Session of 2024

House Substitute for SENATE BILL No. 291

By Committee on Legislative Modernization

3-22

AN ACT concerning information technology; relating to transferring cybersecurity 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, Kansas bureau of investigation, secretary of state, state treasurer and insurance commissioner to appoint chief information security 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; requiring the information technology executive council to develop a plan to integrate all information technology services for the executive branch 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; requiring legislative review of state agencies not in compliance with this act; amending K.S.A. 40-110, 75-413, 75-623, 75-710, 75-711 and 75-7203 and K.S.A. 2023 Supp. 45-229, 75-7201, 75-7202, 75-7205, 75-7206, 75-7208, 75-7209, 75-7237, 75-7238, 75-7239 and 75-7240 and repealing the existing sections.

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

New Section 1. (a) On and after July 1, 2027, all 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 cybersecurity employees within each branch of state government shall work at the direction of the chief information technology officer of the branch. The provisions of this subsection do not apply to the regents' institutions.

(b) Prior to January 1, 2026:

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

with each agency head when developing such plan.

(2) 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.

(c) The information technology executive council 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.

(d) Prior to February 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.

New 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 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 cybersecurity of all judicial branch data and information resources;

(7) collaborate with the chief information security officers of the other branches of state government to respond to cybersecurity incidents;

(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) review all contracts related to information technology entered into by a person or entity within the judicial branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure each contract contains standard security language; and

(10) 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier 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)(10) 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 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 judicial 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)(10) 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.

New Sec. 3. (a) There is hereby established the position of legislative branch chief information security officer. The legislative chief information security officer shall be in the unclassified service under the Kansas civil

service act, shall be appointed by the legislative coordinating council and shall receive compensation determined by the legislative coordinating council.

(b) The legislative chief information security officer shall:

(1) Report to the legislative chief information technology officer;

(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 legislative 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 cybersecurity of all legislative branch data and information resources and obtain approval from the revisor of statutes prior to taking any action on any matter that involves a legal issue related to the security of information technology;

(7) collaborate with the chief information security officers of the other branches of state government to respond to cybersecurity incidents;

(8) ensure that all legislators and legislative 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) review all contracts related to information technology entered into by a person or entity within the legislative branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure each contract contains standard security language; and

(10) 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier 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)(10) 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)(10) 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.

New 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 fund has no expenditure limitation, then an expenditure limitation shall be established for such fiscal year on such special revenue fund by the director of the budget in an amount that is 5% less than the amount of moneys credited to and available in such special revenue fund for such fiscal year.

(b) The director of the budget shall submit a detailed written report to the legislature on or before the first day of the regular session of the legislature concerning such compliance determinations, including factors considered by the director when making such determination, and the amounts certified for each state agency for such fiscal year.

(c) During the regular session of the legislature, the senate committee on ways and means and the house of representatives committee on appropriations shall consider such compliance determinations and whether to lapse amounts appropriated and reappropriated and decrease the expenditure limitations of special revenue funds for such state agencies during the budget committee hearings for such noncomplying agency.

New Sec. 5.

OFFICE OF INFORMATION TECHNOLOGY SERVICES

(a) There is appropriated for the above agency from the state general fund for the fiscal year ending June 30, 2026, the following:

Kansas information technology office (335-00-1000).....$15,000,000

(b) During fiscal year 2026, the director of the budget, in consultation with the executive branch chief information technology officer and executive branch chief information security officer, shall determine the amount of moneys from the state general fund and each special revenue fund that each executive branch agency has expended during fiscal years 2021 through 2025 for services performed by the Kansas information security office or other cybersecurity services for such state agency: *Provided,* That the director of the budget shall determine such five-year average of each state agency's expenditures from the state general fund and each special revenue fund: *Provided further,* That during fiscal year 2026, the director of the budget shall certify the amount so determined to the director of accounts and reports and, at the same time as such certification is transmitted to the director of accounts and reports, shall transmit a copy of such certification to the director of legislative research: *And provided further,* That upon receipt of each such certification, the director of accounts and reports shall: (1) For the amounts from the state general fund, lapse such funds; and (2) for each special revenue fund, transfer the amount from the special revenue fund of the state agency to the information technology security fund established in K.S.A. 75-7239, and amendments thereto.

New Sec. 6.

KANSAS INFORMATION SECURITY OFFICE

(a) There is appropriated for the above agency from the following special revenue fund or funds for the fiscal year ending June 30, 2025, all moneys now or hereafter lawfully credited to and available in such fund or funds, except that expenditures other than refunds authorized by law shall not exceed the following:

Information technology security fund.....No limit

New Sec. 7.

KANSAS INFORMATION SECURITY OFFICE

(a) There is appropriated for the above agency from the following special revenue fund or funds for the fiscal year ending June 30, 2026, all moneys now or hereafter lawfully credited to and available in such fund or funds, except that expenditures other than refunds authorized by law shall not exceed the following:

Information technology security fund.....No limit

New Sec. 8.

ADJUTANT GENERAL

(a) There is appropriated for the above agency from the state general fund for the fiscal year ending June 30, 2025, the following:
Operating expenditures (034-00-1000-0053).....$250,000
Provided, That expenditures shall be made by the above agency from such account for two full-time employees in the Kansas intelligence fusion center to assist in monitoring state information technology systems: *Provided further,* That such employees shall be in the unclassified service of the civil service act and shall be in addition to the positions of the above agency as authorized pursuant to K.S.A. 2023 Supp. 48-3706, and amendments thereto.

