Proposed Amendments to HB 2842 - judicial branch
House Legislative Modernization Committee
Prepared by the Office of Revisor of Statutes
March 18, 2024

1

Session of 2024

HOUSE BILL No. 2842

By Committee on Appropriations

Requested by Representative B. Carpenter

3-15

AN ACT concerning information technology; relating to transferring information technology employees under the chief information technology officer of each branch; creating a chief information security officer within the judicial and legislative branches; requiring the attorney general, secretary of state, state treasurer and insurance commissioner to appoint chief information technology officers; placing the duty of cybersecurity under the chief information technology officer; requiring state agencies to comply with certain minimum cybersecurity standards; exempting certain audit reports from the open records act and eliminating the five-year review of such exemption; 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; legislative review of state agencies not in compliance with this act; amending K.S.A. 40-110, 75-413, 75-623, 75-710 and 75-7203 and K.S.A. 2023 Supp. 45-229, 75-7205, 75-7206, 75-7208, 75-7238, 75-7239 and 75-7240 and repealing the existing sections.

75-7201,

75-7237,

Be it enacted by the Legislature of the State of Kansas:

Section 1. (a) 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 such branch. All information technology employees within each branch of state government shall work at the direction of the chief information technology officer of the branch, except that each state agency that maintains confidential information, including, but not limited to, legal, healthcare or tax information may maintain one employee to assist with the information technology related to such information.

(b) Prior to January 1, 2026:

(1) The executive chief information technology officer shall develop a plan to integrate all information technology services into the office of information technology services. The executive chief information

technology officer shall consult with each cabinet agency head when developing such plan.

(2) The judicial chief information technology officer shall develop a plan to integrate all information technology services into the office of the state judicial administrator. The judicial chief information technology officer shall develop an estimated project cost to provide information technology hardware to state and county employees in each judicial district who access applications administered by the judicial branch. Such employees shall be required to use such state issued information technology hardware to access such applications. The judicial chief information technology officer shall consult with the executive chief information technology officer to develop a plan to allow each piece of information technology hardware that is used to access an application administered by the judicial branch to be part of the KANWIN network prior to July 1, 2027.

(3) The legislative chief information technology officer shall develop a plan to integrate all information technology services under the legislative chief information technology officer. The legislative chief information technology officer shall consult with each legislative agency head when developing such plan.

(c) Each chief information technology officer shall report the plan developed pursuant to subsection (b) 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.

February

(d) Prior to ~~January~~ 1, 2025, every website that is maintained by a branch of government or state agency shall be moved to a ".gov" domain.

(e) On July 1, 2025, and each year thereafter, moneys appropriated from the state general fund to or any special revenue fund of any state agency for information technology and cybersecurity expenditures shall be appropriated as a separate line item and shall not be merged with other items of appropriation for such state agency to allow for detailed review by the senate committee on ways and means and the house of representatives committee on appropriations during each regular legislative session.

Sec. 2. (a) There is hereby established the position of judicial branch chief information security officer. The judicial chief information security officer shall be in the unclassified service under the Kansas civil service act, shall be appointed by the judicial administrator, subject to approval by the chief justice and shall receive compensation determined by the judicial administrator, subject to approval of the chief justice.

(b) The judicial chief information security officer shall:

(1) Report to the judicial ~~branch chief information technology officer~~;

administrator

(2) establish security standards and policies to protect the branch's

information technology systems and infrastructure in accordance with subsection (c);

(3) ensure the confidentiality, availability and integrity of the information transacted, stored or processed in the branch's information technology systems and infrastructure;

(4) develop a centralized cybersecurity protocol for protecting and managing judicial branch information technology assets and infrastructure;

(5) detect and respond to security incidents consistent with information security standards and policies;

(6) be responsible for the security of all judicial branch data and information resources;

(7) create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged and tagged with an inventory device;

(8) ensure that all justices, judges and judicial branch employees complete cybersecurity awareness training annually and if an employee does not complete the required training, such employee's access to any state issued hardware or the state network is revoked;

