Summary of KS SB 291

Notes to the reader

The bill can be found here: https://kslegislature.org/li/b2023_24/measures/sb291/

The bill summary on the Kansas site (aka "short title"):

> House Substitute for SB 291 by Committee on Legislative Modernization - Transferring all cybsersecurity services under the chief information technology officer of each branch of government, creating chief information security officers within the judicial and legislative branches, requiring a chief information security officer to be appointed by the attorney general, Kansas bureau of investigation, secretary of state, state treasurer and insurance commissioner and requiring the chief information security officers to implement certain minimum cybersecurity standards, requiring the information technology executive council to develop a plan to integrate executive branch information technology services under the executive chief information technology officer, making and concerning appropriations for the fiscal years ending June 30, 2025, and June 30, 2026, for the office of information technology, Kansas information security office and the adjutant general, authorizing certain transfers and imposing certain limitations and restrictions and directing or authorizing certain disbursements and procedures for all state agencies and requiring legislative review of state agencies not in compliance with this act.

What follows is

- Part 1 - a three-page high level outline of the bill – the actions in the bill are grouped by the parts of government they impact: executive branch, judicial branch, legislative branch, and other agencies.
- Part 2 - a more detailed summary of each section or group of sections, roughly one page per section. Here the bill is summarized in sequential order of the sections.

"New Section" is the actual bill language. Where multiple sections are combined, the latter section is usually a lightly modified version of the previous section (e.g., "Sections 22 and 23 establish the Executive Chief Information Technology Officer (ECITO)").

The overall theme of the bill is to establish a robust cybersecurity program in every agency. Kansas has aligned on the NIST Cybersecurity Framework, version 2.0 (CSF version 2). The references to CSF tier 3.0 and CSF tier 4.0 are referring to the maturity level in implementing CSF version 2; you can read CSF tier 3.0 as "maturity level 3 of CSF version 2".

Part 1 - Gartner's bill summary

1. Executive Branch

A. Creation of CIO Position (ECITO) within the Office of Information Technology (OIT) (Sections 22, 23)

The ECITO, appointed by the Governor, will oversee IT plans, ensure compliance with state standards, and coordinate IT implementation across state agencies. This position will maintain confidentiality, enforce data center regulations, and report directly to the Governor, playing a significant role in shaping and securing the state's technological landscape by setting IT policies, standards, and strategic plans for executive branch agencies.

B. Creation of CISO Position Reporting to the CIO (Sections 32, 33)

The executive branch will establish a CISO position reporting to the ECITO, responsible for enforcing security standards and policies for IT systems, ensuring data confidentiality, availability, and integrity, and developing centralized cybersecurity protocols. The CISO will also manage incident response, develop agency cybersecurity programs in compliance with national standards, provide training, review contracts, and coordinate cybersecurity efforts among agencies.

C. Creation of the Kansas Information Security Office (KISO) in OIT (Sections 34, 35)

The KISO, managed by the executive CISO, will administer the Kansas Cybersecurity Act, develop and monitor state security programs, ensure legal compliance, coordinate annual audits, and manage incident response. The office will also provide cybersecurity staff and training, report audit failures within 30 days, and maintain audit report confidentiality until July 1, 2028. An IT Security Fund will be created for related expenditures.

D. Requirement for Agencies to Report Breaches and Conduct Self-Assessments (Sections 36, 37)

Agency heads must report breaches within 12 hours, submit biennial self-assessments, and conduct annual internal assessments. They will also participate in statewide initiatives, develop self-assessment templates, and summarize data for legislative review. Additionally, annual cybersecurity training for leadership and staff is required, with confidentiality of assessment data maintained until July 1, 2028.

E. Establishment of New Processes Around IT Projects and Procurement (Sections 28, 29)

New processes for IT project proposals and procurement will require thorough documentation aligned with state IT policies and standards, especially for high-risk projects. The Joint Committee on Information Technology will oversee this process, ensuring transparency and accountability. Vendor relationships will face scrutiny, with restrictions on contracting to maintain integrity, and agencies will have annual reporting requirements to ensure adherence to strategic IT plans and prompt reporting of any deviations.

F. Allocation of Funds for Executive Branch IT Security Operations (New Sections 5-8)

Funds will be allocated for various IT security operations within the executive branch. The Kansas Information Security Office will receive unspecified special revenue funds for 2025 and $15,000,000 plus special revenue funds for 2026, with the Budget Director certifying average cybersecurity expenditures for 2021-2025. The Adjutant General will receive $250,000 for operating expenditures

and will hire two full-time employees for the Kansas Intelligence Fusion Center to monitor state IT systems for the fiscal year ending June 30, 2025.

2. Judicial Branch

A. Creation of Judicial Chief Information Technology Officer (JCITO)

The JCITO will be established within the Office of the State Judicial Administrator. This position will be responsible for reviewing judicial IT plans, ensuring compliance with state standards, coordinating IT implementation, and managing IT resources. The JCITO must ensure necessary IT staffing, maintain US-based data centers, and keep an inventory of electronic devices while maintaining confidentiality and requesting security assessments from the Kansas National Guard. (Sections 24, 25)

B. Creation of Judicial Branch Chief Information Security Officer (CISO)

A Judicial Branch CISO, appointed by the Judicial Administrator with the Chief Justice's approval, will be responsible for setting security standards, developing centralized cybersecurity protocols, ensuring data protection, managing incident response, conducting annual training and audits, and reviewing IT contracts for security risks. The CISO must achieve NIST CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030, and report audit failures within 30 days. (New Section 2)

C. Allocation of Funds for Judicial Branch IT Security Operations

The Judicial Branch will receive $659,368 for operations for the fiscal year ending June 30, 2025. These funds are allocated for various IT security operations and judiciary functions to ensure compliance with the new cybersecurity requirements. (New Sections 5-8)

3. Legislative Branch

A. Creation of Legislative Chief Information Technology Officer (LCITO)

The LCITO will be established within the legislative branch and will be responsible for overseeing information technology. This includes reviewing and consulting on IT plans, ensuring compliance with IT policies and standards, and coordinating IT implementation across legislative agencies. The LCITO will also oversee confidentiality, security assessments, and maintain a database of electronic devices within the legislative branch. Additionally, they must consult with legal counsel on IT-related matters and ensure each agency has the necessary IT staff. (Sections 26, 27)

B. Creation of Legislative Branch Chief Information Security Officer (CISO)

A Legislative Branch CISO, appointed by the Legislative Coordinating Council, will be tasked with setting security standards, developing centralized cybersecurity protocols, ensuring data protection, managing incident response, conducting annual training and audits, and reviewing IT contracts for security risks. The CISO must achieve NIST CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030, and report audit failures within 30 days. (New Section 3)

C. Allocation of Funds for Legislative Branch IT Security Operations

Funds will be allocated for various IT security operations within the legislative branch to ensure compliance with the new cybersecurity requirements. These funds will support the implementation and maintenance of IT security measures and staff training.