Sec. 9. K.S.A. 40-110 is hereby amended to read as follows: 40-110. (a) The commissioner of insurance is hereby authorized to appoint an assistant commissioner of insurance, actuaries, two special attorneys who shall have been regularly admitted to practice, an executive secretary, policy examiners, two field representatives, and a secretary to the commissioner. Such appointees shall each receive an annual salary to be determined by the commissioner of insurance, within the limits of available appropriations. The commissioner is also authorized to appoint, within the provisions of the civil service law, and available appropriations, other employees as necessary to administer the provisions of this act. The field representatives authorized by this section may be empowered to conduct inquiries, investigations or to receive complaints. Such field representatives shall not be empowered to make, or direct to be made, an examination of the affairs and financial condition of any insurance company in the process of organization, or applying for admission or doing business in this state.

(b) The appointees authorized by this section shall take the proper official oath and shall be in no way interested, except as policyholders, in any insurance company. In the absence of the commissioner of insurance the assistant commissioner shall perform the duties of the commissioner of insurance, but shall in all cases execute papers in the name of the commissioner of insurance, as assistant. The commissioner of insurance shall be responsible for all acts of an official nature done and performed by the commissioner's assistant or any person employed in such office. All the appointees authorized by this section shall hold their office at the will and pleasure of the commissioner of insurance.

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

(1) Develop a cybersecurity program for the department 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

(2) ensure that the commissioner 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) (i) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the department for compliance with applicable state and federal laws, rules and regulations and department policies and standards; and

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

(B) 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. 10. K.S.A. 2023 Supp. 45-229 is hereby amended to read as follows: 45-229. (a) It is the intent of the legislature that exceptions to disclosure under the open records act shall be created or maintained only if:

(1) The public record is of a sensitive or personal nature concerning individuals;

(2) the public record is necessary for the effective and efficient administration of a governmental program; or

(3) the public record affects confidential information.

The maintenance or creation of an exception to disclosure must be compelled as measured by these criteria. Further, the legislature finds that the public has a right to have access to public records unless the criteria in this section for restricting such access to a public record are met and the criteria are considered during legislative review in connection with the particular exception to disclosure to be significant enough to override the strong public policy of open government. To strengthen the policy of open government, the legislature shall consider the criteria in this section before enacting an exception to disclosure.

(b) Subject to the provisions of subsections (g) and (h), any new exception to disclosure or substantial amendment of an existing exception shall expire on July 1 of the fifth year after enactment of the new exception or substantial amendment, unless the legislature acts to continue the exception. A law that enacts a new exception or substantially amends an existing exception shall state that the exception expires at the end of five years and that the exception shall be reviewed by the legislature before the scheduled date.

(c) For purposes of this section, an exception is substantially amended if the amendment expands the scope of the exception to include more records or information. An exception is not substantially amended if the amendment narrows the scope of the exception.

(d) This section is not intended to repeal an exception that has been amended following legislative review before the scheduled repeal of the exception if the exception is not substantially amended as a result of the review.

(e) In the year before the expiration of an exception, the revisor of statutes shall certify to the president of the senate and the speaker of the house of representatives, by July 15, the language and statutory citation of each exception that will expire in the following year that meets the criteria of an exception as defined in this section. Any exception that is not identified and certified to the president of the senate and the speaker of the house of representatives is not subject to legislative review and shall not expire. If the revisor of statutes fails to certify an exception that the revisor subsequently determines should have been certified, the revisor shall include the exception in the following year's certification after that determination.

(f) "Exception" means any provision of law that creates an exception to disclosure or limits disclosure under the open records act pursuant to K.S.A. 45-221, and amendments thereto, or pursuant to any other provision of law.

(g) A provision of law that creates or amends an exception to disclosure under the open records law shall not be subject to review and expiration under this act if such provision:

(1) Is required by federal law;

(2) applies solely to the legislature or to the state court system;

(3) has been reviewed and continued in existence twice by the legislature; ~~or~~

(4) has been reviewed and continued in existence by the legislature during the 2013 legislative session and thereafter*; or*

(5) is a report of the results of an audit conducted by the United States cybersecurity and infrastructure security agency.

(h) (1) The legislature shall review the exception before its scheduled expiration and consider as part of the review process the following:

(A) What specific records are affected by the exception;

(B) whom does the exception uniquely affect, as opposed to the general public;

(C) what is the identifiable public purpose or goal of the exception;

(D) whether the information contained in the records may be obtained readily by alternative means and how it may be obtained;

(2) an exception may be created or maintained only if it serves an

identifiable public purpose and may be no broader than is necessary to meet the public purpose it serves. An identifiable public purpose is served if the legislature finds that the purpose is sufficiently compelling to override the strong public policy of open government and cannot be accomplished without the exception and if the exception:

(A) Allows the effective and efficient administration of a governmental program that would be significantly impaired without the exception;

(B) protects information of a sensitive personal nature concerning individuals, the release of such information would be defamatory to such individuals or cause unwarranted damage to the good name or reputation of such individuals or would jeopardize the safety of such individuals. Only information that would identify the individuals may be excepted under this paragraph; or

(C) protects information of a confidential nature concerning entities, including, but not limited to, a formula, pattern, device, combination of devices, or compilation of information that is used to protect or further a business advantage over those who do not know or use it, if the disclosure of such information would injure the affected entity in the marketplace.

(3) Records made before the date of the expiration of an exception shall be subject to disclosure as otherwise provided by law. In deciding whether the records shall be made public, the legislature shall consider whether the damage or loss to persons or entities uniquely affected by the exception of the type specified in paragraph (2)(B) or (2)(C) would occur if the records were made public.

