State Cybersecurity and Information Technology Projects; HB 2019

HB 2019 creates 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 authorizes 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 also makes 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 amends the definitions of "information technology project" and "IT project change or overrun."

The bill makes changes to membership requirements, membership terms, and quorum requirements for the Information Technology Executive Council (ITEC).

Cybersecurity Provisions

Cybersecurity Incident Reporting (New Section 1 and Section 3)

The bill requires any public entity that has a cybersecurity incident to notify the Kansas Information Security Office within 12 hours of discovering an incident. Any government contractor that experiences such an incident that involves involving the following must notify the Kansas Information Security Office (KISO) within 72 hours of a determination that such an incident has occurred:

- Confidentiality; or

- Integrity or availability of personal or confidential information provided by the State of Kansas, networks or information systems operated by or for the State.

The bill also requires the contractor to notify the KISO within 12 hours after a determination is made during an investigation that such an incident directly impacted state data, networks or information systems. Additionally, if the incident involved election data, then the public entity or contractor must notify the Secretary of State within 12 hours or 72 hours, respectively.

The bill also requires entities connected to the Kansas Criminal Justice Information System (KCJIS) to report such incidents per the rules and regulations to be adopted by the Kansas Criminal Justice Information System Committee (KCJIS Committee). Such entities are 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) must notify the KISO of reports it receives per rules and regulations adopted by the KCJIS Committee within 12 hours of receiving such reports.

The bill specifies that information related to such an incident can 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. These confidentiality provisions will expire July 1, 2028, unless the Legislature reviews and reenacts the confidentiality provisions prior to their expiration.

The bill requires the KISO to provide instructions on its website, prior to October 1, 2023, detailing the submission of the required cybersecurity incident reports. Instructions must include, at a minimum, the types of incidents for which incident reports are required, and any information that must be included an incident report.

The bill also clarifies that provisions cannot supersede notification requirements in current contracts between the State and other entities.

Definitions

The bill defines the terms "cybersecurity incident," "entity," "government contractor," "information system," "personal information," "private entity," "public entity," "security breach," "significant cybersecurity incident," and "unauthorized disclosure."

CISO and KISO Requirements (Sections 13 and 14)

The bill modifies the CISO's duties to include setting cybersecurity policy and standards for executive branch agencies, and makes similar technical changes to provisions related to requirements of the KISO. The bill requires the KISO to perform audits of Executive Branch agencies for compliance with applicable laws, rules, policies, and standards adopted by ITEC. The audit results are subject to the provisions of the Kansas Open Records Act through July 1, 2028.

The bill requires the KISO to ensure a cybersecurity awareness training program is available to all branches of state government and remove the requirement that such 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 removes 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 establishes new requirements for executive agency heads with regard to cybersecurity. The requirements 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 renames the agency cybersecurity reports that are submitted to the CISO by October 16 of even-numbered years, from "assessment report" to "self-assessment report." The appropriate agency head must provide authorization prior to the release of the reports. Agency heads are 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 and the House Committee on Appropriations with any confidential information redacted.

The CISO, with input from JCIT and the Joint Committee on Kansas Security (Security Committee), is 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. These confidentiality provisions will expire July 1, 2028, unless the Legislature reviews and reenacts the provisions prior to their expiration.

Confidentiality (Section 16)

The bill requires 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 requires JCIT to advise and consult on state IT projects that have a significant business risk per ITEC policy. Furthermore, the bill expands the items on which the JCIT is required to make recommendations to Senate Committee on Ways and Means and the House Committee on Appropriations to include IT project requests for proposals (RFPs).

[*Note*: JCIT has been required to make recommendations on implementation plans, budget estimates, and three-year IT plans.]

Definitions (Section 4)

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

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

The bill defines "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 amends the definition for "information technology project change or overrun" by replacing the existing $1.0 million threshold with regard to project expenditures with a threshold established per ITEC policy. The definition also includes 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.

Submission of Project Documentation

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

- 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.

Any IT project with significant business risk, as determined by ITEC policy, must 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 must:

- 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 bill requires the project plan summary include the project, project plan, IT architecture information, cost benefit analysis, and date the summary was mailed or emailed.

The bill allows 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 authorizes JCIT members to request a presentation and review of the proposed IT project in a meeting. To request a meeting, members 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 so request, the Director of Legislative Research has 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 must 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 prohibits 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 deems 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 changes the submission date of three-year IT plans from October 1 to November 1 of each year.

The bill also changes, 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 is responsible for making recommendations on the merit of associated appropriations to the House Committee on Appropriations and the Senate Committee on Ways and Means.

Legislative CITO and JCIT Direction (Section 11)

The bill changes 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 must include proposed expenditures or any revisions for the current and subsequent fiscal years.

The bill authorizes 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 also authorizes JCIT to provide updates to the House Committee on Appropriations and the Senate Committee on Ways and Means.

The bill requires 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 removes 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 Senate Committee on Ways and Means or the House Committee on Government, Technology and Security or its successor committee.

The bill further clarifies 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 can 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 specifies that a quorum for actions taken by the council is nine members. Additionally, the bill requires all ITEC actions to be taken by a majority of all members.

Technical and Clarifying Changes (Sections 3, 6, 7, 8, and 12)

The bill makes 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 regarding when reports on IT projects must be provided to other entities such as the Division of the Budget and Legislative Coordinating Council.

The bill also clarifies the budget requests of KISO will be separate from those of the Office of Information and Technology Services.