4. Other Agencies and Exemptions

A. Commissioner of Insurance

The Commissioner of Insurance will appoint a CISO responsible for developing a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. The CISO will conduct annual training, manage audits, ensure audit confidentiality, and develop cybersecurity standards and policies. (Section 9)

B. Secretary of State

The Secretary of State will appoint a CISO responsible for cybersecurity standards and policies. The CISO will develop a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. Annual cybersecurity training for all employees is required, with access revoked for non-compliance. The CISO will also coordinate annual audits with the US Cybersecurity and Infrastructure Security Agency, ensuring audit results are confidential. (Section 12)

C. State Treasurer

The State Treasurer will appoint a CISO responsible for developing and managing a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. The CISO will ensure annual cybersecurity training, revoke access for non-compliance, and coordinate annual confidential audits with the US Cybersecurity and Infrastructure Security Agency. (Section 13)

D. Attorney General and Kansas Bureau of Investigation (KBI)

The Attorney General will appoint a CISO responsible for developing a cybersecurity program, with similar requirements for the Kansas Bureau of Investigation (KBI). Both positions require Senate confirmation for the Director. The CISOs will develop cybersecurity programs compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. They will ensure annual cybersecurity training, revoke access for non-compliance, and coordinate confidential annual audits with the US Cybersecurity and Infrastructure Security Agency. Provisions related to the CISO's duties will expire on July 1, 2026. (Sections 14, 15)

E. Exemptions

1. **State Educational Institutions**
    - State educational institutions are exempt from the provisions mandating centralization of cybersecurity services and integration plans. (New Section 1)
2. **Specific Exemptions Under the Open Records Act**

- Sections 10 and 11 establish criteria for exceptions to disclosure under the open records act, which are necessary, narrowly tailored, and serve a public purpose. New or amended exceptions expire five years after enactment unless continued by the legislature.

Part 2 - Gartner's bill analysis

New Section 1 Summary

New Section 1 mandates the centralization of cybersecurity services for all state branches by July 1, 2027, overseen by CITO and CISO, and requires an integration plan by January 2026. It includes transitioning all state websites to ".gov" domains by February 2025 and mandates separate line item budgeting for IT and cybersecurity starting July 1, 2025. State educational institutions are exempt from these provisions.

High-Level Tasks and Objectives

1. **Centralization of Cybersecurity Services (Effective July 1, 2027)**:
    - **Objective**: Administer all cybersecurity services for each branch of state government.
    - **Responsibility**: Chief Information Technology Officer (CITO) and Chief Information Security Officer (CISO) of each branch.
    - **Tasks**: Direct and manage all cybersecurity employees within the legislative and executive branches.
2. **Development and Reporting of Integration Plan (Due by January 1, 2026 & January 15, 2026)**:
    - **Objective**: Integrate all executive branch IT services into the Office of Information Technology Services.
    - **Responsibility**: Information Technology Executive Council (ITEC).
    - **Tasks**:
        - Develop the integration plan in consultation with agency heads.
        - Report the plan to the Senate Standing Committee on Ways and Means and the House Standing Committee on Legislative Modernization.
3. **Judicial IT Cost Estimation and Cybersecurity Planning (Due by January 1, 2026)**:
    - **Objective**: Estimate project costs for IT services and develop a cybersecurity program for judicial agencies.
    - **Responsibility**: Judicial Chief Information Technology Officer.
    - **Tasks**:
        - Estimate costs for IT hardware and services for judicial employees.
        - Develop a plan for judicial branch hardware to access the KANWIN network.
        - Create a cybersecurity program compliant with NIST CSF 2.0.
4. **Website Domain Transition (Due by February 1, 2025)**:

    - **Objective**: Move all government and state agency websites to a ".gov" domain.
    - **Responsibility**: All branches of government and state agencies.
    - **Tasks**: Transition websites to ".gov" domains.
5. **Separate Line Item Budgeting for IT and Cybersecurity (Effective July 1, 2025)**:
    - **Objective**: Ensure IT and cybersecurity expenditures are listed as separate line items in the budget.
    - **Responsibility**: State agencies.
    - **Tasks**: Present IT and cybersecurity budgets as separate line items for detailed legislative review.

Key Details and Deadlines

- **July 1, 2027**: Centralization of cybersecurity services begins.
- **January 1, 2026**: Deadline for the integration plan and judicial IT cost estimation.
- **January 15, 2026**: Deadline for reporting the integration plan.
- **February 1, 2025**: Deadline for transitioning websites to ".gov" domains.
- **July 1, 2025**: Separate line item budgeting for IT and cybersecurity starts.
- **July 1, 2026**: Expiration date of this section.

Exclusions:

- State educational institutions as defined in K.S.A. 76-711 are not subject to these provisions.

New Section 2 Summary

New Section 2 establishes the position of Judicial Branch Chief Information Security Officer (CISO), appointed by the Judicial Administrator with the Chief Justice's approval. The Judicial CISO will set security standards, develop centralized cybersecurity protocols, ensure data protection, manage incident response, conduct annual training and audits, and review IT contracts for security risks. The CISO must achieve NIST CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030, and report audit failures within 30 days.

High-Level Tasks and Objectives:

1. **Establishment of Judicial CISO**:
    - **Objective**: Create and appoint the position of Judicial Branch Chief Information Security Officer (CISO).
    - **Responsibility**: Judicial Administrator, with approval from the Chief Justice.
2. **Responsibilities of the Judicial CISO**:
    - **Reporting**: Report to the Judicial Administrator.
    - **Security and Compliance**:
        - Establish security standards and policies for judicial IT systems.
        - Develop centralized cybersecurity protocols.

        - Ensure data confidentiality, availability, and integrity.
        - Develop cybersecurity programs compliant with NIST CSF 2.0, aiming for tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
    - **Incident Response and Collaboration**:
        - Detect and respond to security incidents.
        - Collaborate with other state branches' CISOs.
    - **Training and Access Management**:
        - Ensure annual cybersecurity training for all judicial employees.
        - Revoke access for employees who do not complete training.
    - **Contract and Audit Management**:
        - Review IT-related contracts for security risks and standard security language.
        - Coordinate annual audits with the US Cybersecurity and Infrastructure Security Agency.
        - Manage audit failures and mitigation plans, report to legislative leaders, and ensure confidentiality of audit results.

Key Details and Deadlines:

- **Immediate**: Establish and appoint Judicial CISO.
- **Annual**: Conduct cybersecurity awareness training and audits.
- **July 1, 2028**: Achieve CSF tier 3.0 for cybersecurity programs.
- **July 1, 2030**: Achieve CSF tier 4.0 for cybersecurity programs.
- **30 Days Post-Audit Failure**: Report audit failures and mitigation plans to legislative leaders.
- **July 1, 2026**: Expiration date of this section.

New Section 3 Summary

New Section 3 establishes the position of Legislative Branch Chief Information Security Officer (CISO), appointed by the Legislative Coordinating Council. The Legislative CISO will set security standards, develop centralized cybersecurity protocols, ensure data protection, manage incident response, conduct annual training and audits, review IT contracts for security risks, and obtain legal approval from the Revisor of Statutes. The CISO must achieve NIST CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030, and report audit failures within 30 days.

High-Level Tasks and Objectives:

1. **Establishment of Legislative CISO**:
    - **Objective**: Create and appoint the position of Legislative Branch Chief Information Security Officer (CISO).
    - **Responsibility**: Legislative Coordinating Council.
2. **Responsibilities of the Legislative CISO**:
    - **Reporting and Collaboration**:
        - Report to the Legislative Chief Information Technology Officer.
        - Collaborate with CISOs of other state branches.