(i) (1) Exceptions contained in the following statutes as continued in existence in section 2 of chapter 126 of the 2005 Session Laws of Kansas and that have been reviewed and continued in existence twice by the legislature as provided in subsection (g) are hereby continued in existence: 1-401, 2-1202, 5-512, 9-1137, 9-1712, 9-2217, 10-630, 12-189, 12-1,108, 12-1694, 12-1698, 12-2819, 12-4516, 16-715, 16a-2-304, 17-1312e, 17-2227, 17-5832, 17-7511, 17-76,139, 19-4321, 21-2511, 22-3711, 22-4707, 22-4909, 22a-243, 22a-244, 23-605, 23-9,312, 25-4161, 25-4165, 31-405, 34-251, 38-2212, 39-709b, 39-719e, 39-934, 39-1434, 39-1704, 40-222, 40-2,156, 40-2c20, 40-2c21, 40-2d20, 40-2d21, 40-409, 40-956, 40-1128, 40-2807, 40-3012, 40-3304, 40-3308, 40-3403b, 40-3421, 40-3613, 40-3805, 40-4205, 44-510j, 44-550b, 44-594, 44-635, 44-714, 44-817, 44-1005, 44-1019, 45-221(a)(1) through (43), 46-256, 46-259, 46-2201, 47-839, 47-844, 47-849, 47-1709, 48-1614, 49-406, 49-427, 55-1,102, 58-4114, 59-2135, 59-2802, 59-2979, 59-29b79, 60-3333, 60-3336, 65-102b, 65-118, 65-119, 65-153f, 65-170g, 65-177, 65-1,106, 65-1,113, 65-1,116, 65-1,157a, 65-1,163, 65-1,165, 65-1,168, 65-1,169, 65-1,171, 65-1,172, 65-436, 65-445, 65-507, 65-525, 65-531, 65-657, 65-1135, 65-1467, 65-

1627, 65-1831, 65-2422d, 65-2438, 65-2836, 65-2839a, 65-2898a, 65-3015, 65-3447, 65-34,108, 65-34,126, 65-4019, 65-4922, 65-4925, 65-5602, 65-5603, 65-6002, 65-6003, 65-6004, 65-6010, 65-67a05, 65-6803, 65-6804, 66-101c, 66-117, 66-151, 66-1,190, 66-1,203, 66-1220a, 66-2010, 72-2232, 72-3438, 72-6116, 72-6267, 72-9934, 73-1228, 74-2424, 74-2433f, 74-32,419, 74-4905, 74-4909, 74-50,131, 74-5515, 74-7308, 74-7338, 74-8104, 74-8307, 74-8705, 74-8804, 74-9805, 75-104, 75-712, 75-7b15, 75-1267, 75-2943, 75-4332, 75-4362, 75-5133, 75-5266, 75-5665, 75-5666, 75-7310, 76-355, 76-359, 76-493, 76-12b11, 76-12c03, 76-3305, 79-1119, 79-1437f, 79-3234, 79-3395, 79-3420, 79-3499, 79-34,113, 79-3614, 79-3657, 79-4301 and 79-5206.

(2) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) and that have been reviewed during the 2015 legislative session and continued in existence by the legislature as provided in subsection (g) are hereby continued in existence: 17-2036, 40-5301, 45-221(a)(45), (46) and (49), 48-16a10, 58-4616, 60-3351, 72-3415, 74-50,217 and 75-53,105.

(j) (1) Exceptions contained in the following statutes as continued in existence in section 1 of chapter 87 of the 2006 Session Laws of Kansas and that have been reviewed and continued in existence twice by the legislature as provided in subsection (g) are hereby continued in existence: 1-501, 9-1303, 12-4516a, 39-970, 65-525, 65-5117, 65-6016, 65-6017 and 74-7508.

(2) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) during 2015 and that have been reviewed during the 2016 legislative session are hereby continued in existence: 12-5611, 22-4906, 22-4909, 38-2310, 38-2311, 38-2326, 40-955, 44-1132, 45-221(a)(10)(F) and (a)(50), 60-3333, 65-4a05, 65-445(g), 65-6154, 71-218, 75-457, 75-712c, 75-723 and 75-7c06.

(k) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) and that have been reviewed during the 2014 legislative session and continued in existence by the legislature as provided in subsection (g) are hereby continued in existence: 1-205, 2-2204, 8-240, 8-247, 8-255c, 8-1324, 8-1325, 12-17,150, 12-2001, 17-12a607, 38-1008, 38-2209, 40-5006, 40-5108, 41-2905, 41-2906, 44-706, 44-1518, 45-221(a)(44), (45), (46), (47) and (48), 50-6a11, 65-1,243, 65-16,104, 65-3239, 74-50,184, 74-8134, 74-99b06, 77-503a and 82a-2210.

(l) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the

house of representatives pursuant to subsection (e) during 2016 and that have been reviewed during the 2017 legislative session are hereby continued in existence: 12-5711, 21-2511, 22-4909, 38-2313, 45-221(a)(51) and (52), 65-516, 65-1505, 74-2012, 74-5607, 74-8745, 74-8752, 74-8772, 75-7d01, 75-7d05, 75-5133, 75-7427 and 79-3234.

(m) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) during 2012 and that have been reviewed during the 2013 legislative session and continued in existence by the legislature as provided in subsection (g) are hereby continued in existence: 12-5811, 40-222, 40-223j, 40-5007a, 40-5009a, 40-5012a, 65-1685, 65-1695, 65-2838a, 66-1251, 66-1805, 72-8268, 75-712 and 75-5366.

