Session of 2026

HOUSE BILL No. 2574

By Joint Committee on Information Technology

1-28

AN ACT concerning cybersecurity; relating to consolidation of cybersecurity services; modifying the duties of the chief information security officers for each branch of government, removing maturity requirements for cybersecurity programs; requiring periodic audits of such programs; creating the judicial branch technology oversight council; requiring the executive branch chief information security officer to assess executive branch agencies for compliance with cybersecurity standards and report findings to the legislature; providing for consideration of cybsersecurity compliance during the budgeting process; modifying the membership and duties of the information technology executive council; amending K.S.A. 2025 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7202, 75-7203, 75-7206a, 75-7208a, 75-7237, 75-7238, 75-7239, 75-7240, 75-7245 and 75-7246 and repealing the existing sections; also repealing K.S.A. 75-7203, as amended by section 21 of chapter 95 of the 2024 Session Laws of Kansas, and 75-7205, as amended by section 23 of chapter 95 of the 2024 Session Laws of Kansas and K.S.A. 2023 Supp. 75-7201, as amended by section 17 of chapter 95 of the 2024 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206, as amended by section 25 of chapter 95 of the 2024 Session Laws of Kansas, 75-7208, as amended by section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209, as amended by section 29 of chapter 95 of the 2024 Session Laws of Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter 95 of the 2024 Session Laws of Kansas, 75-7239, as amended by section 35 of chapter 95 of the 2024 Session Laws of Kansas, and 75-7240, as amended by section 37 of chapter 95 of the 2024 Session Laws of Kansas.

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

New Section 1. There is hereby established the judicial branch technology oversight council. The membership of the council shall be determined by the chief justice. The council shall:

(a) Set standards for judicial branch information technology;

(b) establish information technology policies for the judicial branch;

(c) approve strategic information technology plans;

(d) oversee information technology projects to ensure alignment with judicial branch goals;

(e) evaluate information technology and cybersecurity programs; and

(f) support the judicial chief information technology officer and the judicial branch chief information security officer.

Sec. 2. K.S.A. 2025 Supp. 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) ~~(1)~~ 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:

~~(A)~~*(1)* Develop a cybersecurity program for the department ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of*

representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program;

~~(B)~~*(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

~~(C) (i) (a)~~*(3) (A)* coordinate ~~with the United States cybersecurity and infrastructure security agency to perform annual audits of the department~~ *periodic audits of the cybersecurity program* for compliance with applicable state and federal laws, rules and regulations and department policies and standards~~; and~~

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

~~(ii)~~*(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. *The provisions of this subparagraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 3. K.S.A. 2025 Supp. 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) ~~(1)~~ 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:

~~(A)~~*(1)* Develop a cybersecurity program for the office ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*;

~~(B)~~*(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

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

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

~~(ii)~~*(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. *The provisions of this subparagraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 4. K.S.A. 2025 Supp. 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) ~~(1)~~ 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:

~~(A)~~*(1)* Develop a cybersecurity program for the office ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026. Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*;

~~(B)~~*(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

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

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

~~(ii)~~*(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. *The provisions of this subparagraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 5. K.S.A. 2025 Supp. 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)~~ (1)~~ 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:

~~(A)~~*(1)* Develop a cybersecurity program for the office~~ that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1,~~ 2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate*

standing committee on ways and means on the maturity level of the program;

~~(B)~~*(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

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

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

~~(ii)~~*(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. *The provisions of this subparagraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 6. K.S.A. 2025 Supp. 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) ~~(1)~~ 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:

~~(A)~~*(1)* Develop a cybersecurity program for the bureau ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*;

~~(B)~~*(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

~~(C) (i) (a)~~*(3) (A)* coordinate ~~with the United States cybersecurity and infrastructure security agency to perform annual audits of the department~~ *for periodic audits of the cybersecurity program* for compliance with applicable state and federal laws, rules and regulations and department policies and standards~~; and~~

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

~~audit~~.

~~(ii)~~*(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. *The provisions of this subparagraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 7. K.S.A. 2025 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 ~~13~~ *17* 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 executive chief information security officer;*

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

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

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

~~(G)~~*(H)* 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;

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

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

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

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

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

(N) 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~~,~~ *and* 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 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 the executive chief information technology officer.