- **Security and Compliance**:
  - Establish security standards and policies for legislative IT systems.
  - Develop centralized cybersecurity protocols.
  - Ensure data confidentiality, availability, and integrity.
  - Develop cybersecurity programs compliant with NIST CSF 2.0, aiming for tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
  - Obtain approval from the Revisor of Statutes on legal issues related to IT security.
- **Incident Response and Training**:
  - Detect and respond to security incidents.
  - Ensure annual cybersecurity training for all legislators and legislative employees.
  - Revoke access for employees who do not complete training.
- **Contract Review and Audit Management**:
  - Review IT-related contracts for security risks and standard security language.
  - Coordinate annual audits with the US Cybersecurity and Infrastructure Security Agency.
  - Manage audit failures and mitigation plans, report to legislative leaders, and ensure confidentiality of audit results.

Key Details and Deadlines:

- **Immediate**: Establish and appoint Legislative CISO.
- **Annual**: Conduct cybersecurity awareness training and audits.
- **July 1, 2028**: Achieve CSF tier 3.0 for cybersecurity programs.
- **July 1, 2030**: Achieve CSF tier 4.0 for cybersecurity programs.
- **30 Days Post-Audit Failure**: Report audit failures and mitigation plans to legislative leaders.
- **July 1, 2026**: Expiration date of this section.

New Section 4 Summary

New Section 4 mandates the Director of the Budget to annually determine state agencies' compliance with the act starting July 1, 2028, in consultation with legislative, executive, and judicial IT officers. Non-compliant agencies will have 5% of their general and special revenue fund amounts certified and expenditure limitations set for special revenue funds without existing limits. The Director must report compliance determinations and certified amounts to the legislature by the first day of the regular session, with reviews during budget hearings.

High-Level Tasks and Objectives:

1. **Annual Compliance Determination (Effective July 1, 2028)**:
   - **Objective**: Ensure state agencies comply with the provisions of the act.
   - **Responsibility**: Director of the Budget, in consultation with legislative, executive, and judicial chief information technology officers.

- **Tasks**:
    - Determine compliance of each state agency for the previous fiscal year.
    - Certify 5% of the state general fund and special revenue fund amounts if a state agency is non-compliant.
    - Establish an expenditure limitation for non-compliant special revenue funds without an existing limitation.

2. **Reporting and Legislative Review**:
    - **Objective**: Report compliance determinations and certified amounts.
    - **Responsibility**: Director of the Budget.
    - **Tasks**:
        - Submit a detailed written report to the legislature by the first day of the regular session.
        - Include factors considered in compliance determinations and certified amounts for each state agency.
        - Senate Committee on Ways and Means and House Committee on Appropriations to review and consider compliance determinations during budget hearings.

Key Details and Deadlines:

- **July 1, 2028**: Start of annual compliance determination.
- **First Day of Regular Legislative Session**: Deadline for the Director of the Budget to submit the compliance report.
- **July 1, 2026**: Expiration date of this section.

New Sections 5-8 Summary

New Sections 5-8 allocate funds for various IT security operations and judiciary and adjutant general functions. The Judicial Branch receives $659,368 for operations for the fiscal year ending June 30, 2025. The Kansas Information Security Office receives unspecified special revenue funds for 2025 and $15,000,000 plus special revenue funds for 2026, with the Budget Director certifying average cybersecurity expenditures for 2021-2025. The Adjutant General receives $250,000 for operating expenditures and will hire two full-time employees for the Kansas Intelligence Fusion Center to monitor state IT systems for the fiscal year ending June 30, 2025.

High-Level Tasks and Objectives:

1. **Judicial Branch Appropriation**:
    - **Objective**: Allocate funds for judiciary operations.
    - **Responsibility**: Judicial Branch.
    - **Tasks**:
        - Manage appropriated funds for fiscal year ending June 30, 2025.
        - **Amount**: $659,368 from the state general fund.
2. **Kansas Information Security Office (2025)**:

- **Objective**: Allocate funds for IT security operations.
- **Responsibility**: Kansas Information Security Office.
- **Tasks**:
  - Manage funds from special revenue funds with no expenditure limit for fiscal year ending June 30, 2025.

3. **Kansas Information Security Office (2026)**:
   - **Objective**: Allocate funds for IT security operations.
   - **Responsibility**: Kansas Information Security Office.
   - **Tasks**:
     - Manage $15,000,000 from the state general fund for fiscal year ending June 30, 2026.
     - Manage funds from special revenue funds with no expenditure limit for fiscal year ending June 30, 2026.
     - Director of the Budget to determine and certify the average expenditures on cybersecurity services for each executive branch agency for fiscal years 2021-2025.
     - Transfer lapsed funds from the state general fund and special revenue funds to the Information Technology Security Fund.
4. **Adjutant General Appropriation**:
   - **Objective**: Allocate funds for monitoring state IT systems.
   - **Responsibility**: Adjutant General.
   - **Tasks**:
     - Use $250,000 from the state general fund for operating expenditures for fiscal year ending June 30, 2025.
     - Hire two full-time employees for the Kansas Intelligence Fusion Center to monitor state IT systems.

Key Details and Deadlines:

- **June 30, 2025**: Fiscal year end for appropriations in Sections 5, 6, and 8.
- **June 30, 2026**: Fiscal year end for appropriations in Section 7.
- **Fiscal Year 2026**: Budget Director to determine and certify average expenditures for cybersecurity services (Section 7(c)).

Section 9 Summary

Section 9 authorizes the Commissioner of Insurance to appoint various officials and employees, including an assistant commissioner, actuaries, special attorneys, and others, with salaries determined within appropriations. Appointees must take an oath, avoid conflicts of interest, and the assistant commissioner will act in the commissioner's absence. The Chief Information Security Officer (CISO) will develop a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030, conduct annual training, manage audits, and ensure audit confidentiality.

High-Level Tasks and Objectives:

1. **Commissioner of Insurance Appointments**:
    - **Objective**: Authorize the Commissioner of Insurance to appoint various officials and employees.
    - **Responsibility**: Commissioner of Insurance.
    - **Tasks**:
        - Appoint an assistant commissioner, actuaries, special attorneys, an executive secretary, policy examiners, field representatives, and a secretary.
        - Determine annual salaries within available appropriations.
        - Appoint additional employees as necessary under civil service law and available appropriations.
        - Ensure field representatives conduct inquiries, investigations, or receive complaints but do not examine insurance companies' financial conditions.
2. **Appointees' Requirements and Responsibilities**:
    - **Objective**: Ensure appointees meet certain standards and outline their roles.
    - **Responsibility**: Appointees.
    - **Tasks**:
        - Take the official oath.
        - Avoid conflicts of interest, except as policyholders.
        - Assistant commissioner to perform duties in the commissioner's absence.
        - Commissioner responsible for actions of appointees.
3. **Chief Information Security Officer (CISO) Role**:
    - **Objective**: Establish and manage cybersecurity standards and policies for the department.
    - **Responsibility**: Chief Information Security Officer (CISO).
    - **Tasks**:
        - **Cybersecurity Program**:
            - Develop a program compliant with NIST CSF 2.0.
            - Achieve CSF tier of 3.0 by July 1, 2028, and tier of 4.0 by July 1, 2030.
        - **Training and Access Management**:
            - Ensure annual cybersecurity awareness training for all employees.
            - Revoke access to state-issued hardware or network for non-compliant employees.
        - **Audit Management**:
            - Coordinate with the US Cybersecurity and Infrastructure Security Agency for annual audits.
            - Make annual audit requests.
            - Maintain audit confidentiality and report results confidentially, exempt from discovery or disclosure under the open records act.