(9) maintain all third-party data centers at locations within the United States or with companies that are based in the United States;

(10) review all contracts ~~related to information~~ technology entered into by a ~~person or entity~~ within the judicial branch to ~~ensure that there are no~~ security vulnerabilities within the supply chain or product and ~~each~~ contract contains standard security language; and

make efforts to reduce the risk of

ensure

(11) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of judicial branch agencies for compliance with applicable state and federal laws, rules and regulations and judicial branch policies and standards. The judicial chief information security officer shall make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

(c) The judicial chief information security officer shall develop a cybersecurity program of each judicial agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The judicial chief information security officer shall ensure that such programs achieve a national institute of standards and technology score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The agency head of each judicial agency shall coordinate with the executive chief information security officer to achieve such standards.

(d) (1) If an audit conducted pursuant to subsection (b)(11) results in a failure, the judicial chief information security officer shall report such failure to the speaker of the house of representatives and the president of

make efforts to reduce the risk of

ensure

into by a person ~~or entity within~~ the legislative branch to ~~ensure that there are no~~ security vulnerabilities within the supply chain or product and each contract contains standard security language; and

(11) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of legislative branch agencies for compliance with applicable state and federal laws, rules and regulations and legislative branch policies and standards. The legislative chief information security officer shall make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

(c) The legislative chief information security officer shall develop a cybersecurity program of each legislative agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The legislative chief information security officer shall ensure that such programs achieve a national institute of standards and technology score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The agency head of each legislative agency shall coordinate with the legislative chief information security officer to achieve such standards.

(d) (1) If an audit conducted pursuant to subsection (b)(11) results in a failure, the legislative chief information security officer shall report such failure to the speaker of the house of representatives and the president of the senate within 30 days of receiving notice of such failure. Such report shall contain a plan to mitigate any security risks identified in the audit. The legislative chief information security officer shall coordinate for an additional audit after the mitigation plan is implemented and report the results of such audit to the speaker of the house of representatives and the president of the senate.

(2) Results of audits conducted pursuant to subsection (b)(11) and the reports described in subsection (d)(1) shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

Sec. 4. (a) On July 1, 2028, and each year thereafter, the director of the budget, in consultation with the legislative, executive and judicial chief information technology officers as appropriate, 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 with the provisions of this act for such fiscal year, the director shall certify an amount equal to 5% of the amount:

(1) Appropriated and reappropriated from the state general fund for such state agency for such fiscal year; and

(2) credited to and available in each special revenue fund for such state agency in such fiscal year. If during any fiscal year, a special revenue

reports until a verified account of the fees collected by them, or either of them, during the preceding month, has been filed in the director of accounts and reports' office. Assistants appointed by the attorney general shall perform the duties and exercise the powers as prescribed by law and shall perform other duties as prescribed by the attorney general. Assistants shall act for and exercise the power of the attorney general to the extent the attorney general delegates them the authority to do so.

(b) The attorney general shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the office's information technology systems and infrastructure. The chief information security officer shall:

(1) Develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a national institute of standards and technology score of 3.0 prior to July 1, 2028, and a score of 4.0 prior to July 1, 2030;

(2) ensure that the attorney general and all employees complete cybersecurity awareness training annually and that if an employee does not complete the required training, such employee's access to any state issued hardware or the state network is revoked; and

(3) (A) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the office for compliance with applicable state and federal laws, rules and regulations and office policies and standards;

(B) make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit; and

(C) results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

Sec. 14. K.S.A. 75-7203 is hereby amended to read as follows: 75-7203. (a) The information technology executive council ~~is hereby authorized to adopt such policies and rules and regulations as necessary to implement, administer and enforce the provisions of this act.~~

~~(b) The council~~ shall:

~~(1) Adopt: (A) Information technology resource policies and procedures and project management methodologies for all state agencies; (B) an information technology architecture, including telecommunications systems, networks and equipment, that covers all state agencies; (C) standards for data management for all state agencies; and (D) a strategic information technology management plan for the state;~~

~~(2) provide direction and coordination for the application of the~~

Sec. 14. K.S.A. 75-7201 is hereby amended to read as follows: 75-7201. As used in K.S.A. 75-7201 through 75-7212, and amendments thereto:

(a) "Business risk" means the overall level of risk determined by a business risk assessment that includes, but is not limited to, cost, information security and other elements as determined by the information technology executive council's policies.

