

Substitute for HOUSE BILL No. 2077

By Committee on Appropriations

2-9

1 AN ACT concerning information technology; requiring reporting of
2 significant cybersecurity incidents; changing membership, terms and
3 quorum requirements for the information technology executive council;
4 relating to information technology projects and reporting requirements;
5 information technology security training and cybersecurity reports;
6 duties of the chief information security officer; requiring certain
7 information to be provided to the joint committee on information
8 technology; amending K.S.A. 46-2102, 75-7201, 75-7202, 75-7205,
9 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238, 75-
10 7239, 75-7240 and 75-7242 and repealing the existing sections.

11

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

13 New Section 1. (a) Any entity that transmits, receives, processes or
14 stores personal information that is provided by the state of Kansas or
15 supports information systems operated by the state of Kansas or any
16 governmental entity that accesses information systems operated by the
17 state of Kansas that has a significant cybersecurity incident shall, not later
18 than 12 hours after the discovery of the significant cybersecurity incident,
19 notify the Kansas information security office and, if the significant
20 cybersecurity incident involves election data, the secretary of state.

21 (b) (1) The information provided pursuant to subsection (a) shall only
22 be shared with individuals who need to know such information for
23 response and defensive activities to preserve the integrity of state
24 information systems and networks or to provide assistance if requested.

25 (2) Such information shall be confidential and shall not be subject to
26 disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and
27 amendments thereto. This paragraph shall expire on July 1, 2028, unless
28 the legislature reviews and acts to continue such provision pursuant to
29 K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.

30 (3) The Kansas information security office shall only report the
31 information provided pursuant to subsection (a) as aggregate data.

32 (c) For the purposes of this section, "significant cybersecurity
33 incident" means a cybersecurity event, incident, breach, suspected breach
34 or unauthorized disclosure that requires the entity to initiate a response or
35 recovery.

36 Sec. 2. K.S.A. 46-2102 is hereby amended to read as follows: 46-

1 2102. In addition to other powers and duties authorized or prescribed by
2 law or by the legislative coordinating council, the joint committee on
3 information technology shall:

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

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

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

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

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

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

32 Sec. 3. K.S.A. 75-7201 is hereby amended to read as follows: 75-
33 7201. As used in K.S.A. 75-7201 through 75-7212, and amendments
34 thereto:

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

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

43 ~~(b)~~(c) "Executive agency" means any state agency in the executive

1 branch of government.

2 ~~(e)~~(d) "Information technology project" means a project for a major
3 computer, telecommunications or other information technology
4 improvement with an estimated cumulative cost of \$250,000 or more and
5 includes any such project that has proposed expenditures for: (1) New or
6 replacement equipment or software; (2) upgrade improvements to existing
7 equipment and any computer systems, programs or software upgrades
8 therefor; or (3) data or consulting or other professional services for such a
9 project *an information technology effort by a state agency of defined and*
10 *limited duration that implements, effects a change in or presents a risk to*
11 *processes, services, security, systems, records, data, human resources or*
12 *architecture.*

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

15 (1) ~~Any change in~~ Planned expenditures for an information
16 technology project that would result in the total authorized cost of the
17 project being increased above the currently authorized cost of such project
18 by more than ~~either \$1,000,000 or 10%~~ of such currently authorized cost
19 of such project, ~~whichever is lower~~ *or an established threshold within the*
20 *information technology executive council's policies;*

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

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

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

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

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

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

42 ~~(i)~~(j) "Project completion" means the date and time when the head of
43 a state agency having primary responsibility for an information technology

1 project certifies that the improvement being produced or altered under the
2 project is ready for operational use.

3 ~~(j)~~(k) "Project start" means the date and time when a state agency
4 begins a formal study of a business process or technology concept to
5 assess the needs of the state agency, determines project feasibility or
6 prepares an information technology project budget estimate under K.S.A.
7 75-7209, and amendments thereto.

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

11 Sec. 4. K.S.A. 75-7202 is hereby amended to read as follows: 75-
12 7202. (a) There is hereby established the information technology executive
13 council which shall be attached to the office of information technology
14 services for purposes of administrative functions.