(n) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) and that have been reviewed during the 2018 legislative session are hereby continued in existence: 9-513c(c)(2), 39-709, 45-221(a)(26), (53) and (54), 65-6832, 65-6834, 75-7c06 and 75-7c20.

(o) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) that have been reviewed during the 2019 legislative session are hereby continued in existence: 21-2511(h)(2), 21-5905(a)(7), 22-2302(b) and (c), 22-2502(d) and (e), 40-222(k)(7), 44-714(e), 45-221(a)(55), 46-1106(g) regarding 46-1106(i), 65-2836(i), 65-2839a(c), 65-2842(d), 65-28a05(n), article 6(d) of 65-6230, 72-6314(a) and 74-7047(b).

(p) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) that have been reviewed during the 2020 legislative session are hereby continued in existence: 38-2310(c), 40-409(j)(2), 40-6007(a), 45-221(a)(52), 46-1129, 59-29a22(b)(10) and 65-6747.

(q) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) that have been reviewed during the 2021 legislative session are hereby continued in existence: 22-2302(c)(4)(J) and (c)(6)(B), 22-2502(e)(4)(J) and (e)(6)(B) and 65-6111(d)(4).

(r) Exceptions contained in the following statutes as certified by the revisor of statutes to the president of the senate and the speaker of the house of representatives pursuant to subsection (e) that have been reviewed during the 2023 legislative session are hereby continued in

existence: 2-3902 and 66-2020.

Sec. 11. K.S.A. 75-413 is hereby amended to read as follows: 75-413. *(a)* The secretary of state may appoint such other assistants and clerks as may be authorized by law~~;~~, but the secretary of state shall be responsible for the proper discharge of the duties of all assistants and clerks, and they shall hold their offices at the will and pleasure of the secretary and shall do and perform such general duties as the secretary may require.

(b) The secretary of state 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

(2) ensure that the secretary of state 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) (i) 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; and

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

(B) 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. 12. K.S.A. 75-623 is hereby amended to read as follows: 75-623. *(a)* The treasurer shall appoint such other assistants, clerks, bookkeepers, accountants and stenographers as may be authorized by law, each of which persons shall take the oath of office required of public officers. Such persons shall hold their offices at the will and pleasure of the state treasurer.

(b) The treasurer 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

(2) ensure that the treasurer 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) (i) 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; and

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

(B) 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. 13. K.S.A. 75-710 is hereby amended to read as follows: 75-710. *(a)* The attorney general shall appoint such assistants, clerks, and stenographers as shall be authorized by law, and who shall hold their office at the will and pleasure of the attorney general. All fees and allowances earned by said assistants or any of them, or allowed to them by any statute or order of court in any civil or criminal case whatsoever, shall be turned into the general revenue fund of the state treasury, and the vouchers for their monthly salaries shall not be honored by the director of accounts and 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier 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) (i) 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; and

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

(B) 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. 75-711 is hereby amended to read as follows: 75-711. *(a)* There is hereby established, under the jurisdiction of the attorney general, a division to be known as the Kansas bureau of investigation. The director of the bureau shall be appointed by the attorney general, subject to confirmation by the senate as provided in K.S.A. 75-4315b, and amendments thereto, and shall have special training and qualifications for such position. Except as provided by K.S.A. 46-2601, and amendments thereto, no person appointed as director shall exercise any power, duty or function as director until confirmed by the senate. In accordance with appropriation acts, the director shall appoint agents who shall be trained in the detection and apprehension of criminals. The director shall appoint an associate director, and any such assistant directors from within the agency as are necessary for the efficient operation of the bureau, who shall have the qualifications and employee benefits, including longevity, of an agent. The director also may appoint a deputy director and, in accordance with appropriation acts, such administrative employees as are necessary for the efficient operation of the bureau. No person shall be appointed to a position within the Kansas bureau of investigation if the person has been convicted of a felony.

(b) The director, associate director, deputy director, assistant directors and any assistant attorneys general assigned to the bureau shall be within the unclassified service under the Kansas civil service act. All other agents and employees of the bureau shall be in the classified service under the Kansas civil service act and their compensation shall be determined as provided in the Kansas civil service act and shall receive actual and necessary expenses.

(c) Any person who was a member of the bureau at the time of appointment as director, associate director or assistant director, upon the expiration of their appointment, shall be returned to an unclassified or regular classified position under the Kansas civil service act with compensation comparable to and not lower than compensation being received at the time of appointment to the unclassified service. If all such

possible positions are filled at that time, a temporary additional position shall be created for the person until a vacancy exists in the position. While serving in the temporary additional position, the person shall continue to be a contributing member of the retirement system for the agents of the Kansas bureau of investigation.

(d) Each agent of the bureau shall subscribe to an oath to faithfully discharge the duties of such agent's office, as is required of other public officials.

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

(1) Develop a cybersecurity program for the bureau 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

(2) ensure that the director 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) (i) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the department for compliance with applicable state and federal laws, rules and regulations and department policies and standards; and

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

(B) 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. 15. K.S.A. 2023 Supp. 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 *or policies adopted by the judicial branch or the legislative coordinating council*.

(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 not the 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 *or policies adopted by the judicial branch or the legislative coordinating council*;

(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 policies adopted by the judicial branch or the legislative coordinating council*; 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.

Sec. 16. K.S.A. 2023 Supp. 75-7202 is hereby amended to read as follows: 75-7202. (a) There is hereby established the information technology executive council which shall be attached to the office of information technology services for purposes of administrative functions.

