KANSAS OFFICE of
REVISOR of STATUTES
LEGISLATURE of THE STATE of KANSAS
Legislative Attorneys transforming ideas into legislation.

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

MEMORANDUM

To: House Committee on Legislative Modernization

From: Office of Revisor of Statutes

Date: March 15, 2024

Subject: Bill Brief on HB 2842

HB 2842 transfers all information technology services under the chief information technology officer of each branch of government, creates chief information security officers within the judicial and legislative branches, requires a chief information security officer to be appointed by the attorney general, secretary of state, state treasurer and insurance commissioner and requires those chief information security officers to implement certain minimum cybersecurity standards, makes 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, authorizes certain transfers and imposes certain limitations and restrictions, directors or authorizes certain disbursements and procedures for all state agencies and requires legislative review of state agencies not in compliance with this act.

Section 1 provides that on and after July 1, 2027, all information technology services, including cybersecurity services, for each branch of state government shall be administered by the chief information technology officer and the chief information security officer of each branch. All information technology employees within each branch shall work at the direction of the chief information technology officer, except that each state agency that maintains confidential information may maintain one employee to assist with the information technology related to such information. Prior to July 1, 2026, the chief information technology officer of each branch is required to develop a plan to integrate all information technology services under the officer. The executive branch chief information technology officer is required to consult with each cabinet agency head when developing such plan. The judicial chief information technology officer is required to develop an estimated project cost to provide hardware to state and county employees in each judicial district who access applications administered by the judicial branch.

Such officer is also required to consult with the executive chief information technology officer to develop a plan to allow each piece of hardware to be a part of the KANWIN network. The legislative chief information technology officer is required to consult with each legislative agency head. Each chief information technology officer shall report the plans developed to the senate standing committee on ways and means and the house standing committee on legislative modernization prior to January 15, 2026. Prior to January 1, 2025, all websites maintained by a branch of government or state agency shall be moved to the ".gov" domain. On July 1, 2025, and each year thereafter, moneys appropriated for information technology and cybersecurity expenditures shall be appropriated as a separate line item and shall not be merged with other items of appropriation to allow for a detailed review of each appropriation.

Sections 2 and 3 create chief information technology officers within the judicial and legislative branches. The judicial CISO will be appointed by the judicial administrator subject to approval by the chief justice, and the legislative CISO will be appointed by the legislative coordinating council. Such officers will be required to (1) report to their respective CITO, (2) establish security standards and policies for the branch, (3) ensure the confidentiality, availability and integrity of branch information technology systems and infrastructure, (4) develop a centralized cybersecurity protocol, (5) detect and respond to security incidents, (6) be responsible for the security of all branch data and information resources, (7) create a database to inventory all branch devices and tag them with inventory devices, (8) ensure all employees of the branch (including justices, judges and legislators) complete cybersecurity training annually, (9) maintain third-party data centers in the United States or with United States-based companies, (10) review all contracts related to information technology to ensure there are no security vulnerabilities, and (11) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the branch. The CISO of each branch shall develop a cybersecurity program for each agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. If an audit conducted results in a failure, the CISO shall report such failure to the speaker of the house and the president of the senate with a plan to mitigate security risks. These audit results are confidential and not subject to the open records act. The legislative CISO is required to obtain approval from the revisor of statutes prior to taking any action on any matter that involves a legal issue.

Section 4 provides that on July 1, 2028, and each year after, the director of the budget, in consultation with each CITO shall determine if each state agency is in compliance with the

provisions of this act for the previous fiscal year. If the director of the budget determines that a state agency is not in compliance, the director shall certify an amount equal to 5% of the money appropriated and reappropriated from the state general fund and credited to and available in each special revenue fund of the noncomplying state agency. The director of the budget shall submit a detailed written report to the legislature before the regular session concerning such compliance determinations and during such regular session, the house appropriations committee and senate ways and means committee shall consider whether to lapse amounts appropriated and reappropriated and decrease expenditure limitations for such noncomplying state agencies.

Section 5 appropriates $65,000,000 to the office of information technology services for fiscal year 2026. The director of the budget shall determine the amount of money from each account and special revenue fund during fiscal years 2021 through 2025 that each executive branch agency has expended for services performed by the office of information technology services or the Kansas information security office, determine the five-year average, and certify the amount to the director of accounts and reports who shall lapse the amount from such account and transfer the amount from such special revenue fund to the information technology fund.

Sections 6 and 7 appropriate the information technology security fund within the Kansas information security office for fiscal years 2025 and 2026 as a no limit fund.

Section 8 appropriates $250,000 to the operating expenditures account of the adjutant general for fiscal year 2025, for two full-time employees in the Kansas intelligence fusion center to assist in monitoring state information technology systems.

Section 9 amends K.S.A. 40-110 to require the commissioner of insurance to appoint a chief information security officer who shall develop a cybersecurity program for the department that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The CISO shall also ensure that the commissioner and all employees complete cybersecurity training annually and coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits, the results of which shall be confidential and not subject to the open records act.