15 (b) (I) The council shall be composed of 17 voting members as
16 follows:

- 17 (A) Two cabinet agency heads or such persons' designees;
- 18 (B) two noncabinet agency heads or such persons' designees;
- 19 (C) the executive chief information technology officer;
- 20 (D) the legislative chief information technology officer;
- 21 (E) the judicial chief information technology officer;
- 22 (F) the chief executive officer of the state board of regents or such
23 person's designee;

24 (G) one representative of cities;

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

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

32 (J) one representative appointed by the Kansas criminal justice
33 information system committee;

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

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

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

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

1 (2) The chief information technology architect shall be a nonvoting
2 member of the council.

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

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

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

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

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

32 Sec. 5. K.S.A. 75-7205 is hereby amended to read as follows: 75-
33 7205. (a) There is hereby established within and as a part of the office of
34 information technology services the position of executive chief
35 information technology officer. The executive chief information
36 technology officer shall be in the unclassified service under the Kansas
37 civil service act, shall be appointed by the governor, and shall receive
38 compensation in an amount fixed by the governor. The executive chief
39 information technology officer shall maintain a presence in any cabinet
40 established by the governor and shall report to the governor.

41 (b) The executive chief information technology officer shall:

42 (1) Review and consult with each executive agency regarding
43 information technology plans, deviations from the state information

1 technology architecture, information technology project estimates and
2 information technology project changes and overruns submitted by such
3 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine
4 whether the agency has complied with:

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

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

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

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

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

17 (3) submit recommendations to the division of the budget as to the
18 technical and management merit of information technology ~~project~~
19 ~~estimates~~ *projects* and information technology project changes and
20 overruns submitted by executive agencies *that are reportable* pursuant to
21 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
22 ~~made pursuant to subsection (b)(1)~~;

23 (4) monitor executive agencies' compliance with:

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

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

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

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

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

36 (6) designate the ownership of information resource processes and the
37 lead agency for implementation of new technologies and networks shared
38 by multiple agencies within the executive branch of state government; and

39 (7) perform such other functions and duties as provided by law or as
40 directed by the governor.

41 Sec. 6. K.S.A. 75-7206 is hereby amended to read as follows: 75-
42 7206. (a) There is hereby established within and as a part of the office of
43 the state judicial administrator the position of judicial chief information

1 technology officer. The judicial chief information technology officer shall
2 be appointed by the judicial administrator, subject to approval of the chief
3 justice, and shall receive compensation determined by the judicial
4 administrator, subject to approval of the chief justice.

5 (b) The judicial chief information technology officer shall:

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

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

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

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

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

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

24 (3) submit recommendations to the judicial administrator as to the
25 technical and management merit of information technology ~~project~~
26 ~~estimates~~ *projects* and information technology project changes and
27 overruns submitted by judicial agencies *that are reportable* pursuant to
28 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
29 ~~pursuant to subsection (b)(1)~~;

30 (4) monitor judicial agencies' compliance with:

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

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

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

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

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

43 (6) designate the ownership of information resource processes and the

1 lead agency for implementation of new technologies and networks shared
2 by multiple agencies within the judicial branch of state government; and

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

5 Sec. 7. K.S.A. 75-7208 is hereby amended to read as follows: 75-
6 7208. The legislative chief information technology officer shall:

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

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

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

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

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

22 (b) report to the chief information technology architect all deviations
23 from the state information architecture that are reported to the legislative
24 information technology officer by legislative agencies;

25 (c) submit recommendations to the legislative coordinating council as
26 to the technical and management merit of information technology ~~project~~
27 ~~estimates~~ *projects* and information technology project changes and
28 overruns submitted by legislative agencies *that are reportable* pursuant to
29 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
30 ~~pursuant to subsection (a)~~;

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

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

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

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

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

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

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

4 (g) serve as staff of the joint committee; and

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

7 Sec. 8. K.S.A. 75-7209 is hereby amended to read as follows: 75-

8 7209. (a) (1) Whenever an agency proposes an information technology
9 project, such agency shall prepare and submit *information technology*
10 *project documentation* to the chief information technology officer of the
11 branch of state government of which the agency is a part of a project
12 budget estimate therefor, and for each amendment or revision thereof, in
13 accordance with this section. Each information technology project budget
14 estimate shall be in such form as required by the director of the budget, in
15 consultation with the chief information technology architect, and by this
16 section. In each case, the agency shall prepare and include as a part of such
17 project budget estimate a plan consisting of a written program statement
18 describing the project. The program statement shall:

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

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

29 (3) include a financial plan showing: (A) The proposed source of
30 funding and categorized expenditures for each phase of the project; and
31 (B) cost estimates for any needs analyses or other investigations,
32 consulting or other professional services, computer programs, data,
33 equipment, buildings or major repairs or improvements to buildings and
34 other items or services necessary for the project; and

35 (4) include a cost-benefit statement based on an analysis of
36 qualitative as well as financial benefits. *Such information technology*
37 *project documentation shall:*

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

1 (B) be consistent with:

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

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

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

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

10 (2) Any information technology project with significant business risk,
11 as determined pursuant to the information technology executive council's
12 policies, shall be presented to the joint committee on information
13 technology by such branch chief information technology officer.