(d) The council shall hold 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 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. 8. K.S.A. 2025 Supp. 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 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 executive branch agencies; and

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

(2) provide direction and coordination for the application of the 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 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 all cybersecurity services for state educational institutions as defined in K.S.A. 76-711, and amendments thereto, into the office of information technology services and the Kansas information security office; 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 K.S.A. 2025 Supp. 75-7245, and amendments thereto.~~

Sec. 9. K.S.A. 2025 Supp. 75-7206a is hereby amended to read as follows: 75-7206a. (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*, in coordination with the judicial technology oversight council,* 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~~ *ensure that* all contracts related to information technology entered into by a person or entity within the judicial branch ~~to make efforts~~ *contain provisions* 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~~ *periodic* audits of ~~judicial branch agencies~~ *the cybersecurity program* 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~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~*, 2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*.

(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 and minority leader of the house of representatives and the president and minority leader 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 and minority leader of the house of representatives and the president and minority leader 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. *The provisions of this subsection shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(c) This section shall expire on July 1, 2026.~~

Sec. 10. K.S.A. 2025 Supp. 75-7208a is hereby amended to read as follows: 75-7208a. (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 technology officer shall appoint a legislative chief information security officer.* The legislative chief information security officer shall develop a cybersecurity program of each legislative agency ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*.

~~(d)~~*(b)* (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 and minority leader of the house of representatives and the president and minority leader 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 and minority leader of the house of representatives and the president and minority leader of the senate~~*The legislative chief information security officer shall:*

(A) Ensure that all employees of each legislative agency and all legislators complete cybersecurity awareness training annually and that if an employee or legislator does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

(B) coordinate periodic audits of the cybersecurity program for compliance with applicable state and federal laws, rules and regulations and branch policies and standards.

(2) Results of audits conducted pursuant to *this* 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. *The provisions of this paragraph shall expire on July 1, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

~~(e) This section shall expire on July 1, 2026.~~

Sec. 11. K.S.A. 2025 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" 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 not 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. 12. K.S.A. 2025 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) 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~~*ensure that* all contracts related to information technology entered into by a person or entity within the executive branch ~~to make efforts~~ *contain provisions* to reduce the risk of security vulnerabilities within the supply chain or product and ~~ensure~~ each contract contains

standard security language*; and*

(10) adopt statewide cybersecurity standards, controls, directives and maturity and tier expectations for the executive branch and continually evaluate standards and expectations to address evolving threats, federal requirements, technological changes and statewide risk conditions.

(c) The executive CISO shall develop a cybersecurity program for each executive branch agency ~~that complies with~~ *based on* the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ *2026*. *Beginning in 2027 and every two years thereafter,* 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~~ *report to the joint committee on information technology, the house of representatives standing committee on appropriations and the senate standing committee on ways and means on the maturity level of the program*. The agency head of each executive branch agency shall coordinate with the executive CISO to achieve such standards.

Sec. 13. K.S.A. 2025 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) develop, implement and monitor strategic and comprehensive information security risk-management programs;

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

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

(5) coordinate ~~with the United States cybersecurity and infrastructure security agency to perform annual~~ *periodic* audits of ~~executive branch~~

~~agencies~~ *the cybersecurity program* for compliance with applicable state and federal laws, rules and regulations and executive branch policies and standards~~. 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;

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

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

(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;

(10) coordinate with executive branch agencies to provide cybersecurity staff to such agencies as necessary;

(11) *conduct periodic cybersecurity assessments of each executive branch agency that may include a review of controls, processes, technologies, governance, incident preparedness, operational security and compliance with statewide policies and standards;*

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

~~(12)~~*(13)* 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 and minority leader of the house of representatives and the president and minority leader 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 and minority leader of the house of representatives and the president and minority leader of the senate.~~

~~(2)~~ Results of audits conducted pursuant to subsection (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, 2030, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto.*

(e) *When conducting the assessments required by subsection (c)(11),*

the executive CISO may utilize KISO personnel, qualified third-party assessors or a combination thereof. The CISO may establish an assessment cycle that includes an initial baseline assessment for each agency and periodic assessments thereafter. After conducting such assessment, the executive CISO shall issue written findings, recommendations and a timeline for any corrective action that is needed based on the results of such assessments to be used in conjunction with 2025 Supp. K.S.A. 75-7246, and amendments thereto. After receiving such written findings, recommendations and timeline, an agency shall develop and maintain a written plan of action and milestones that details efforts to remediate the findings from such assessment.