Section 10 amends K.S.A. 45-229 to exempt reports of results of audits conducted by the United States cybersecurity and infrastructure security agency from the requirement that each new open records exception expire five years after its creation unless reviewed and continued into existence by the legislature prior to its expiration.

Section 11 amends K.S.A. 75-413 to require the secretary of state to appoint a chief information security officer who shall develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The CISO shall also ensure that the secretary of state and all employees complete cybersecurity training annually and coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits, the results of which shall be confidential and not subject to the open records act.

Section 12 amends K.S.A. 75-623 to require the treasurer to appoint a chief information security officer who shall develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The CISO shall also ensure that the treasurer and all employees complete cybersecurity training annually and coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits, the results of which shall be confidential and not subject to the open records act.

Section 13 amends K.S.A. 75-710 to require the attorney general to appoint a chief information security officer who shall develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The CISO shall also ensure that the attorney general and all employees complete cybersecurity training annually and coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits, the results of which shall be confidential and not subject to the open records act.

Section 14 amends K.S.A. 75-7203, the statute that provides duties of the information technology executive council. The section is amended to remove all current law duties and provide that the council shall meet as it deems necessary to discuss information technology policies and procedures.

Section 15 amends K.S.A. 75-7205, the statute that creates the executive chief information technology officer. The duties of the officer are amended to require that the officer consult with the appropriate legal counsel on topics related to confidentiality of information, the open records act, the open meetings act and any other legal matter related to information technology and to ensure that each executive agency has the necessary information technology

and cybersecurity staff imbedded within the agency. An employee of the CITO shall not disclose confidential information of an agency, and violation is a severity level 5, nonperson felony. The executive CITO shall make a request to the adjutant general to permit the 184th wing cyber operations group to practice a white hat hack of the branch and shall notify the agency that owns the information of the hack.

Section 16 amends K.S.A. 75-7206, the statute that creates the judicial chief information technology officer. The duties of the officer are amended to ensure that each executive agency has the necessary information technology and cybersecurity staff imbedded within the agency. An employee of the CITO shall not disclose confidential information of an agency, and violation is a severity level 5, nonperson felony. The judicial CITO shall make a request to the adjutant general to permit the 184th wing cyber operations group to practice a white hat hack of the branch and shall notify the agency that owns the information of the hack.

Section 17 amends K.S.A. 75-7208, the statute that creates the legislative chief information technology officer. The duties of the officer are amended to require that the officer consult and obtain approval from the revisor of statutes prior to taking action on topics related to confidentiality of information, the open records act, the open meetings act and any other legal matter related to information technology and to ensure that each legislative agency has the necessary information technology and cybersecurity staff imbedded within the agency. An employee of the legislative office of information services or the division of legislative administrative services shall not disclose confidential information of an agency, and violation is a severity level 5, nonperson felony. The legislative CITO shall make a request to the adjutant general to permit the 184th wing cyber operations group to practice a white hat hack of the branch and shall notify the agency that owns the information of the hack.

Section 18 amends K.S.A. 75-7238, the statute that creates the executive chief information security officer. The duties of the officer are amended to match the duties of the new judicial and legislative chief information security officers. They are to (1) report to the executive CITO, (2) establish security standards and policies for the branch, (3) ensure the confidentiality, availability and integrity of branch information technology systems and infrastructure, (4) develop a centralized cybersecurity protocol, (5) detect and respond to security incidents, (6) be responsible for the security of all branch data and information resources, (7) create a database to inventory all branch devices and tag them with inventory devices, (8) ensure all employees of the branch (including the governor) complete cybersecurity training annually, (9) maintain third-party data centers in the United States or with United States-based companies, and (10) review

all contracts related to information technology to ensure there are no security vulnerabilities. The executive CISO shall develop a cybersecurity program for each agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0. Such programs shall be required to achieve a score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030.

Section 19 amends K.S.A. 75-7239, the statute that creates the Kansas information security office. The duties of the KISO are amended to require that the office (1) administer the Kansas cybersecurity act, (2) develop, implement and monitor information security risk-management programs, (3) facilitate a framework to measure the efficiency and effectiveness of information security programs, (4) provide the executive branch guidance for information technology projects, (5) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits, the results of which shall be confidential and not subject to the open records act, (6) coordinate the use of external resources including negotiating contracts and fees, (7) liaise with external agencies, (8) assist in developing a plan to manage services in the event of a cyberattack, (9) coordinate with executive branch agencies to provide staff, (10) ensure cybersecurity awareness training is available to all branches of state government, and (11) perform other functions and duties as directed by the executive CISO. If an audit conducted results in a failure, the CISO shall report such failure to the speaker of the house and the president of the senate with a plan to mitigate security risks. Subsection (e) creates the information technology security fund. All expenditures shall be made as approved by the executive CISO.

Finally, Section 20 amends K.S.A. 75-7240, the statute that provides duties of each executive branch agency head related to information technology. Most current law duties, including the duty to perform a cybersecurity self-assessment, are removed to allow the executive CITO and CISO to take over most information technology duties, and each agency head will be required to coordinate with the executive CISO to implement the security standards described in K.S.A. 75-7238.