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

22 (2) ~~All specifications for bids or proposals related to an approved~~
23 ~~information technology project of one or more state agencies shall be~~
24 ~~reviewed by the chief information technology officer of each branch of~~
25 ~~state government of which the agency or agencies are a part. Prior to the~~
26 ~~release of any request for proposal for an information technology project~~
27 ~~with significant business risk:~~

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

34 (B) (i) ~~The chief information technology officer of the appropriate~~
35 ~~branch over the state agency or agencies that are involved in such project~~
36 ~~shall submit the project, the project plan, including the architecture, and~~
37 ~~the cost-benefit analysis to the joint committee on information technology~~
38 ~~to advise and consult on the project. Such chief information technology~~
39 ~~officer shall submit such information to each member of the joint~~
40 ~~committee and to the director of the legislative research department. Each~~
41 ~~such project plan summary shall include a notice specifying the date the~~
42 ~~summary was mailed or emailed. After receiving any such project plan~~
43 ~~summary, each member shall review the information and may submit~~

1 questions, requests for additional information or request a presentation
2 and review of the proposed project at a meeting of the joint committee. If
3 two or more members of the joint committee contact the director of the
4 legislative research department within seven business days of the date
5 specified in the summary description and request that the joint committee
6 schedule a meeting for such presentation and review, then the director of
7 the legislative research department shall notify the chief information
8 technology officer of the appropriate branch, the head of such agency and
9 the chairperson of the joint committee that a meeting has been requested
10 for such presentation and review on the next business day following the
11 members' contact with the director of the legislative research department.
12 Upon receiving such notification, the chairperson shall call a meeting of
13 the joint committee as soon as practicable for the purpose of such
14 presentation and review and shall furnish the chief information technology
15 officer of the appropriate branch and the head of such agency with notice
16 of the time, date and place of the meeting. Except as provided in
17 subsection (b)(1)(B)(ii), the state agency shall not authorize or approve
18 the release of any request for proposal or other bid event for an
19 information technology project without having first advised and consulted
20 with the joint committee at a meeting.

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

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

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

37 ~~(3)(2)~~ (A) Agencies are prohibited from contracting with a vendor to
38 implement the project if that vendor prepared or assisted in the preparation
39 of the program statement ~~required under subsection (a)~~, the project
40 planning documents ~~required under subsection (b)(1)~~, or any other project
41 plans prepared prior to the project being approved by the chief information
42 technology officer as required ~~under subsection (b)(1)~~ by this section.

43 (B) Information technology projects with an estimated cumulative

1 cost of less than \$5,000,000 are exempted from the provisions of
2 subparagraph (A).

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

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

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

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

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

17 Sec. 9. K.S.A. 75-7210 is hereby amended to read as follows: 75-
18 7210. ~~(a) Not later than October~~ *November* 1 of each year, the executive,
19 judicial and legislative chief information technology officers shall submit
20 to the joint committee and to the legislative research department all
21 information technology project budget estimates and amendments and
22 revisions thereto, all three-year plans and all deviations from the state
23 information technology architecture submitted to such officers pursuant to
24 K.S.A. 75-7209, and amendments thereto. ~~The legislative chief~~
25 ~~information technology officer~~ *joint committee* shall review all such
26 estimates and amendments and revisions thereto, plans and deviations and
27 shall make recommendations to the ~~joint committee~~ *house standing*
28 *committee on appropriations and the senate standing committee on ways*
29 *and means* regarding the merit thereof and appropriations therefor.

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

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

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

39 Sec. 10. K.S.A. 75-7211 is hereby amended to read as follows: 75-
40 7211. (a) ~~The legislative chief information technology officer, under the~~
41 ~~direction of the joint committee,~~ shall monitor state agency execution of
42 *reported* information technology projects ~~and, at times agreed upon by.~~
43 *The joint committee shall require* the three chief information technology

1 officers, ~~shall~~ to report progress regarding the implementation of such
2 projects and all proposed expenditures therefor, including all revisions to
3 such proposed expenditures for the current fiscal year and for ensuing
4 fiscal years.

