HOUSE BILL No. 2019

AN ACT concerning information technology; requiring reporting of significant cybersecurity incidents; changing membership, terms and quorum requirements for the information technology executive council; relating to information technology projects and reporting requirements; information technology security training and cybersecurity reports; duties of the chief information security officer; requiring certain information to be provided to the joint committee on information technology; amending K.S.A. 46-2102, 74-5704, 75-7201, 75-7202, 75-7205, 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238, 75-7239, 75-7240 and 75-7242 and repealing the existing sections.

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

New Section 1. (a) Except as provided in subsection (b):

(1) Any public entity that has a significant cybersecurity incident shall notify the Kansas information security office within 12 hours after discovery of such incident.

(2) Any government contractor that has a significant cybersecurity incident that involves the confidentiality, integrity or availability of personal information or confidential information provided by the state of Kansas, networks or information systems operated by or on behalf of the state of Kansas shall notify the Kansas information security office:

(A) Within 72 hours after the government contractor reasonably believes that such significant cybersecurity incident occurred; or

(B) if a determination is made during the investigation that such information, networks or systems were directly impacted, within 12 hours after such determination is made.

(3) If a significant cybersecurity incident described in paragraph (1) or (2) involves election data, then the public entity or government contractor shall also notify the secretary of state of such incident within the time period required by paragraph (1) or (2).

(b) (1) Any entity that is connected to the Kansas criminal justice information system shall report any cybersecurity incident in accordance with rules and regulations adopted by the Kansas criminal justice information system committee pursuant to K.S.A. 74-5704, and amendments thereto.

(2) An entity that is connected to the Kansas criminal justice information system and is not connected to any other state of Kansas information system shall not be required to make the report required in subsection (a).

(3) The Kansas bureau of investigation shall notify the Kansas information security office of any significant cybersecurity incident report it receives in accordance with rules and regulations adopted pursuant to K.S.A. 74-5704, and amendments thereto, not later than 12 hours after receipt of such report.

(c) (1) The information provided pursuant to this section shall only be shared with individuals who need to know such information for response and defensive activities to preserve the integrity of state information systems and networks or to provide assistance if requested.

(2) Such information shall be confidential and shall not be subject to disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto. This paragraph 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.

(3) The Kansas information security office shall only report the information provided pursuant to this section as aggregate data.

(d) Nothing in this section shall be construed to supersede notification requirements in currently existing contracts between the state of Kansas and entities.

(e) Prior to October 1, 2023, the Kansas information security office shall post instructions on its website for submitting the significant cybersecurity reports required by this section. Such instructions shall include, but not be limited to, the types of incidents that are required to be reported and any information that is required to be included in the report made through the established cybersecurity incident reporting system.

(f) For the purposes of this section:

(1) "Cybersecurity incident" means an event or combination that threatens, without lawful authority, the confidentiality, integrity or availability of information or information systems and that requires an entity to initiate a response or recovery activity;

(2) "entity" means a public entity or government contractor;

(3) "government contractor" means an individual or private entity that performs work for or on behalf of the state of Kansas on a contract basis that has access to or is hosting state networks, systems, application or information;

(4) "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;

(5) "personal information" means the same as defined in K.S.A. 2022 Supp. 50-7a01, and amendments thereto;

(6) "private entity" means an individual, corporation, company, partnership, firm, association or other entity that is not a public entity;

(7) "public entity" means any public agency of the state or any political subdivision thereof;

(8) "security breach" means the same as defined in K.S.A. 2022 Supp. 50-7a01, and amendments thereto;

(9) "significant cybersecurity incident" means a cybersecurity incident that results in or is likely to result in financial loss or demonstrable harm to public confidence or public health and safety in the state of Kansas; and

(10) "unauthorized disclosure" means the accidental exposure of personal information to a person or entity that is not authorized or does not have a valid need to view the information.