(b) (1) The council shall be composed of ~~17~~ *13* voting members as follows:

(A) Two cabinet agency heads or such persons' designees;

(B) two noncabinet agency heads or such persons' designees;

(C) the executive chief information technology officer;

(D) ~~the legislative chief information technology officer;~~

~~(E) the judicial chief information technology officer;~~

~~(F)~~ the chief executive officer of the state board of regents or such person's designee;

~~(G)~~*(E)* one representative of cities;

~~(H)~~*(F)* one representative of counties; the network manager of the information network of Kansas (INK);

~~(I)~~*(G)* one representative with background and knowledge in technology and cybersecurity from the private sector, except that such representative or such representative's employer shall not be an information technology or cybersecurity vendor that does business with the state of Kansas;

~~(J)~~*(H)* one representative appointed by the Kansas criminal justice information system committee; *and*

~~(K) one member of the senate appointed by the president of the senate or such member's designee;~~

~~(L) one member of the senate appointed by the minority leader of the senate or such member's designee;~~

~~(M) one member of the house of representatives appointed by the speaker of the house of representatives or such member's designee; and~~

~~(N) one member of the house of representatives appointed by the minority leader of the house of representatives or such member's designee~~*(I) two information technology employees from state board of regents institutions appointed by the board of regents*.

(2) The chief information technology architect*, the legislative chief information technology officer, the judicial chief information technology officer, one member of the senate appointed by the president of the senate, one member of the senate appointed by the minority leader of the senate, one member of the house of representatives appointed by the speaker of*

the house of representatives and one member of the house of representatives appointed by the minority leader of the house of representatives shall be ~~a nonvoting member~~ *nonvoting members* of the council.

(3) The cabinet agency heads, the noncabinet agency heads, the representative of cities, the representative of counties and the representative from the private sector shall be appointed by the governor for a term not to exceed 18 months. Upon expiration of an appointed member's term, the member shall continue to hold office until the appointment of a successor. Legislative members shall remain members of the legislature in order to retain membership on the council and shall serve until replaced pursuant to this section. Vacancies of members during a term shall be filled in the same manner as the original appointment only for the unexpired part of the term. The appointing authority for a member may remove the member, reappoint the member or substitute another appointee for the member at any time. Nonappointed members shall serve ex officio.

(c) The chairperson of the council shall be ~~drawn from the chief information technology officers, with each chief information technology officer serving a one-year term. The term of chairperson shall rotate among the chief information technology officers on an annual basis~~ *the executive chief information technology officer*.

(d) The council shall hold ~~quarterly~~ *monthly* meetings and hearings in the city of Topeka or at such other places as the council designates, on call of the executive chief information technology officer or on request of four or more members. A quorum of the council shall be ~~nine~~ *seven members*. All actions of the council shall be taken by a majority of all of the members of the council.

(e) Except for members specified as a designee in subsection (b), members of the council may not appoint an individual to represent them on the council and only members of the council may vote.

(f) Members of the council shall receive mileage, tolls and parking as provided in K.S.A. 75-3223, and amendments thereto, for attendance at any meeting of the council or any subcommittee meeting authorized by the council.

Sec. 17. 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~~ *executive branch* 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~~ *executive branch* agencies; and

(D) a strategic information technology management plan for the ~~state~~ *executive branch*;

(2) provide direction and coordination for the application of the ~~state's~~ *executive branch's* information technology resources;

(3) designate the ownership of information resource processes and the lead *executive branch* agency for implementation of new technologies and networks shared by multiple agencies ~~in different branches~~ *within the executive branch* of state government; ~~and~~

(4) *develop a plan to integrate all information technology services for the executive branch into the office of information technology services; and*

(5) perform such other functions and duties as necessary to carry out the provisions of this act.

(c) 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, in accordance with section 1, and amendments thereto.

Sec. 18. K.S.A. 2023 Supp. 75-7205 is hereby amended to read as follows: 75-7205. (a) There is hereby established within and as a part of the office of information technology services the position of executive chief information technology officer. The executive chief information technology officer 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. The executive chief information technology officer shall maintain a presence in any cabinet established by the governor and shall report to the governor.

(b) The executive chief information technology officer shall:

(1) Review and consult with each executive agency regarding information technology plans, deviations from the state information technology architecture, information technology project estimates and information technology project changes and overruns submitted by such agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine whether the agency has complied with:

(A) The information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;

(B) the information technology architecture adopted by the information technology executive council;

(C) the standards for data management adopted by the information technology executive council; and

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

(2) report to the chief information technology architect all deviations from the state information architecture that are reported to the executive information technology officer by executive agencies;

(3) submit recommendations to the division of the budget as to the technical and management merit of information technology projects and information technology project changes and overruns submitted by executive agencies that are reportable pursuant to K.S.A. 75-7209, and amendments thereto;

(4) monitor executive agencies' compliance with:

(A) The information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;

(B) the information technology architecture adopted by the information technology executive council;

(C) the standards for data management adopted by the information technology executive council; and

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

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

(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 executive branch of state government; ~~and~~

(7) perform such other functions and duties as provided by law or as directed by the governor*;*

(8) consult with the appropriate legal counsel 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;

(9) ensure that each executive agency has the necessary information technology and cybersecurity staff imbedded within the agency to accomplish the agency's duties;

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

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

(c) An employee of the office of information technology services shall not disclose confidential information of an executive agency. Violation of this subsection is a severity level 5, nonperson felony.

(d) The executive chief information technology officer may make a request to the adjutant general to permit the Kansas national guard in a state active duty capacity to perform vulnerability assessments or other assessments of the branch for the purpose of enhancing security. During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed. The executive chief information technology officer shall notify the executive agency that owns the information systems being assessed about such assessment and coordinate to mitigate the security risk.