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

6 (1) *Require the head of a any state agency with primary responsibility*
7 *for an information technology project may authorize or approve, without*
8 *prior consultation with the joint committee, any change in planned*
9 *expenditures for an information technology project that would result in the*
10 *total cost of the project being increased above the currently authorized cost*
11 *of such project but that increases the total cost of such project by less than*
12 *the lower of either \$1,000,000 or 10% of the currently authorized cost, and*
13 *any change in planned expenditures for an information technology project*
14 *involving a cost reduction, other than a change in the proposed use of any*
15 *new or replacement information technology equipment or in the use of any*
16 *existing information technology equipment that has been significantly*
17 *upgraded to advise and consult on the status and progress of such*
18 *information technology project, including revisions to expenditures for the*
19 *current fiscal year and ensuing fiscal years; and*

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

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

36 Sec. 11. K.S.A. 75-7237 is hereby amended to read as follows: 75-
37 7237. As used in K.S.A. 75-7236 through 75-7243, and amendments
38 thereto:

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

40 (b) "Breach" or "breach of security" means unauthorized access of
41 data in electronic form containing personal information. Good faith access
42 of personal information by an employee or agent of an executive branch
43 agency does not constitute a breach of security, provided that the

1 information is not used for a purpose unrelated to the business or subject to
2 further unauthorized use.

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

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

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

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

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

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

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

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

22 (i) Social security number;

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

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

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

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

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

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

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

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

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

3 Sec. 12. K.S.A. 75-7238 is hereby amended to read as follows: 75-
4 7238. (a) There is hereby established the position of executive branch chief
5 information security officer. The CISO shall be in the unclassified service
6 under the Kansas civil service act, shall be appointed by the governor and
7 shall receive compensation in an amount fixed by the governor.

8 (b) The CISO shall:

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

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

12 (3) serve as the executive branch chief cybersecurity strategist and
13 authority on policies, compliance, procedures, guidance and technologies
14 impacting executive branch cybersecurity programs;

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

18 (5) coordinate cybersecurity efforts between executive branch
19 agencies;

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

23 (7) *set cybersecurity policy and standards for executive branch*
24 *agencies; and*

25 (8) perform such other functions and duties as provided by law and as
26 directed by the executive chief information technology officer.

27 Sec. 13. K.S.A. 75-7239 is hereby amended to read as follows: 75-
28 7239. (a) There is hereby established within and as a part of the office of
29 information technology services the Kansas information security office.
30 The Kansas information security office shall be administered by the CISO
31 and be staffed appropriately to effect the provisions of the Kansas
32 cybersecurity act.

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

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

2 (1) Administer the Kansas cybersecurity act;

3 (2) assist the executive branch in developing, implementing and
4 monitoring strategic and comprehensive information security risk-
5 management programs;

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

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

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

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

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

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

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

30 ~~(9)~~(10) liaise with external agencies, such as law enforcement and
31 other advisory bodies as necessary, to ensure a strong security posture;

32 ~~(10)~~(11) assist in the development of plans and procedures to manage
33 and recover business-critical services in the event of a cyberattack or other
34 disaster;

35 ~~(11)~~(12) assist executive branch agencies to create a framework for
36 roles and responsibilities relating to information ownership, classification,
37 accountability and protection;

38 ~~(12)~~(13) ~~ensure a cybersecurity training program is provided to~~
39 ~~executive branch agencies at no cost to the agencies~~ *awareness training*
40 *program is made available to all branches of state government;*

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

43 ~~(14)~~ ~~provide an annual status report of executive branch cybersecurity~~

1 ~~programs of executive branch agencies to the joint committee on~~
2 ~~information technology and the house committee on government,~~
3 ~~technology and security; and~~

4 ~~(15)(14)~~ perform such other functions and duties as provided by law
5 and as directed by the CISO.