Sec. 2. K.S.A. 46-2102 is hereby amended to read as follows: 46-2102. In addition to other powers and duties authorized or prescribed by law or by the legislative coordinating council, the joint committee on information technology shall:

(a) Study the use by state agencies and institutions of computers, telecommunications and other information technologies;

(b) review new governmental computer hardware and software acquisition, information storage, transmission, processing and telecommunications technologies proposed by state agencies and institutions, and the implementation plans therefor, including all information technology project budget estimates and three-year strategic information technology plans that are submitted to the joint committee pursuant to K.S.A. 75-7210*,* and amendments thereto;

(c) *advise and consult on all state agency information technology projects, as defined in K.S.A. 75-7201, and amendments thereto, that pose a significant business risk as determined by the information technology executive council's policies and in accordance with K.S.A. 75-7209, and amendments thereto;*

(d) make recommendations on all such implementation plans, budget estimates*, requests for proposals for information technology projects* and three-year plans to the ways and means committee of the senate and the committee on appropriations of the house of representatives;

~~(d)~~*(e)* study the progress and results of all newly implemented governmental computer hardware and software, information storage, transmission, processing and telecommunications technologies of state agencies and institutions including all information technology projects for state agencies which have been authorized or for which appropriations have been approved by the legislature; and

~~(e)~~*(f)* make an annual report to the legislative coordinating council as provided in K.S.A. 46-1207*,* and amendments thereto*,* and such special reports to committees of the house of representatives and senate as are deemed appropriate by the joint committee.

Sec. 3. K.S.A. 74-5704 is hereby amended to read as follows: 74-5704. The committee shall*:*

(a) Adopt and enforce ~~such~~ rules, regulations and policies ~~as~~ *that* are necessary for the establishment, maintenance, upgrading and

operation of the statewide criminal justice information system*; and*

(b) adopt rules and regulations that require entities connected to the Kansas criminal justice information system to report any cybersecurity incident to the Kansas bureau of investigation not later than 12 hours after the discovery of such cybersecurity incident.

Sec. 4. K.S.A. 75-7201 is hereby amended to read as follows: 75-7201. As used in K.S.A. 75-7201 through 75-7212, and amendments thereto:

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

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

~~(b)~~*(c)* "Executive agency" means any state agency in the executive branch of government.

~~(c)~~*(d)* "Information technology project" means~~ a project for a major computer, telecommunications or other information technology improvement with an estimated cumulative cost of $250,000 or more and includes any such project that has proposed expenditures for: (1) New or replacement equipment or software; (2) upgrade improvements to existing equipment and any computer systems, programs or software upgrades therefor; or (3) data or consulting or other professional services for such a project~~ *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*.

~~(d)~~*(e)* "Information technology project change or overrun" means ~~any of the following~~ *any change in*:

(1) ~~Any change in~~ 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~~ either $1,000,000 or~~ 10% of such currently authorized cost of such project~~, whichever is lower~~ *or an established threshold within the information technology executive council's policies*;

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

(3) ~~any change in~~ 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.

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

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

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

~~(h)~~*(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.

~~(i)~~*(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.

~~(j)~~*(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.

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

Sec. 5. K.S.A. 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 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) one representative of cities;

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

(I) one representative with background and knowledge in technology and cybersecurity from the private sector, ~~however,~~ *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) one representative appointed by the Kansas criminal justice information system committee;

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

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

(M) one member of the house ~~government, technology and security committee or its successor committee~~ *of representatives* appointed by the speaker of the house of representatives or such member's designee; and

(N) one member of the house ~~government, technology and security committee or its successor committee~~ *of representatives* appointed by the minority leader of the house of representatives or such member's designee.

(2) The chief information technology architect shall be a nonvoting member 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.

(d) The council shall hold quarterly 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. 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. 6. K.S.A. 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 ~~project estimates~~ *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~~, based on the determinations made pursuant to subsection (b)(1)~~;

(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.

Sec. 7. K.S.A. 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;

(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 ~~project estimates~~ *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~~, based on the determinations pursuant to subsection (b)(1)~~;

(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) coordinate implementation of new information technology among judicial agencies and with the executive 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 judicial branch of state government; and

(7) perform such other functions and duties as provided by law or as directed by the judicial administrator.

Sec. 8. K.S.A. 75-7208 is hereby amended to read as follows: 75-7208. The legislative chief information technology officer shall:

(a) 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)~~The~~ Information technology resource policies and procedures

and project management methodologies adopted by the information technology executive council;

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

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

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

(b) 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) submit recommendations to the legislative coordinating council as to the technical and management merit of information technology~~ project estimates~~ *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~~, based on the determinations pursuant to subsection (a)~~;

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

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

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

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

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

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

(f) 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) serve as staff of the joint committee; and

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

Sec. 9. K.S.A. 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~~ of a project budget estimate therefor, and for each amendment or revision thereof, in accordance with this section. Each information technology project budget estimate shall be in such form as required by the director of the budget, in consultation with the chief information technology architect, and by this section. In each case, the agency shall prepare and include as a part of such project budget estimate a plan consisting of a written program statement describing the project. The program statement shall:

~~(1) Include a detailed description of and justification for the project, including: (A) An analysis of the programs, activities and other needs and intended uses for the additional or improved information technology; (B) a statement of project scope including identification of the organizations and individuals to be affected by the project and a definition of the functionality to result from the project; and (C) an analysis of the alternative means by which such information technology needs and uses could be satisfied;~~

~~(2) describe the tasks and schedule for the project and for each phase of the project, if the project is to be completed in more than one phase;~~

~~(3) include a financial plan showing: (A) The proposed source of funding and categorized expenditures for each phase of the project; and~~

~~(B) 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~~

~~(4) include a cost-benefit statement based on an analysis of qualitative as well as financial benefits~~. *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, shall be presented to the joint committee on information technology by such branch chief information technology officer.

(b) (1) ~~Before one or more state agencies proposing an information technology project begin implementation of the project, the project plan, including the architecture and the cost-benefit analysis, shall be approved by the head of each state agency proposing the project and by the chief information technology officer of each branch of state government of which the agency or agencies are a part. Approval of those projects that involve telecommunications services shall also be subject to the provisions of K.S.A. 75-4709, 75-4710 and 75-4712, and amendments thereto.~~

~~(2) All specifications for bids or proposals related to an approved information technology project of one or more state agencies shall be reviewed by the chief information technology officer of each branch of state government of which the agency or agencies are a part~~ *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.

~~(3)~~*(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 ~~required under subsection (a)~~, the project planning documents ~~required under subsection (b)(1),~~ or any other project plans prepared prior to the project being approved by the chief information technology officer as required ~~under subsection (b)(1)~~ *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. 10. K.S.A. 75-7210 is hereby amended to read as follows: 75-7210. ~~(a)~~ Not later than ~~October~~ *November* 1 of each year, the executive, judicial and legislative chief information technology officers shall submit to the joint committee and to the legislative research department all information technology project budget estimates and amendments and revisions thereto, all three-year plans and all deviations from the state information technology architecture submitted to such officers pursuant to K.S.A. 75-7209, and amendments thereto.

The ~~legislative chief information technology officer~~ *joint committee* shall review all such estimates and amendments and revisions thereto, plans and deviations and shall make recommendations to the ~~joint committee~~ *house standing committee on appropriations and the senate standing committee on ways and means* regarding the merit thereof and appropriations therefor.

~~(b) The executive and judicial chief information technology officers shall report to the legislative chief information technology officer, at times agreed upon by the three officers:~~

~~(1) Progress regarding implementation of information technology projects of state agencies within the executive and judicial branches of state government; and~~

~~(2) all proposed expenditures for such projects, including all revisions to such proposed expenditures, for the current fiscal year and for ensuing fiscal years.~~

Sec. 11. K.S.A. 75-7211 is hereby amended to read as follows: 75-7211. (a) The ~~legislative chief information technology officer, under the direction of the~~ joint committee~~,~~ shall monitor state agency execution of *reported* information technology projects ~~and, at times agreed upon by~~. *The joint committee shall require* the three chief information technology officers~~,~~ ~~shall~~ *to* report progress regarding the implementation of such projects and all proposed expenditures therefor, including all revisions to such proposed expenditures for the current fiscal year and for ensuing fiscal years.

(b) *For information technology projects, the joint committee may:*

(1) Require the head of ~~a~~ *any* state agency with primary responsibility for an information technology project ~~may authorize or approve, without prior consultation with the joint committee, any change in planned expenditures for an information technology project that would result in the total cost of the project being increased above the currently authorized cost of such project but that increases the total cost of such project by less than the lower of either $1,000,000 or 10% of the currently authorized cost, and any change in planned expenditures for an information technology project involving a cost reduction, other than a change in 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~~ *to advise and consult on the status and progress of such information technology project, including revisions to expenditures for the current fiscal year and ensuing fiscal years; and*

(2) report on the status and progress of such information technology projects to the senate standing committee on ways and means, the house of representatives standing committee on appropriations and the legislative budget committee.

(c) *Prior to authorizing or approving any information technology project change or overrun,* the head of a state agency with primary responsibility for ~~an~~ *such* information technology project shall ~~not authorize or approve, without first advising and consulting with the joint committee any information technology project change or overrun~~ *report all such information technology project changes or overruns to the joint committee through the chief information technology officer of the branch of state government of which the agency is a part pursuant to the information technology executive council's policy*. The joint committee shall report all such changes and overruns to the senate standing committee on ways and means ~~and~~, the house *of representatives* standing committee on appropriations *and the legislative budget committee*.