Key Details and Deadlines:

- **July 1, 2026**: Expiration date for provisions related to the Chief Information Security Officer's duties (Sec. 9(c)(2)).
- **July 1, 2028**: Deadline to achieve CSF tier of 3.0 for the cybersecurity program.
- **July 1, 2030**: Deadline to achieve CSF tier of 4.0 for the cybersecurity program.

Sections 10 and 11 Combined Summary

Sections 10 and 11 establish criteria for exceptions to disclosure under the open records act, requiring exceptions to be necessary, narrowly tailored, and serving a public purpose. New or amended exceptions expire five years after enactment unless continued by the legislature. The Revisor of Statutes certifies expiring exceptions by July 15 of the preceding year, and exceptions reviewed and continued twice are exempt from expiration. Specific exemptions include those required by federal law, applicable solely to the legislature or state courts, and audit reports from the US Cybersecurity and Infrastructure Security Agency.

High-Level Tasks and Objectives:

1. **Criteria for Exceptions to Disclosure**:
    - **Objective**: Establish criteria for creating or maintaining exceptions to disclosure under the open records act.
    - **Responsibility**: Legislature.
    - **Criteria**:
        - Sensitive or personal nature of public records.
        - Necessity for effective and efficient administration of a governmental program.
        - Impact on confidential information.
    - **Tasks**:
        - Consider criteria before enacting exceptions to disclosure.
        - Ensure exceptions serve an identifiable public purpose and are not broader than necessary.
2. **Review and Expiration of Exceptions**:
    - **Objective**: Set expiration and review process for exceptions to disclosure.
    - **Responsibility**: Legislature and Revisor of Statutes.
    - **Tasks**:
        - New or substantially amended exceptions expire five years after enactment unless continued.
        - Revisor of Statutes to certify expiring exceptions by July 15 of the year before expiration.
        - Exceptions not certified do not expire.
        - Exceptions reviewed and continued twice are exempt from expiration.
3. **Specific Exemptions from Review and Expiration**:
    - **Objective**: Identify exceptions not subject to the standard review and expiration process.

- **Responsibility**: Legislature.
- **Tasks**:
  - Exemptions required by federal law.
  - Exemptions applying solely to the legislature or state court system.
  - Exemptions reviewed and continued twice by the legislature.
  - Reports of audit results from the US Cybersecurity and Infrastructure Security Agency.

4. **Legislative Review Process**:
   - **Objective**: Review exceptions before expiration.
   - **Responsibility**: Legislature.
   - **Tasks**:
     - Consider specific records affected, unique impact, public purpose, and alternative means of obtaining information.
     - Determine if the exception is necessary to serve an identifiable public purpose.
5. **Continuation of Existing Exceptions**:
   - **Objective**: Continue existing exceptions that have been reviewed and maintained by the legislature.
   - **Responsibility**: Legislature and Revisor of Statutes.
   - **Tasks**:
     - Maintain a list of exceptions continued in existence based on review sessions specified by year and statute.

Key Details and Deadlines:

- **Five-Year Expiration**: New or substantially amended exceptions expire five years after enactment unless continued by the legislature.
- **July 15 Certification**: Revisor of Statutes to certify expiring exceptions by July 15 of the year before expiration.
- **Exemptions**: Exceptions reviewed and continued twice, required by federal law, solely applying to the legislature or state court system, and audit reports from the US Cybersecurity and Infrastructure Security Agency, are exempt from standard review and expiration.

Section 12 Summary

Section 12 authorizes the Secretary of State to appoint assistants and clerks and establishes a Chief Information Security Officer (CISO) responsible for cybersecurity standards and policies. The CISO must develop a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. Annual cybersecurity training is required for all employees, with access revoked for non-compliance. The CISO will coordinate annual audits with the US Cybersecurity and Infrastructure Security Agency, ensuring audit results are confidential.

High-Level Tasks and Objectives:

1. **Secretary of State Appointments**:
    - **Objective**: Authorize the Secretary of State to appoint assistants and clerks.
    - **Responsibility**: Secretary of State.
    - **Tasks**:
        - Appoint assistants and clerks as authorized by law.
        - Ensure proper discharge of duties by assistants and clerks, who serve at the Secretary's pleasure.
2. **Appointment and Responsibilities of Chief Information Security Officer (CISO)**:
    - **Objective**: Establish and manage cybersecurity standards and policies for the office.
    - **Responsibility**: Secretary of State.
    - **Tasks**:
        - Appoint a Chief Information Security Officer (CISO).
        - **Cybersecurity Program**:
            - Develop a program compliant with NIST CSF 2.0.
            - Achieve CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
        - **Training and Access Management**:
            - Ensure annual cybersecurity awareness training for all employees.
            - Revoke access to state-issued hardware or network for non-compliant employees.
        - **Audit Management**:
            - Coordinate with the US Cybersecurity and Infrastructure Security Agency for annual audits.
            - Make annual audit requests and maintain audit confidentiality.
            - Audit results are confidential and exempt from discovery or disclosure under the open records act.

Key Details and Deadlines:

- **July 1, 2026**: Expiration date for provisions related to the CISO's duties.
- **July 1, 2028**: Deadline to achieve CSF tier 3.0 for the cybersecurity program.
- **July 1, 2030**: Deadline to achieve CSF tier 4.0 for the cybersecurity program.

Section 13 Summary

Section 13 authorizes the State Treasurer to appoint necessary personnel, including assistants, clerks, bookkeepers, accountants, and stenographers, who serve at the Treasurer's pleasure and must take an oath of office. It also establishes the appointment of a Chief Information Security Officer (CISO) responsible for developing and managing a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. The CISO must ensure annual cybersecurity training, revoke access for non-compliance, and coordinate annual confidential audits with the US Cybersecurity and Infrastructure Security Agency.

High-Level Tasks and Objectives:

1. **State Treasurer Appointments**:
    - **Objective**: Authorize the State Treasurer to appoint necessary personnel.
    - **Responsibility**: State Treasurer.
    - **Tasks**:
        - Appoint assistants, clerks, bookkeepers, accountants, and stenographers as authorized by law.
        - Ensure appointed personnel take the oath of office.
        - Personnel serve at the pleasure of the State Treasurer.
2. **Appointment and Responsibilities of Chief Information Security Officer (CISO)**:
    - **Objective**: Establish and manage cybersecurity standards and policies for the office.
    - **Responsibility**: State Treasurer.
    - **Tasks**:
        - Appoint a Chief Information Security Officer (CISO).
        - **Cybersecurity Program**:
            - Develop a program compliant with NIST CSF 2.0.
            - Achieve CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
        - **Training and Access Management**:
            - Ensure annual cybersecurity awareness training for all employees.
            - Revoke access to state-issued hardware or network for non-compliant employees.
        - **Audit Management**:
            - Coordinate with the US Cybersecurity and Infrastructure Security Agency for annual audits.
            - Make annual audit requests and maintain audit confidentiality.
            - Audit results are confidential and exempt from discovery or disclosure under the open records act.