Sec. 19. K.S.A. 2023 Supp. 75-7206 is hereby amended to read as follows: 75-7206. (a) There is hereby established within and as a part of the office of the state judicial administrator the position of judicial chief information technology officer. The judicial chief information technology officer shall be appointed by the judicial administrator, subject to approval of the chief justice, and shall receive compensation determined by the judicial administrator, subject to approval of the chief justice.

(b) The judicial chief information technology officer shall:

(1) Review and consult with each judicial agency regarding information technology plans, deviations from the state information technology architecture, information technology project estimates and information technology project changes and overruns ~~submitted by such agency pursuant to K.S.A. 75-7209, and amendments thereto,~~ to determine whether the agency has complied with~~:~~

~~(A) The information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;~~

~~(B) the information technology architecture adopted by the information technology executive council;~~

~~(C) the standards for data management adopted by the information technology executive council; and~~

~~(D) the strategic information technology management plan adopted by the information technology executive council~~ *policies and procedures adopted by the judicial branch*;

(2) report to the chief information technology architect all deviations from the state information architecture that are reported to the judicial information technology officer by judicial agencies;

(3) submit recommendations to the judicial administrator as to the technical and management merit of information technology projects and information technology project changes and overruns submitted by judicial agencies that are reportable pursuant to K.S.A. 75-7209, and amendments

thereto;

~~(4) monitor judicial agencies' compliance with:~~

~~(A) The information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;~~

~~(B) the information technology architecture adopted by the information technology executive council;~~

~~(C) the standards for data management adopted by the information technology executive council; and~~

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

~~(5)~~*(4)* coordinate implementation of new information technology among judicial agencies and with the executive and legislative chief information technology officers;

~~(6)~~*(5)* designate the ownership of information resource processes and the lead agency for implementation of new technologies and networks shared by multiple agencies within the judicial branch of state government; ~~and~~

~~(7)~~*(6)* perform such other functions and duties as provided by law or as directed by the judicial administrator*;*

(7) ensure that each judicial agency has the necessary information technology and cybersecurity staff imbedded within the agency to accomplish the agency's duties;

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

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

(c) An employee of the office of the state judicial administrator shall not disclose confidential information of a judicial agency. Violation of this subsection is a severity level 5, nonperson felony.

(d) The judicial chief information technology officer may make a request to the adjutant general to permit the Kansas national guard in a state active duty capacity to perform vulnerability assessments or other assessments of the branch for the purpose of enhancing security. During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed. The judicial chief information technology officer shall notify the judicial agency that owns the information systems being assessed about such assessment and coordinate to mitigate the security risk.

Sec. 20. K.S.A. 2023 Supp. 75-7208 is hereby amended to read as follows: 75-7208. *(a)* The legislative chief information technology officer shall:

~~(a)~~*(1)* Review and consult with each legislative agency regarding information technology plans, deviations from the state information technology architecture, information technology project estimates and information technology project changes and overruns submitted by such agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine whether the agency has complied with the~~:~~

~~(1) Information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;~~

~~(2) information technology architecture adopted by the information technology executive council;~~

~~(3) standards for data management adopted by the information technology executive council; and~~

~~(4) strategic information technology management plan adopted by the information technology executive council~~ *policies and procedures adopted by the legislative coordinating council*;

~~(b)~~*(2)* report to the chief information technology architect all deviations from the state information architecture that are reported to the legislative information technology officer by legislative agencies;

~~(c)~~*(3)* submit recommendations to the legislative coordinating council as to the technical and management merit of information technology projects and information technology project changes and overruns ~~submitted by legislative agencies that are reportable pursuant to K.S.A. 75-7209, and amendments thereto~~;

~~(d) monitor legislative agencies' compliance with the:~~

~~(1) Information technology resource policies and procedures and project management methodologies adopted by the information technology executive council;~~

~~(2) information technology architecture adopted by the information technology executive council;~~

~~(3) standards for data management adopted by the information technology executive council; and~~

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

~~(e)~~*(4)* coordinate implementation of new information technology among legislative agencies and with the executive and judicial chief information technology officers;

~~(f)~~*(5)* 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)~~*(6)* serve as staff of the joint committee;~~ and~~

~~(h)~~*(7)* perform such other functions and duties as provided by law or

as directed by the legislative coordinating council or the joint committee*;*

(8) 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;

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

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

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

(12) set standards for the legislative division of post audit to use when conducting information technology audits that are subject to approval by the legislative coordinating council.

(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 Kansas national guard in a state active duty capacity to perform vulnerability assessments or other assessments of the branch for the purpose of enhancing security. During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed. The legislative chief information technology officer shall notify the legislative agency that owns the information systems being assessed about such assessement and coordinate to mitigate the security risk.

Sec. 21. K.S.A. 2023 Supp. 75-7209 is hereby amended to read as follows: 75-7209. (a) (1) Whenever an agency proposes an information technology project, such agency shall prepare and submit information technology project documentation to the chief information technology officer of the branch of state government of which the agency is a part. Such information technology project documentation shall:

(A) Include a financial plan showing the proposed source of funding and categorized expenditures for each phase of the project and cost estimates for any needs analyses or other investigations, consulting or other professional services, computer programs, data, equipment, buildings or major repairs or improvements to buildings and other items or services necessary for the project; and

(B) be consistent with:

(i) Information technology resource policies and procedures and project management methodologies for all state agencies;

(ii) an information technology architecture, including telecommunications systems, networks and equipment, that covers all state agencies;

(iii) standards for data management for all state agencies; and

(iv) a strategic information technology management plan for the state.