(b) "Cumulative cost" means the total expenditures, from all sources, for any information technology project by one or more state agencies to meet project objectives from project start to project completion or the date and time the project is terminated if it is not completed.

(c) "Executive agency" means any state agency in the executive branch of government including the judicial council, but does not include elected office agencies.

(d) "Information technology project" means an information technology effort by a state agency of defined and limited duration that implements, effects a change in or presents a risk to processes, services, security, systems, records, data, human resources or architecture.

(e) "Information technology project change or overrun" means any change in:

(1) Planned expenditures for an information technology project that would result in the total authorized cost of the project being increased above the currently authorized cost of such project by more than 10% of such currently authorized cost of such project or an established threshold within the information technology executive council's policies;

(2) the scope or project timeline of an information technology project, as such scope or timeline was presented to and reviewed by the joint committee or the chief information technology officer to whom the project was submitted pursuant to K.S.A. 75-7209, and amendments thereto, that is a change of more than 10% or a change that is significant as determined by the information technology executive council's policies; or

(3) the proposed use of any new or replacement information technology equipment or in the use of any existing information technology equipment that has been significantly upgraded.

(f) "Joint committee" means the joint committee on information technology.

(g) "Judicial agency" means any state agency in the judicial branch of government.

(h) "Legislative agency" means any state agency in the legislative branch of government.

(i) "Project" means a planned series of events or activities that is intended to accomplish a specified outcome in a specified time period, under consistent management direction within a state agency or shared among two or more state agencies, and that has an identifiable budget for anticipated expenses.

(j) "Project completion" means the date and time when the head of a state agency having primary responsibility for an information technology project certifies that the improvement being produced or altered under the project is ready for operational use.

(k) "Project start" means the date and time when a state agency begins a formal study of a business process or technology concept to assess the needs of the state agency, determines project feasibility or prepares an information technology project budget estimate under K.S.A. 75-7209, and amendments thereto.

(l) "State agency" means any state office or officer, department, board, commission, institution or bureau, or any agency, division or unit thereof.

~~(4)~~*(D)* strategic information technology management plan adopted by the information technology executive council;

~~(e)~~*(5)* coordinate implementation of new information technology among legislative agencies and with the executive and judicial chief information technology officers;

~~(f)~~*(6)* designate the ownership of information resource processes and the lead agency for implementation of new technologies and networks shared by multiple agencies within the legislative branch of state government;

~~(g)~~*(7)* serve as staff of the joint committee; ~~and~~

~~(h)~~*(8)* perform such other functions and duties as provided by law or as directed by the legislative coordinating council or the joint committee*;*

(9) consult and obtain approval from the revisor of statutes prior to taking action on topics related to confidentiality of information, the open records act, K.S.A. 45-215 et seq., and amendments thereto, the open meetings act, K.S.A. 75-4317 et seq., and amendments thereto, and any other legal matter related to information technology; and

(10) ensure that each legislative agency has the necessary information technology and cybersecurity staff imbedded within the agency to accomplish the agency's duties.

(b) An employee of the Kansas legislative office of information services or the division of legislative administrative services shall not disclose confidential information of a legislative agency. Violation of this subsection is a severity level 5, nonperson felony.

(c) The legislative chief information technology officer may make a request to the adjutant general to permit the 184th wing cyber operations group to practice and white hat hack the branch for the purpose of enhancing security. Such hack shall not harm or shutdown any critical infrastructure. The legislative chief information technology officer shall notify the legislative agency that owns the information that is hacked about such white hat hack and coordinate to mitigate the security risk.