Key Details and Deadlines:

- **July 1, 2026**: Expiration date for provisions related to the CISO's duties.
- **July 1, 2028**: Deadline to achieve CSF tier 3.0 for the cybersecurity program.
- **July 1, 2030**: Deadline to achieve CSF tier 4.0 for the cybersecurity program.

Section 14 Summary

Section 14 authorizes the Attorney General to appoint necessary personnel, including a Chief Information Security Officer (CISO) responsible for developing a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. The CISO must ensure annual cybersecurity training, revoke access for non-compliant employees, and coordinate confidential annual audits with the US Cybersecurity and Infrastructure Security Agency. Provisions related to the CISO's duties expire on July 1, 2026.

High-Level Tasks and Objectives:

1. **Attorney General Appointments**:
    - **Objective**: Authorize the Attorney General to appoint necessary personnel.
    - **Responsibility**: Attorney General.
    - **Tasks**:
        - Appoint assistants, clerks, and stenographers as authorized by law.
        - Ensure appointees serve at the pleasure of the Attorney General.
        - Turn all fees and allowances earned by assistants into the general revenue fund.
        - File verified accounts of fees collected with the Director of Accounts and Reports before vouchers for salaries are honored.
        - Assistants perform duties as prescribed by law and the Attorney General and can act with the Attorney General's delegated authority.
2. **Appointment and Responsibilities of Chief Information Security Officer (CISO)**:
    - **Objective**: Establish and manage cybersecurity standards and policies for the office.
    - **Responsibility**: Attorney General.
    - **Tasks**:
        - Appoint a Chief Information Security Officer (CISO).
        - **Cybersecurity Program**:
            - Develop a program compliant with NIST CSF 2.0.
            - Achieve CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
        - **Training and Access Management**:
            - Ensure annual cybersecurity awareness training for all employees.
            - Revoke access to state-issued hardware or network for non-compliant employees.
        - **Audit Management**:
            - Coordinate with the US Cybersecurity and Infrastructure Security Agency for annual audits.
            - Make annual audit requests and maintain audit confidentiality.
            - Audit results are confidential and exempt from discovery or disclosure under the open records act.

Key Details and Deadlines:

- **July 1, 2026**: Expiration date for provisions related to the CISO's duties.
- **July 1, 2028**: Deadline to achieve CSF tier 3.0 for the cybersecurity program.
- **July 1, 2030**: Deadline to achieve CSF tier 4.0 for the cybersecurity program.

Section 15 Summary

Section 15 establishes the Kansas Bureau of Investigation (KBI) under the Attorney General, requiring Senate confirmation for the Director and ensuring no appointees have felony convictions. It mandates the appointment of a Chief Information Security Officer (CISO) to develop a cybersecurity program compliant with NIST CSF 2.0, achieving tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030. The CISO must ensure annual cybersecurity training, revoke access for non-compliant employees,

and coordinate confidential annual audits with the US Cybersecurity and Infrastructure Security Agency. Provisions related to the CISO's duties expire on July 1, 2026.

High-Level Tasks and Objectives:

1. **Establishment of the Kansas Bureau of Investigation (KBI)**:
    - **Objective**: Create a division under the jurisdiction of the Attorney General.
    - **Responsibility**: Attorney General and Director of KBI.
    - **Tasks**:
        - Appoint a Director, subject to Senate confirmation.
        - Ensure the Director has special training and qualifications.
        - Appoint agents, associate director, assistant directors, deputy director, and administrative employees as necessary.
        - Ensure no appointees have felony convictions.
2. **Personnel Management**:
    - **Objective**: Manage the classification and compensation of KBI personnel.
    - **Responsibility**: Director of KBI.
    - **Tasks**:
        - Maintain Director, Associate Director, Deputy Director, Assistant Directors, and Assistant Attorneys General within the unclassified service.
        - Place all other agents and employees in the classified service.
        - Return appointed members to comparable positions after their term, creating temporary positions if necessary.
        - Ensure all agents take an oath to faithfully discharge their duties.
3. **Appointment and Responsibilities of Chief Information Security Officer (CISO)**:
    - **Objective**: Establish and manage cybersecurity standards and policies for the bureau.
    - **Responsibility**: Director of KBI.
    - **Tasks**:
        - Appoint a Chief Information Security Officer (CISO).
        - **Cybersecurity Program**:
            - Develop a program compliant with NIST CSF 2.0.
            - Achieve CSF tier 3.0 by July 1, 2028, and tier 4.0 by July 1, 2030.
        - **Training and Access Management**:
            - Ensure annual cybersecurity awareness training for all employees.
            - Revoke access to state-issued hardware or network for non-compliant employees.
        - **Audit Management**:
            - Coordinate with the US Cybersecurity and Infrastructure Security Agency for annual audits.
            - Make annual audit requests and maintain audit confidentiality.
            - Audit results are confidential and exempt from discovery or disclosure under the open records act.

Key Details and Deadlines:

- **July 1, 2026**: Expiration date for provisions related to the CISO's duties.
- **July 1, 2028**: Deadline to achieve CSF tier 3.0 for the cybersecurity program.
- **July 1, 2030**: Deadline to achieve CSF tier 4.0 for the cybersecurity program.

Sections 16 and 17 Combined Summary

Sections 16 and 17 introduces a series of definitions.

Definitions:

1. **Business Risk**: Overall level of risk determined by a business risk assessment, including cost, information security, and other elements as defined by relevant policies.
2. **Cumulative Cost**: Total expenditures from all sources for an IT project by one or more state agencies from project start to completion or termination.
3. **Executive Agency**: Any state agency in the executive branch of government, including the judicial council but excluding elected office agencies.
4. **Information Technology Project**: An IT effort by a state agency of defined and limited duration that affects processes, services, security, systems, records, data, human resources, or architecture.
5. **Information Technology Project Change or Overrun**: Changes exceeding 10% in project cost, scope, timeline, or significant upgrades/changes in IT equipment use.
6. **Joint Committee**: Joint Committee on Information Technology.
7. **Judicial Agency**: Any state agency in the judicial branch of government.
8. **Legislative Agency**: Any state agency in the legislative branch of government.
9. **Project**: Planned series of events or activities to accomplish a specified outcome within a specified time, with an identifiable budget.
10. **Project Completion**: When the head of a state agency certifies that the IT project is ready for operational use.
11. **Project Start**: When a state agency begins a formal study of a business process or technology concept to assess needs, determine feasibility, or prepare a project budget estimate.
12. **State Agency**: Any state office or officer, department, board, commission, institution, bureau, or any agency, division, or unit thereof.

Combined Summary of Sections 18, 19, 20, and 21

Sections 18, 19, 20, and 21 establish the Information Technology Executive Council, comprising 13-17 voting members from various state agencies and sectors. The Council, chaired by rotating Chief Information Technology Officers, will set IT policies, standards, and strategic plans for state executive branch agencies. It meets quarterly until July 1, 2026, then monthly, with a quorum of seven increasing to nine members. The Council reports a plan to integrate executive branch IT services and educational cybersecurity services by January 15, 2026, and members receive mileage reimbursements for meetings.