6 *(d) Results of audits conducted pursuant to subsection (c)(8) shall be*
7 *confidential and shall not be subject to discovery or disclosure pursuant to*
8 *the open records act, K.S.A. 45-215 et seq., and amendments thereto. The*
9 *provisions of this subsection shall expire on July 1, 2028, unless the*
10 *legislature reviews and acts to continue such provision pursuant to K.S.A.*
11 *45-229, and amendments thereto, prior to July 1, 2028.*

12 Sec. 14. K.S.A. 75-7240 is hereby amended to read as follows: 75-
13 7240. (a) The executive branch agency heads shall:

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

- 17 ~~(1)(A)~~ Agency sites;
- 18 ~~(2)(B)~~ agency real property;
- 19 ~~(3)(C)~~ infrastructure in state data centers;
- 20 ~~(4)(D)~~ third-party locations; and
- 21 ~~(5)(E)~~ in transit between locations;

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

24 ~~(e)(3)~~ designate an information security officer to administer the
25 agency's information security program that reports directly to executive
26 leadership;

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

29 ~~(e)(5)~~ implement policies and standards to ensure that all the agency's
30 data and information technology resources are maintained in compliance
31 with applicable state and federal laws and rules and regulations;

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

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

38 ~~(h)(1)(8) (A)~~ submit a cybersecurity ~~assessment~~ *self-assessment*
39 report to the CISO by October 16 of each even-numbered year, including
40 an executive summary of the findings, that assesses the extent to which a
41 ~~computer, a computer program, a computer network, a computer system, a~~
42 ~~printer, an interface to a computer system, including mobile and peripheral~~
43 ~~devices, computer software, or the data processing of the agency or of a~~

1 contractor of the agency is vulnerable to unauthorized access or harm,
2 including the extent to which the agency's or contractor's electronically
3 stored information is vulnerable to alteration, damage, erasure or
4 inappropriate use;

5 ~~(2)~~(B) ensure that the agency conducts annual internal assessments of
6 its security program. Internal assessment results shall be considered
7 confidential and shall not be subject to discovery by or release to any
8 person or agency, outside of the KISO or CISO, *without authorization*
9 *from the executive branch agency director or head.* This provision
10 regarding confidentiality shall expire on July 1, 2023, unless the
11 legislature reviews and reenacts such provision pursuant to K.S.A. 45-229,
12 and amendments thereto, prior to July 1, 2023; and

13 ~~(3)~~(C) prepare or have prepared a ~~summary~~ *financial summary*
14 *identifying cybersecurity expenditures addressing the findings* of the
15 ~~cybersecurity assessment self-assessment~~ report required in ~~paragraph (1)~~
16 ~~subparagraph (A)~~, excluding information that might put the data or
17 information resources of the agency or its contractors at risk and submit
18 such report to the house of representatives committee on ~~government,~~
19 ~~technology and security or its successor committee appropriations~~ and the
20 senate committee on ways and means;

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

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

37 ~~(1)~~(A) Comply with the notification requirements set out in K.S.A.
38 2022 Supp. 50-7a01 et seq., and amendments thereto, and applicable
39 federal laws and rules and regulations, to the same extent as a person who
40 conducts business in this state; and

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

1 election data, the secretary of state.

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

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

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

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

10 (C) *how cyberattacks and data breaches occur; and*

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

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

17 (3) *require that all employees with access to information technology*
18 *receive a minimum of one hour of information technology security training*
19 *per year.*

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

28 (2) *Self-assessment reports made to the CISO pursuant to subsection*
29 *(a)(8)(A) shall be confidential and shall not be subject to the provisions of*
30 *the Kansas open records act, K.S.A. 45-215 et seq., and amendments*
31 *thereto. The provisions of this paragraph shall expire on July 1, 2028,*
32 *unless the legislature reviews and reenacts this provision pursuant to*
33 *K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.*

34 Sec. 15. K.S.A. 75-7242 is hereby amended to read as follows: 75-
35 7242. Information collected to effectuate this act shall be considered
36 confidential by ~~the executive branch agency and KISO~~ *all state and local*
37 *governmental organizations* unless all data elements or information that
38 specifically identifies a target, vulnerability or weakness that would place
39 the organization at risk have been redacted, including: (a) System
40 information logs; (b) vulnerability reports; (c) risk assessment reports; (d)
41 system security plans; (e) detailed system design plans; (f) network or
42 system diagrams; and (g) audit reports. The provisions of this section shall
43 expire on July 1, 2023, unless the legislature reviews and reenacts this

1 provision pursuant to K.S.A. 45-229, and amendments thereto, prior to
2 July 1, 2023.

3 Sec. 16. K.S.A. 46-2102, 75-7201, 75-7202, 75-7205, 75-7206, 75-
4 7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238, 75-7239, 75-7240
5 and 75-7242 are hereby repealed.

6 Sec. 17. This act shall take effect and be in force from and after its
7 publication in the statute book.