(2) Any information technology project with significant business risk, as determined pursuant to the information technology executive council's policies *or policies adopted by the judicial branch or the legislative coordinating council*, shall be presented to the joint committee on information technology by such branch chief information technology officer.

(b) (1) Prior to the release of any request for proposal for an information technology project with significant business risk:

(A) Specifications for bids or proposals for such project shall be submitted to the chief information technology officer of the branch of state government of which the agency or agencies are a part. Information technology projects requiring chief information technology officer approval shall also require the chief information technology officer's written approval on specifications for bids or proposals; and

(B) (i) The chief information technology officer of the appropriate branch over the state agency or agencies that are involved in such project shall submit the project, the project plan, including the architecture, and the cost-benefit analysis to the joint committee on information technology to advise and consult on the project. Such chief information technology officer shall submit such information to each member of the joint committee and to the director of the legislative research department. Each such project plan summary shall include a notice specifying the date the summary was mailed or emailed. After receiving any such project plan summary, each member shall review the information and may submit questions, requests for additional information or request a presentation and review of the proposed project at a meeting of the joint committee. If two or more members of the joint committee contact the director of the legislative research department within seven business days of the date specified in the summary description and request that the joint committee schedule a meeting for such presentation and review, then the director of the legislative research department shall notify the chief information technology officer of the appropriate branch, the head of such agency and the chairperson of the joint committee that a meeting has been requested for such presentation and review on the next business day following the members' contact with the director of the legislative research department. Upon receiving such notification, the chairperson shall call a meeting of

the joint committee as soon as practicable for the purpose of such presentation and review and shall furnish the chief information technology officer of the appropriate branch and the head of such agency with notice of the time, date and place of the meeting. Except as provided in subsection (b)(1)(B)(ii), the state agency shall not authorize or approve the release of any request for proposal or other bid event for an information technology project without having first advised and consulted with the joint committee at a meeting.

(ii) The state agency or agencies shall be deemed to have advised and consulted with the joint committee about such proposed release of any request for proposal or other bid event for an information technology project and may authorize or approve such proposed release of any request for proposal or other bid event for an information technology project if:

(a) Fewer than two members of the joint committee contact the director of the legislative research department within seven business days of the date the project plan summary was mailed and request a committee meeting for a presentation and review of any such proposed request for proposal or other bid event for an information technology project; or

(b) a committee meeting is requested by at least two members of the joint committee pursuant to this paragraph, but such meeting does not occur within two calendar weeks of the chairperson receiving the notification from the director of the legislative research department of a request for such meeting.

(2) (A) Agencies are prohibited from contracting with a vendor to implement the project if that vendor prepared or assisted in the preparation of the program statement, the project planning documents or any other project plans prepared prior to the project being approved by the chief information technology officer as required by this section.

(B) Information technology projects with an estimated cumulative cost of less than $5,000,000 are exempted from the provisions of subparagraph (A).

(C) The provisions of subparagraph (A) may be waived with prior written permission from the chief information technology officer.

(c) Annually at the time specified by the chief information technology officer of the branch of state government of which the agency is a part, each agency shall submit to such officer:

(1) A copy of a three-year strategic information technology plan that sets forth the agency's current and future information technology needs and utilization plans for the next three ensuing fiscal years, in such form and containing such additional information as prescribed by the chief information technology officer; and

(2) any deviations from the state information technology architecture adopted by the information technology executive council.

(d) The provisions of this section shall not apply to the information network of Kansas (INK).

Sec. 22. 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~~ *means* 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~~ *the* 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.

Sec. 23. 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 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 cybersecurity of all executive branch data and information resources;

(7) collaborate with the chief information security officers of the other branches of state government to respond to cybersecurity incidents;

(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; and

(9) review all contracts related to information technology entered into by a person or entity within the executive branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure 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 CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030. The agency head of each executive agency shall coordinate with the executive CISO to achieve such standards.

Sec. 24. K.S.A. 2023 Supp. 75-7239 is hereby amended to read as follows: 75-7239. (a) There is hereby established within and as a part of the office of information technology services the Kansas information security office. The Kansas information security office shall be administered by the *executive* CISO and be staffed appropriately to effect the provisions of the Kansas cybersecurity act.

(b) For the purpose of preparing the governor's budget report and related legislative measures submitted to the legislature, the Kansas information security office, established in this section, shall be considered a separate state agency and shall be titled for such purpose as the "Kansas information security office." The budget estimates and requests of such office shall be presented as from a state agency separate from the office of information technology services, and such separation shall be maintained in the budget documents and reports prepared by the director of the budget and the governor, or either of them, including all related legislative reports and measures submitted to the legislature.