Establishment and Composition:

1. **Information Technology Executive Council**:
    - **Objective**: Establish the Information Technology Executive Council attached to the Office of Information Technology Services for administrative functions.
    - **Council Composition**:
        - **Voting Members (13-17)**:
            - Two cabinet agency heads or designees.
            - Two noncabinet agency heads or designees.
            - Executive Chief Information Technology Officer.
            - Legislative Chief Information Technology Officer.
            - Judicial Chief Information Technology Officer.
            - Chief Executive Officer of the State Board of Regents or designee.
            - One representative of cities.
            - One representative of counties; Network Manager of the Information Network of Kansas (INK).
            - One representative with background in technology and cybersecurity from the private sector (non-vendor).
            - One representative appointed by the Kansas Criminal Justice Information System Committee.
            - Two IT employees from State Board of Regents institutions appointed by the Board of Regents.
            - One senator appointed by the President of the Senate or designee.
            - One senator appointed by the Senate Minority Leader or designee.
            - One House representative appointed by the Speaker of the House or designee.
            - One House representative appointed by the House Minority Leader or designee.
        - **Nonvoting Members**:
            - Chief Information Technology Architect.
            - Legislative Chief Information Technology Officer.
            - Judicial Chief Information Technology Officer.
            - One senator appointed by the President of the Senate.
            - One senator appointed by the Senate Minority Leader.
            - One House representative appointed by the Speaker of the House.
            - One House representative appointed by the House Minority Leader.

Appointment and Terms:

2. **Appointments**:
    - Cabinet and noncabinet agency heads, representatives of cities, counties, and private sector appointed by the governor for a term not exceeding 18 months.
    - Legislative members must remain legislators to retain membership.
    - Vacancies filled in the same manner as the original appointment for the unexpired term.
    - Appointing authority may remove, reappoint, or substitute members at any time.

- Nonappointed members serve ex officio.

Leadership and Meetings:

3. **Leadership**:
    - **Chairperson**: Drawn from the Chief Information Technology Officers, rotating annually among them.
4. **Meetings**:
    - Held quarterly (before July 1, 2026) and monthly (after July 1, 2026) in the city of Topeka or designated locations.
    - Called by the Executive Chief Information Technology Officer or at the request of four or more members.
    - **Quorum**: Seven members before July 1, 2026, and nine members after.

Representation and Voting:

5. **Representation and Voting**:
    - Only specified members may appoint designees.
    - Only council members may vote.

Compensation:

6. **Compensation**:
    - Members receive mileage, tolls, and parking reimbursement as provided in K.S.A. 75-3223 for attending meetings.

Authority and Duties:

7. **Authority**:
    - The Information Technology Executive Council is authorized to adopt policies, rules, and regulations to implement, administer, and enforce the provisions of this act.
8. **Council Duties**:
    - Adopt:
        - Information technology resource policies and procedures and project management methodologies for all state executive branch agencies.
        - An information technology architecture, including telecommunications systems, networks, and equipment, covering all state agencies.
        - Standards for data management for all state executive branch agencies.
        - A strategic information technology management plan for the state executive branch.
    - Provide direction and coordination for the application of the state's executive branch's information technology resources.

- Designate the ownership of information resource processes and the lead executive branch agency for implementing new technologies and networks shared by multiple agencies within the executive branch.
- Develop a plan to integrate all information technology services for the executive branch into the Office of Information Technology Services and all cybersecurity services for state educational institutions into the Office of Information Technology Services and the Kansas Information Security Office.
- Perform other necessary functions and duties to carry out the provisions of this act.

Reporting:

9. **Reporting**:
    - The Information Technology Executive Council shall report the plan developed under subsection (b)(4) to the Senate Standing Committee on Ways and Means and the House Standing Committee on Legislative Modernization or its successor committee prior to January 15, 2026.

Combined Summary of Sections 22 and 23

Sections 22 and 23 establish the Executive Chief Information Technology Officer (ECITO) within the Office of Information Technology Services. Appointed by the governor, the ECITO oversees IT plans, ensures compliance with state standards, and coordinates IT implementation across agencies. They maintain confidentiality, request security assessments, and enforce data center regulations. With a direct line to the governor, this role wields significant authority in shaping and securing the state's technological landscape, ensuring efficiency and safeguarding sensitive information.

Establishment:

1. **Executive Chief Information Technology Officer (ECITO)**:
    - Established within the Office of Information Technology Services.
    - Appointed by the governor, unclassified under the Kansas civil service act.
    - Compensation fixed by the governor.
    - Maintains a presence in any cabinet established by the governor and reports directly to the governor.

Responsibilities:

2. **Review and Consultation**:
    - Review and consult with executive agencies on IT plans, deviations from the state IT architecture, project estimates, and changes to ensure compliance with policies and standards set by the Information Technology Executive Council.
3. **Reporting and Recommendations**:

    - Report deviations from the state information architecture to the Chief Information Technology Architect.
    - Submit recommendations on the technical and management merit of IT projects and changes to the Division of the Budget.
4. **Monitoring and Coordination**:
    - Monitor executive agencies' compliance with IT resource policies, IT architecture, data management standards, and strategic IT management plans.
    - Coordinate the implementation of new IT across executive agencies and with judicial and legislative IT officers.
    - Designate ownership of information resource processes and the lead agency for implementing new technologies and networks shared by multiple agencies within the executive branch.
5. **Legal Consultation**:
    - Consult with legal counsel on topics related to confidentiality, the open records act, the open meetings act, and other legal matters related to IT.
6. **Staffing and Data Centers**:
    - Ensure each executive agency has necessary IT and cybersecurity staff.
    - Maintain all third-party data centers within the US or with US-based companies.
    - Create and maintain an inventory database of all electronic devices within the executive branch.

Confidentiality and Security:

7. **Confidentiality**:
    - Employees of the Office of Information Technology Services must not disclose confidential information of an executive agency.
8. **Security Assessments**:
    - The ECITO may request the Kansas National Guard to perform vulnerability assessments to enhance security, ensuring no harm to systems. The ECITO must notify and coordinate with the executive agency owning the systems being assessed.

Combined Summary of Sections 24 and 25

Sections 24 and 25 of Kansas SB 291 establish the Judicial Chief Information Technology Officer (JCITO) within the Office of the State Judicial Administrator. The JCITO reviews judicial IT plans, ensures compliance, coordinates IT implementation, and manages IT resources. They must ensure necessary IT staffing, maintain US-based data centers, and keep an inventory of electronic devices. Confidentiality is mandatory, and the JCITO can request security assessments from the Kansas National Guard.

Establishment:

1. **Judicial Chief Information Technology Officer (JCITO)**:
    - Established within the Office of the State Judicial Administrator.
    - Appointed by the Judicial Administrator, subject to approval by the Chief Justice.
    - Compensation determined by the Judicial Administrator, subject to approval by the Chief Justice.

Responsibilities:

2. **Review and Consultation**:
    - Review and consult with judicial agencies on IT plans, deviations from the state IT architecture, project estimates, and changes to ensure compliance with policies and procedures adopted by the judicial branch and the Information Technology Executive Council.
3. **Reporting and Recommendations**:
    - Report deviations from the state information architecture to the Chief Information Technology Architect.
    - Submit recommendations to the Judicial Administrator on the technical and management merit of IT projects and changes submitted by judicial agencies.
4. **Monitoring and Coordination**:
    - Monitor judicial agencies' compliance with IT resource policies, IT architecture, data management standards, and strategic IT management plans.
    - Coordinate the implementation of new IT across judicial agencies and with executive and legislative IT officers.
    - Designate ownership of information resource processes and the lead agency for new technologies and networks shared by multiple agencies within the judicial branch.
5. **Staffing and Data Centers**:
    - Ensure each judicial agency has necessary IT and cybersecurity staff.
    - Maintain third-party data centers within the US or with US-based companies.
    - Create and maintain an inventory database of all electronic devices within the judicial branch.

