoint, or substitute a member at any time, and any vacancy would be filled in the same manner as the original appointment.

The bill would specify that a quorum for actions taken by the council would be nine members. Additionally, all ITEC

actions would be required to be taken by a majority of all members.

Technical and Clarifying Changes (Sections3, 6 – 8, and 12)

The bill would make several technical changes, which includes replacing references to "IT project estimates" with the term "IT projects," and adding the phrase "that are reportable" in certain sections when IT projects are required to be reported on to other entities such as the Division of the Budget and Legislative Coordinating Council.

The bill would also clarify the budget requests of KISO would be separate from the Office of Information and Technology Services.

Background

HB 2077 was introduced by JCIT as part of the Committee's recommendations to the 2023 Legislature.

House Committee on Appropriations

In the House Committee hearing, Representative Hoffman provided proponent testimony. The Representative noted that the bill, as introduced, is identical to 2022 HB 2548, which was passed by the House, but not considered by the Senate. The Representative also noted budget proviso language that temporarily enacted provisions allowing JCIT to advise and consult on IT projects for FY 2023. Furthermore, the Representative noted the bill would give the Legislature more oversight of IT projects during the project's planning phase and implement a risk-based assessment for state IT projects.

Neutral testimony was provided by the Executive Branch Chief Information Technology Officer (CITO), who stated a

risk-based approach to project evaluation provides a more holistic view of the impact of IT projects, noting the Kansas Information Technology Office has been testing the risk-based model through calendar year 2022. The CITO noted the bill would increase JCIT oversight, but the process does have potential to cause delays.

No other testimony was provided.

The House Committee amended the bill to:

- Authorize the Executive Branch CITO to set cybersecurity standards and create related policies for the Executive Branch, provide audit reports, and establish rules and regulations;

- Require entities connected to state information technology systems to report a significant cybersecurity breach to the Kansas Information Security Office (KISO) within 12 hours of the occurrence, and work with the KISO to mitigate damage; and

- Insert the contents of HB 2078, which are related to ITEC membership and quorum requirements.

The House Committee recommended a substitute bill incorporating these amendments.

House Committee of the Whole

The House Committee of the Whole amended the bill to clarify the reporting requirement procedures for cybersecurity incidents for entities that are connected to KCJIS.

Senate Committee on Ways and Means

In the Senate Committee hearing, neutral testimony provided by the Executive Branch CITO noted the bill would

change the definition of a reportable IT project from a monetary threshold to a risk-based model and would allow the Legislature additional IT project oversight and a more active role in the approval process.

Written-only neutral testimony was provided by the KBI .

A representative of the Kansas Chamber of Commerce provided **opponent** testimony indicating concerns with the 12-hour notification requirement for reporting a significant cybersecurity incident and the impact such a provision would have on a business that had access to personal information provided by the State.

Written-only opponent testimony was provided by the Consumer Data Industry Association, which expressed concerns pertaining to the 12-hour notification period and definition of “significant security incident”

The Senate Committee amended the bill to change the 12-hour notification requirement for cybersecurity incidents to a 48-hour notification requirement.

HB 2078 (ITEC Membership and Meeting Requirements)

HB 2078 was introduced by JCIT at the request of the Legislative CITO as part of the Committee’s recommendations to the 2023 Legislature.

House Committee on Appropriations

In the House Committee hearing, neutral testimony was provided by the Legislative CITO. The CITO noted the changes help to clean up the statute by eliminating references to legislative committees that no longer exist and clarify terms for legislative members.

No other testimony was provided.

Fiscal Information

According to the fiscal note prepared by the Division of the Budget on HB 2077, as introduced, the Office of Information Technology Services anticipates additional expenditures of $120,096 in FY 2024 for training employees from the State Board of Regents, Judicial Branch, and Legislative Branch. These expenditures would be recovered from the branches receiving the training.

The Kansas Department of Transportation anticipates additional workload to complete new documentation and reports, but it could be absorbed within existing resources.

The Kansas Department of Revenue indicates there would be no fiscal effect on agency operations.

According to the fiscal note prepared by the Division of the Budget on HB 2078, as introduced, the Office of Information Technology Services and Legislative Administrative Services state the bill would not have a fiscal effect.

Any fiscal effect associated with enactment of the bill is not reflected in *The FY 2024 Governor's Budget Report*.

Information technology; oversight; Joint Committee on Information Technology; projects; Information Technology Executive Council; cybersecurity; incident reporting