(c) Under direction of the *executive* CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) ~~assist the executive branch in developing, implementing and~~

~~monitoring~~*develop, implement and monitor* strategic and comprehensive information security risk-management programs;

(3) ~~facilitate executive branch information security governance, including the consistent application of information security programs, plans and procedures;~~

~~(4) using standards adopted by the information technology executive council, create and manage a unified and flexible control framework to integrate and normalize requirements resulting from applicable state and federal laws, and rules and regulations;~~

~~(5)~~ facilitate a metrics, logging and reporting framework to measure the efficiency and effectiveness of state information security programs;

~~(6)~~*(4)* provide the executive branch strategic risk guidance for information technology projects, including the evaluation and recommendation of technical controls;

~~(7) assist in the development of executive branch agency cybersecurity programs to ensure compliance with applicable state and federal laws, rules and regulations, executive branch policies and standards and policies and standards adopted by the information technology executive council;~~

~~(8)~~*(5) coordinate with the United States cybersecurity and infrastructure security agency to* perform *annual* audits of executive branch agencies for compliance with applicable state and federal laws, rules and regulations~~,~~ *and* executive branch policies and standards ~~and policies and standards adopted by the information technology executive council~~. *The executive CISO shall make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit*;

(6) perform audits of executive branch agencies for compliance with applicable state and federal laws, rules and regulations, executive branch policies and standards and policies and standards adopted by the information technology executive council;

~~(9)~~*(7)* coordinate the use of external resources involved in information security programs, including, but not limited to, interviewing and negotiating contracts and fees;

~~(10)~~*(8)* liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

~~(11)~~*(9)* assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;

~~(12) assist executive branch agencies to create a framework for roles and responsibilities relating to information ownership, classification, accountability and protection;~~

~~(13)~~*(10) coordinate with executive branch agencies to provide*

cybersecurity staff to such agencies as necessary;

(11) ensure a cybersecurity awareness training program is made available to all branches of state government; and

~~(14)~~*(12)* perform such other functions and duties as provided by law and as directed by the CISO.

(d) *(1) If an audit conducted pursuant to subsection (c)(5) results in a failure, the executive CISO 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 executive CISO 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 ~~(c)(8)~~ *(c)(5) 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. ~~The provisions of this subsection shall expire on July 1, 2028, unless the legislature reviews and acts to continue such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.~~

(e) There is hereby created in the state treasury the information technology security fund. All expenditures from such fund shall be made in accordance with appropriation acts upon warrants of the director of accounts and reports issued pursuant to vouchers approved by the executive CISO or by a person designated by the executive CISO.

Sec. 25. K.S.A. 2023 Supp. 75-7240 is hereby amended to read as follows: 75-7240. (a) The executive branch agency heads shall:

(1) Be ~~solely~~ responsible for security of all data and information technology resources under such agency's purview, irrespective of the location of the data or resources. ~~Locations of data may include:~~

~~(A) Agency sites;~~

~~(B) agency real property;~~

~~(C) infrastructure in state data centers;~~

~~(D) third-party locations; and~~

~~(E) in transit between locations;~~

~~(2) ensure that an agency-wide information security program is in place~~;

~~(3)~~*(2)* designate an information security officer to administer the agency's information security program that reports directly to executive leadership;

~~(4)~~*(3)* participate in CISO-sponsored statewide cybersecurity program initiatives and services;

~~(5) implement policies and standards to ensure that all the agency's~~

~~data and information technology resources are maintained in compliance with applicable state and federal laws and rules and regulations;~~

~~(6) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;~~

~~(7) include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;~~

~~(8) (A) submit a cybersecurity self-assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to which the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure or inappropriate use;~~

~~(B) ensure that the agency conducts annual internal assessments of its security program. Internal assessment results shall be considered confidential and shall not be subject to discovery by or release to any person or agency, outside of the KISO or CISO, without authorization from the executive branch agency director or head; and~~

~~(C) prepare or have prepared a financial summary identifying cybersecurity expenditures addressing the findings of the cybersecurity self-assessment report required in subparagraph (A), excluding information that might put the data or information resources of the agency or its contractors at risk and submit such report to the house of representatives committee on appropriations and the senate committee on ways and means; and~~

~~(9)~~*(4)* ensure that if an agency owns, licenses or maintains computerized data that includes personal information, confidential information or information, the disclosure of which is regulated by law, such agency shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(A) Comply with the notification requirements set out in K.S.A. 2023 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal laws and rules and regulations, to the same extent as a person who conducts business in this state; and

(B) not later than ~~48~~ *12* hours after the discovery of the breach, suspected breach or unauthorized exposure, notify:

(i) The CISO; and

(ii) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

(b) The director or head of each state agency shall:

(1) Participate in annual agency leadership training to ensure understanding of:

(A) The potential impact of common types of cyberattacks and data breaches on the agency's operations and assets;

(B) how cyberattacks and data breaches on the agency's operations and assets may impact the operations and assets of other governmental entities on the state enterprise network;

(C) how cyberattacks and data breaches occur; and

(D) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; *and*

(2) ~~ensure that all information technology login credentials are disabled the same day that any employee ends their employment with the state; and~~

~~(3) require that all employees with access to information technology receive a minimum of one hour of information technology security training per year~~*coordinate with the executive CISO to implement the security standard described in K.S.A. 75-7238, and amendments thereto*.

~~(c) (1) The CISO, with input from the joint committee on information technology and the joint committee on Kansas security, shall develop a self-assessment report template for use under subsection (a)(8)(A). The most recent version of such template shall be made available to state agencies prior to July 1 of each even-numbered year. The CISO shall aggregate data from the self-assessments received under subsection (a)(8)(A) and provide a summary of such data to the joint committee on information technology and the joint committee on Kansas security.~~

~~(2) Self-assessment reports made to the CISO pursuant to subsection (a)(8)(A) shall be confidential and shall not be subject to the provisions of 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. 26. K.S.A. 40-110, 75-413, 75-623, 75-710, 75-711 and 75-7203 and K.S.A. 2023 Supp. 45-229, 75-7201, 75-7202, 75-7205, 75-7206, 75-7208, 75-7209, 75-7237, 75-7238, 75-7239 and 75-7240 are hereby repealed.

Sec. 27. This act shall take effect and be in force from and after its publication in the statute book.