Confidentiality and Security:

6. **Confidentiality**:
    - Employees of the Office of the State Judicial Administrator must not disclose confidential information of a judicial agency.
7. **Security Assessments**:
    - The JCITO may request the Kansas National Guard to perform vulnerability assessments to enhance security, ensuring no harm to systems. The JCITO must notify and coordinate with the judicial agency owning the systems being assessed.

Combined Summary of Sections 26 and 27

Sections 26 and 27. The Legislative Chief Information Technology Officer (LCITO) is established within the legislative branch, tasked with overseeing information technology. Responsibilities include reviewing and consulting on IT plans, ensuring compliance with IT policies and standards, and coordinating IT implementation across legislative agencies. Additionally, the LCITO oversees confidentiality, security assessments, and maintains a database of electronic devices within the legislative branch. They must consult with legal counsel on matters related to IT and ensure each agency has necessary IT staff.

Establishment and Responsibilities:

1. **Legislative Chief Information Technology Officer (LCITO)**:
    - **Role**: Established within the legislative branch to oversee information technology.
    - **Appointment**: Responsibilities include reviewing and consulting with each legislative agency on IT plans, deviations from the state IT architecture, project estimates, and changes.
2. **Responsibilities**:
    - **Review and Consultation**:
        - Ensure compliance with IT resource policies, IT architecture, data management standards, and strategic IT management plans adopted by the Information Technology Executive Council and legislative coordinating council.
    - **Reporting**:
        - Report deviations from the state information architecture to the Chief Information Technology Architect.
    - **Recommendations**:
        - Submit recommendations to the Legislative Coordinating Council on the technical and management merit of IT projects and changes.
    - **Monitoring**:
        - Monitor legislative agencies' compliance with IT policies, architecture, data management standards, and strategic plans.
    - **Coordination**:
        - Coordinate the implementation of new IT across legislative agencies and with executive and judicial IT officers.
    - **Ownership and Implementation**:
        - Designate ownership of information resource processes and the lead agency for new technologies and networks shared by multiple legislative agencies.
    - **Support Role**:
        - Serve as staff of the Joint Committee on Information Technology.
    - **Additional Duties**:
        - Perform other functions and duties as provided by law or directed by the Legislative Coordinating Council or the Joint Committee.
    - **Legal Consultation**:

        - Consult and obtain approval from the Revisor of Statutes on topics related to confidentiality, the Open Records Act, the Open Meetings Act, and other legal matters related to IT.
    - **Staffing**:
        - Ensure each legislative agency has the necessary IT and cybersecurity staff.
    - **Data Centers**:
        - Maintain third-party data centers at locations within the US or with US-based companies.
    - **Device Inventory**:
        - Create and maintain a database of all electronic devices within the legislative branch, ensuring each device is inventoried, cataloged, and tagged.

Confidentiality and Security:

3. **Confidentiality**:
    - Employees of the Kansas Legislative Office of Information Services or the Division of Legislative Administrative Services must not disclose confidential information of a legislative agency.
4. **Security Assessments**:
    - The LCITO may request the Kansas National Guard to perform vulnerability assessments to enhance security. During such assessments, members must ensure no harm is done to the systems being assessed. The LCITO must notify and coordinate with the legislative agency owning the systems being assessed to mitigate the security risk.

Combined Summary of Sections 28 and 29

Sections 28 and 29 establish stringent guidelines for IT project proposals and procurement processes within state agencies. They mandate thorough documentation aligned with state IT policies and standards, especially for projects with significant business risks. The Joint Committee on Information Technology oversees this process, ensuring transparency and accountability. Vendor relationships face scrutiny, with restrictions on contracting to maintain integrity. Annual reporting requirements hold agencies accountable for adherence to strategic IT plans and prompt reporting of deviations.

1. **Project Proposal Requirements**:
    - Agencies must prepare and submit IT project documentation to their respective branch's Chief Information Technology Officer (CITO).
    - Documentation must include a financial plan detailing funding sources and expenditures, and must align with state IT policies, architecture, data management standards, and strategic IT plans.
2. **Significant Business Risk Projects**:
    - Projects with significant business risk must be presented to the Joint Committee on Information Technology by the branch CITO.

3. **Request for Proposal (RFP) Procedures**:
    - Specifications for bids or proposals must be submitted to the branch CITO for approval.
    - Projects requiring CITO approval must also have written approval for RFP specifications.
    - The project plan and cost-benefit analysis must be submitted to the Joint Committee on Information Technology for advisory and consultation purposes.
4. **Advisory and Consultation Process**:
    - Members of the Joint Committee can request a presentation and review of proposed projects.
    - If fewer than two members request a meeting or a meeting is not scheduled within two weeks, the agency may proceed with the RFP release.
5. **Vendor Restrictions**:
    - Agencies cannot contract with vendors who prepared or assisted in the preparation of the project planning documents, unless the project cost is less than $5 million or a waiver is granted by the CITO.
6. **Annual Reporting**:
    - Agencies must submit a three-year strategic IT plan and report any deviations from the state IT architecture to their respective branch CITO.
7. **Exemptions**:
    - The provisions do not apply to the Information Network of Kansas (INK).

Summary of Definitions from Sec. 30 and Sec. 31 of Kansas SB 291:

Section 30 and 31 are more definitions.

- **"Act"**: Refers to the Kansas cybersecurity act.
- **"Breach" or "Breach of Security"**: Unauthorized access to data in electronic form containing personal information. Good faith access by an employee or agent of an executive branch agency does not constitute a breach if the information is not used for unrelated purposes or subject to further unauthorized use.
- **"CISO"**: The executive branch chief information security officer.
- **"Cybersecurity"**: The body of information technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.
- **"Cybersecurity Positions"**: Does not include information technology positions within executive branch agencies.
- **"Data in Electronic Form"**: Any data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.
- **"Executive Branch Agency"**: Any agency in the executive branch of the state of Kansas, including the judicial council but excluding elected office agencies, the adjutant general's department, the Kansas public employees retirement system, regents' institutions, and the board of regents.

- **"KISO"**: The Kansas information security office.
- **"Personal Information"**: includes a name plus a social security number, government ID numbers (e.g., driver's license, passport), financial account numbers with access codes, medical information, health insurance details, and user name/email with password/security question for online accounts. It excludes publicly available information and encrypted or anonymized data.
- **"State Agency"**: Defined as in K.S.A. 75-7201, and amendments thereto.

These definitions provide a foundation for understanding the terminology used in the subsequent sections of the bill.

Combined Summary of Sections 32 and 33 of Kansas SB 291:

Sections 32 and 33. The executive branch establishes the Chief Information Security Officer (CISO) position, reporting to the Chief Information Technology Officer (CITO), tasked with enforcing security standards and policies for IT systems. Responsibilities include ensuring confidentiality, availability, and integrity of data, developing centralized cybersecurity protocols, and overseeing incident response. The CISO develops cybersecurity programs for agencies, ensuring compliance with national standards. Additionally, they provide training, review contracts, and serve as the state's cybersecurity authority, coordinating efforts among agencies and guiding responses to security threats.