(f) 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. 14. K.S.A. 2025 Supp. 75-7240 is hereby amended to read as follows: 75-7240. (a) The executive branch agency heads shall:

(1) Be responsible for security of all data and information technology resources under such agency's purview, irrespective of the location of the data or resources;

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

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

(4) *continuously work toward improving cybersecurity maturity consistent with statewide standards and expectations adopted by the executive CISO pursuant to K.S.A. 75-7238, and amendments thereto;*

(5) prior to acquiring any cybersecurity-related product, service or platform that may materially affect state systems, data or cybersecurity risks, consult with the executive CISO and obtain a written certificate from the executive CISO that such acquisition does not create a cybersecurity risk; and

(6) 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. 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 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) coordinate with the executive CISO to implement the security standard described in K.S.A. 75-7238, and amendments thereto.

Sec. 15. K.S.A. 2025 Supp. 75-7245 is hereby amended to read as follows: 75-7245. (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 the legislative and executive branches of state government shall work at the direction of the chief information technology officer of the branch.

(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 to judicial agencies and all employees of such agencies, including state and county-funded judicial branch district court employees. Such employees shall be required to use such state-issued information technology hardware. The project cost developed pursuant to this paragraph shall include, in consultation with the executive branch information technology officer, a plan to allow each piece of information technology hardware that is used by a judicial branch employee to access a judicial branch application to have access to the KANWIN network and an estimated project cost to develop a cybersecurity program for all judicial districts that complies with the national institute of standards and technology cybersecurity~~

framework (CSF) 2.0, as in effect on July 1, 2024.

(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 *hosted on* a ".gov" domain.

(e)*(c)* 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.

(f)*(d)* The provisions of this section do not apply to state educational institutions as defined in K.S.A. 76-711, and amendments thereto.

(g) This section shall expire on July 1, 2026.

Sec. 16. K.S.A. 2025 Supp. 75-7246 is hereby amended to read as follows: 75-7246. (a) On July *October* 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, *executive CISO* 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 *report to the legislative budget committee any executive branch agency that is not making progress on a written plan of action and milestones based on the assessment of such agency conducted pursuant to K.S.A. 75-7240, and amendments thereto. Each such agency shall present to the legislative budget committee such agency's plan to make progress on the written plan of action and milestones*.

(b) The director of the budget *executive CISO* shall submit a detailed

written report to the ~~legislature~~ *senate committee on ways and means and the house of representatives committee on appropriations* 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~~ *each agency that continues to fail to make progress on a written plan of action and milestones after the presentation made to the legislative budget committee pursuant to subsection (a)*. ~~(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 information technology and cybersecurity expenditures* for such state agencies *by 10%* during the budget committee hearings for such noncomplying agency.

~~(d) This section shall expire on July 1, 2026.~~

Sec. 17. K.S.A. 75-7203, as amended by section 21 of chapter 95 of the 2024 Session Laws of Kansas, and 75-7205, as amended by section 23 of chapter 95 of the 2024 Session Laws of Kansas and K.S.A. 2023 Supp. 75-7201, as amended by section 17 of chapter 95 of the 2024 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206, as amended by section 25 of chapter 95 of the 2024 Session Laws of Kansas, 75-7208, as amended by section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209, as amended by section 29 of chapter 95 of the 2024 Session Laws of Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter 95 of the 2024 Session Laws of Kansas, 75-7239, as amended by section 35 of chapter 95 of the 2024 Session Laws of Kansas, and 75-7240, as amended by section 37 of chapter 95 of the 2024 Session Laws of Kansas, and K.S.A. 2025 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7202, 75-7203, 75-7206a, 75-7208a, 75-7237, 75-7238, 75-7239, 75-7240, 75-7245 and 75-7246 are hereby repealed.

Sec. 18. This act shall take effect and be in force from and after its publication in the statute book.