Sec. 12. K.S.A. 75-7237 is hereby amended to read as follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and amendments thereto:

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

(b) "Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an executive

branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

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

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

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

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

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

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

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

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

(i) Social security number;

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

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

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

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

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

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

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

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

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

Sec. 13. K.S.A. 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. The 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 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; ~~and~~

(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.

Sec. 14. K.S.A. 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 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 ~~department of administration~~ *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 CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) assist the executive branch in developing, implementing and monitoring 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) 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 ~~that are in~~ *to ensure* compliance with applicable state and federal laws ~~and~~, rules and regulations*, executive branch policies and standards and policies* and standards adopted by the information technology executive council;

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

~~(9)~~*(10)* liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

~~(10)~~*(11)* assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;

~~(11)~~*(12)* assist executive branch agencies to create a framework for roles and responsibilities relating to information ownership, classification, accountability and protection;

~~(12)~~*(13)* ensure a cybersecurity ~~training program is provided to executive branch agencies at no cost to the agencies~~ *awareness training program is made available to all branches of state government*;

~~(13) provide cybersecurity threat briefings to the information technology executive council;~~

~~(14) provide an annual status report of executive branch cybersecurity programs of executive branch agencies to the joint committee on information technology and the house committee on government, technology and security;~~ and

~~(15)~~*(14)* perform such other functions and duties as provided by law and as directed by the CISO.

(d) Results of audits conducted pursuant to subsection (c)(8) 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.

Sec. 15. K.S.A. 75-7240 is hereby amended to read as follows: 75-7240. *(a)* The executive branch agency heads shall:

~~(a)~~*(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:

~~(1)~~*(A)* Agency sites;

~~(2)~~*(B)* agency real property;

~~(3)~~*(C)* infrastructure in state data centers;

~~(4)~~*(D)* third-party locations; and

~~(5)~~*(E)* in transit between locations;

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

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

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

~~(e)~~*(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;

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

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

~~(h) (1)~~*(8) (A)* submit a cybersecurity ~~assessment~~ *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 ~~a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or the data processing of the agency or of a contractor of~~ 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;

~~(2)~~*(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*. This provision regarding confidentiality shall expire on July 1, 2023, unless the legislature reviews and reenacts such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023; and

~~(3)~~*(C)* prepare or have prepared a ~~summary~~ *financial summary identifying cybersecurity expenditures addressing the findings* of the cybersecurity ~~assessment~~ *self-assessment* report required in ~~paragraph (1)~~ *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 ~~government, technology and security or its successor committee~~ *appropriations* and the senate committee on ways and means;

~~(i) participate in annual agency leadership training to ensure understanding of: (1) The information and information systems that support the operations and assets of the agency; (2) The potential impact of common types of cyberattacks and data breaches on the agency's operations and assets; (3) how cyberattacks and data breaches on the agency's operations and assets could impact the operations and assets of other governmental entities on the state enterprise network; (4) how cyberattacks and data breaches occur; (5) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and (6) the annual reporting requirements required of the executive director or agency head;~~ and

~~(j)~~*(9)* 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:

~~(1)~~*(A)* Comply with the notification requirements set out in K.S.A. 2022 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

~~(2)~~*(B)* not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: ~~(A)~~*(i)* The CISO; and ~~(B)~~*(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;

(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.

(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. 16. K.S.A. 75-7242 is hereby amended to read as follows: 75-7242. Information collected to effectuate this act shall be considered confidential by ~~the executive branch agency and KISO~~ *all state and local governmental organizations* unless all data elements or information that specifically identifies a target, vulnerability or weakness that would place the organization at risk have been redacted, including: (a) System information logs; (b) vulnerability reports; (c) risk assessment reports; (d) system security plans; (e) detailed system design plans; (f) network or system diagrams; and (g) audit reports. The provisions of this section shall expire on July 1, 2023, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023.

Sec. 17. K.S.A. 46-2102, 74-5704, 75-7201, 75-7202, 75-7205, 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238, 75-7239, 75-7240 and 75-7242 are hereby repealed.

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

I hereby certify that the above BILL originated in the HOUSE, and was adopted by that body

_____

HOUSE adopted
Conference Committee Report_____

_____
Speaker of the House.

_____
Chief Clerk of the House.

Passed the SENATE
as amended _____

SENATE adopted
Conference Committee Report_____

_____
President of the Senate.

_____
Secretary of the Senate.

APPROVED _____

_____
Governor.