- **Establishment and Role**:
    - The position of executive branch Chief Information Security Officer (CISO) is established. The CISO is appointed by the governor, serves in the unclassified service under the Kansas civil service act, and reports to the executive branch Chief Information Technology Officer (CITO).
- **Key Responsibilities**:
    - **Security Standards and Policies**: Establish and enforce security standards and policies to protect the executive branch's IT systems and infrastructure.
    - **Confidentiality, Availability, and Integrity**: Ensure the confidentiality, availability, and integrity of information within the branch's IT systems.
    - **Centralized Cybersecurity Protocol**: Develop a centralized protocol for protecting and managing IT assets and infrastructure.
    - **Incident Detection and Response**: Detect and respond to security incidents according to established standards and policies.
    - **Cybersecurity Oversight**: Oversee the cybersecurity of all executive branch data and information resources.
    - **Inter-Branch Collaboration**: Collaborate with CISOs from other state government branches to respond to cybersecurity incidents.
    - **Training and Compliance**: Ensure annual cybersecurity awareness training for the governor and all executive branch employees. Revoke access for employees who do not complete the training.
    - **Contract Review**: Review IT-related contracts within the executive branch to reduce security vulnerabilities and include standard security language.

- **Program Development**:
    - Develop a cybersecurity program for each executive branch agency that complies with the National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0 by July 1, 2024. Ensure these programs achieve a CSF tier of 3.0 by July 1, 2028, and a CSF tier of 4.0 by July 1, 2030. Agency heads must coordinate with the CISO to meet these standards.
- **Additional Duties**:
    - Serve as the state's CISO and the executive branch's chief cybersecurity strategist and authority on policies, compliance, procedures, guidance, and technologies.
    - Ensure Kansas Information Security Office resources provided to executive branch agencies comply with applicable laws and regulations.
    - Coordinate cybersecurity efforts among executive branch agencies.
    - Provide guidance during security compromises due to high-risk vulnerabilities or threats.
    - Set cybersecurity policies and standards for executive branch agencies.
    - Perform other functions and duties as directed by the executive CITO and as provided by law.

Combined Summary of Sections 34 and 35 of Kansas SB 291:

Sections 34 and 35 of Kansas SB 291 establish the Kansas Information Security Office (KISO) within the Office of Information Technology Services, managed by the executive CISO. KISO is responsible for administering the Kansas Cybersecurity Act, developing and monitoring state security programs, ensuring compliance with laws, coordinating annual audits, managing incident response, and providing cybersecurity staff and training. Audit failures must be reported within 30 days, and audit reports are confidential until July 1, 2028. An IT Security Fund is created for related expenditures.

- **Establishment of Kansas Information Security Office (KISO)**:
    - The KISO is established within the Office of Information Technology Services and administered by the executive CISO. It will be considered a separate state agency for budget purposes and titled "Kansas Information Security Office."
- **Key Responsibilities of KISO under the Executive CISO**:
    - **Administer the Kansas Cybersecurity Act**.
    - **Develop and Monitor Security Programs**: Assist the executive branch in developing, implementing, and monitoring strategic and comprehensive information security risk-management programs.
    - **Information Security Governance**: Facilitate consistent application of information security programs, plans, and procedures.
    - **Unified Control Framework**: Create and manage a control framework to integrate state and federal law requirements.
    - **Metrics and Reporting**: Facilitate a framework to measure the efficiency and effectiveness of state information security programs.
    - **Strategic Risk Guidance**: Provide strategic risk guidance for IT projects, including evaluation and recommendation of technical controls.

    - **Compliance**: Assist in developing executive branch agency cybersecurity programs to ensure compliance with state and federal laws, rules, regulations, and policies.
    - **Annual Audits**: Coordinate with the U.S. Cybersecurity and Infrastructure Security Agency for annual audits of executive branch agencies. Perform audits for compliance with laws, rules, regulations, and policies.
    - **External Resources and Liaison**: Coordinate the use of external resources and liaise with external agencies, such as law enforcement, to maintain a strong security posture.
    - **Incident Management**: Assist in developing plans and procedures to manage and recover business-critical services during cyberattacks or disasters.
    - **Cybersecurity Staff**: Coordinate with executive branch agencies to provide necessary cybersecurity staff.
    - **Training Program**: Ensure a cybersecurity awareness training program is available to all branches of state government.
    - **Other Duties**: Perform other functions as directed by the CISO.
- **Audit Procedures**:
    - Report audit failures to legislative leaders within 30 days, including a mitigation plan. Coordinate additional audits after mitigation and report results.
    - Audit results and reports are confidential and not subject to disclosure under the open records act, with confidentiality expiring on July 1, 2028, unless extended by the legislature.
- **Information Technology Security Fund**:
    - Created in the state treasury for expenditures related to IT security, managed by the executive CISO or a designated person.

Combined Summary of Sections 36 and 37 of Kansas SB 291:

Sections 36 and 37 of Kansas SB 291 mandate that executive branch agency heads are responsible for IT security, must implement security programs, designate security officers, participate in statewide initiatives, and report breaches within 12 hours. They must submit biennial self-assessments and conduct annual internal assessments. Annual cybersecurity training for leadership and staff is required. The CISO develops self-assessment templates and summarizes data for legislative review, with confidentiality until July 1, 2028.

- **Responsibilities of Executive Branch Agency Heads**:
    - Sole responsibility for the security of all data and IT resources under the agency's purview, regardless of location.
    - Ensure an agency-wide information security program is in place and designate an information security officer reporting to executive leadership.
    - Participate in CISO-sponsored statewide cybersecurity initiatives and services.
    - Implement policies and standards to ensure compliance with state and federal laws, and implement cost-effective safeguards against threats.
    - Include appropriate cybersecurity requirements in procurement specifications.

    - Submit a cybersecurity self-assessment report by October 16 of each even-numbered year, conduct annual internal assessments, and prepare financial summaries of cybersecurity expenditures.
    - Notify the CISO and, if relevant, the Secretary of State, within 12 hours of discovering a breach or unauthorized exposure involving personal, confidential, or legally protected information, and comply with notification laws.
- **Annual Leadership Training**:
    - Agency heads must participate in training on the impact of cyberattacks, inter-agency impact, occurrence mechanisms, and protective measures.
    - Ensure IT login credentials are disabled immediately upon an employee's departure and require at least one hour of IT security training per year for all employees with IT access.
- **CISO's Role in Self-Assessment**:
    - Develop a self-assessment report template with input from relevant committees.
    - Aggregate and summarize data from self-assessments for legislative committees.
    - Maintain confidentiality of self-assessment reports, with confidentiality provisions expiring on July 1, 2028, unless extended by the legislature.
- **Kansas Information Security Office (KISO)**:
    - Administer the Kansas Cybersecurity Act and assist in developing and monitoring security programs.
    - Facilitate information security governance and create a unified control framework.
    - Measure the efficiency and effectiveness of state information security programs.
    - Provide strategic risk guidance for IT projects and ensure compliance with laws and policies.
    - Coordinate annual audits and external resources, liaise with external agencies, and assist in developing disaster recovery plans.
    - Ensure a cybersecurity awareness training program is available to all state government branches.