Sec. 18. K.S.A. 2023 Supp. 75-7238 is hereby amended to read as follows: 75-7238. (a) There is hereby established the position of executive branch chief information security officer *(CISO)*. The *executive* CISO shall be in the unclassified service under the Kansas civil service act, shall be appointed by the governor and shall receive compensation in an amount fixed by the governor.

(b) The *executive* CISO shall:

(1) Report to the executive branch chief information technology officer;

(2) ~~serve as the state's CISO;~~

~~(3) serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance and technologies~~

Sec. 18. K.S.A. 2023 Supp. 75-7237 is hereby amended to read as follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and amendments thereto:

(a) "Act" means the Kansas cybersecurity act.

(b) "Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(c) "CISO" means the executive branch chief information security officer.

(d) "Cybersecurity" is the body of information technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

(e) "Cybersecurity positions" do not include information technology positions within executive branch agencies.

(f) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(g) "Executive branch agency" means any agency in the executive branch of the state of Kansas including the judicial council, but does not include elected office agencies, the adjutant general's department, ~~the Kansas public employees retirement system,~~ regents' institutions, or the board of regents.

(h) "KISO" means the Kansas information security office.

(i) (1) "Personal information" means:

(A) An individual's first name or first initial and last name, in combination with at least one of the following data elements for that individual:

(i) Social security number;

(ii) driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity;

(iii) financial account number or credit or debit card number, in combination with any security code, access code or password that is necessary to permit access to an individual's financial account;

(iv) any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional; or

(v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or

(B) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(2) "Personal information" does not include information:

(A) About an individual that has been made publicly available by a federal agency, state agency or municipality; or

(B) that is encrypted, secured or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(j) "State agency" means the same as defined in K.S.A. 75-7201, and amendments thereto.

~~impacting executive branch cybersecurity programs;~~

~~(4) ensure Kansas information security office resources assigned or provided to executive branch agencies are in compliance with applicable laws and rules and regulations;~~

~~(5) coordinate cybersecurity efforts between executive branch agencies;~~

~~(6) provide guidance to executive branch agencies when compromise of personal information or computer resources has occurred or is likely to occur as the result of an identified high-risk vulnerability or threat;~~

~~(7) set cybersecurity policy and standards for executive branch agencies; and~~

~~(8) perform such other functions and duties as provided by law and as directed by the executive chief information technology officer~~*establish security standards and policies to protect the branch's information technology systems and infrastructure in accordance with subsection (c);*

(3) ensure the confidentiality, availability and integrity of the information transacted, stored or processed in the branch's information technology systems and infrastructure;

(4) develop a centralized cybersecurity protocol for protecting and managing executive branch information technology assets and infrastructure;

(5) detect and respond to security incidents consistent with information security standards and policies;

(6) be responsible for the security of all executive branch data and information resources;

(7) create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged and tagged with an inventory device;

(8) ensure that the governor and all executive branch employees complete cybersecurity awareness training annually and that if an employee does not complete the required training such employee's access to any state issued hardware or the state network is revoked;

(9) maintain all third-party data centers at locations within the United States or with companies that are based in the ~~United~~ States; and

(10) review all contracts ~~related to~~ information technology entered into by a ~~person or entity~~ within the executive branch to ~~ensure that there are no~~ security vulnerabilities within the supply chain or product and each contract contains standard security language.

(c) The executive CISO shall develop a cybersecurity program for each executive agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The executive CISO shall ensure that such programs achieve a national institute of standards and technology score of 3.0 prior

make efforts to reduce the risk of

ensure

~~the Kansas open records act, K.S.A. 45-215 et seq., and amendments thereto. The provisions of this paragraph shall expire on July 1, 2028, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.~~

Sec. 21. K.S.A. 40-110, ~~75-413, 75-623,~~ 75-710 and ~~75-7203~~ and K.S.A. 2023 Supp. 45-229, ~~75-7205,~~ 75-7206, ~~75-7208, 75-7238,~~ 75-7239 and 75-7240 are hereby repealed.

75-7201,

75-7237,

Sec. 22. This act shall take effect and be in force from and after its publication in the statute book.