

HOUSE BILL No. 2574

By Joint Committee on Information Technology

1-28

1 AN ACT concerning cybersecurity; relating to consolidation of
2 cybersecurity services; modifying the duties of the chief information
3 security officers for each branch of government, removing maturity
4 requirements for cybersecurity programs; requiring periodic audits of
5 such programs; creating the judicial branch technology oversight
6 council; requiring the executive branch chief information security
7 officer to assess executive branch agencies for compliance with
8 cybersecurity standards and report findings to the legislature; providing
9 for consideration of cybersecurity compliance during the budgeting
10 process; modifying the membership and duties of the information
11 technology executive council; amending K.S.A. 2025 Supp. 40-110,
12 75-413, 75-623, 75-710, 75-711, 75-7202, 75-7203, 75-7206a, 75-
13 7208a, 75-7237, 75-7238, 75-7239, 75-7240, 75-7245 and 75-7246 and
14 repealing the existing sections; also repealing K.S.A. 75-7203, as
15 amended by section 21 of chapter 95 of the 2024 Session Laws of
16 Kansas, and 75-7205, as amended by section 23 of chapter 95 of the
17 2024 Session Laws of Kansas and K.S.A. 2023 Supp. 75-7201, as
18 amended by section 17 of chapter 95 of the 2024 Session Laws of
19 Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024
20 Session Laws of Kansas, 75-7206, as amended by section 25 of chapter
21 95 of the 2024 Session Laws of Kansas, 75-7208, as amended by
22 section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209,
23 as amended by section 29 of chapter 95 of the 2024 Session Laws of
24 Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024
25 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter
26 95 of the 2024 Session Laws of Kansas, 75-7239, as amended by
27 section 35 of chapter 95 of the 2024 Session Laws of Kansas, and 75-
28 7240, as amended by section 37 of chapter 95 of the 2024 Session
29 Laws of Kansas.

30

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

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

- 35 (a) Set standards for judicial branch information technology;
36 (b) establish information technology policies for the judicial branch;

- 1 (c) approve strategic information technology plans;
- 2 (d) oversee information technology projects to ensure alignment with
- 3 judicial branch goals;
- 4 (e) evaluate information technology and cybersecurity programs; and
- 5 (f) support the judicial chief information technology officer and the
- 6 judicial branch chief information security officer.

7 Sec. 2. K.S.A. 2025 Supp. 40-110 is hereby amended to read as
8 follows: 40-110. (a) The commissioner of insurance is hereby authorized
9 to appoint an assistant commissioner of insurance, actuaries, two special
10 attorneys who shall have been regularly admitted to practice, an executive
11 secretary, policy examiners, two field representatives, and a secretary to
12 the commissioner. Such appointees shall each receive an annual salary to
13 be determined by the commissioner of insurance, within the limits of
14 available appropriations. The commissioner is also authorized to appoint,
15 within the provisions of the civil service law, and available appropriations,
16 other employees as necessary to administer the provisions of this act. The
17 field representatives authorized by this section may be empowered to
18 conduct inquiries, investigations or to receive complaints. Such field
19 representatives shall not be empowered to make, or direct to be made, an
20 examination of the affairs and financial condition of any insurance
21 company in the process of organization, or applying for admission or
22 doing business in this state.

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

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

37 (A)(1) Develop a cybersecurity program for the department—that
38 complies with based on the national institute of standards and technology
39 cybersecurity framework (CSF) 2.0, as in effect on July 1, 2026.
40 Beginning in 2027 and every two years thereafter, the chief information
41 security officer shall ensure that such programs achieve a CSF tier of 3.0
42 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030 report to
43 the joint committee on information technology, the house of

1 *representatives standing committee on appropriations and the senate*
2 *standing committee on ways and means on the maturity level of the*
3 *program;*

4 (B)(2) ensure that the commissioner and all employees complete
5 cybersecurity awareness training annually and that if an employee does not
6 complete the required training, such employee's access to any state-issued
7 hardware or the state network is revoked; and

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

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

16 (ii)(B) Results of audits conducted pursuant to this paragraph shall be
17 confidential and shall not be subject to discovery or disclosure pursuant to
18 the open records act, K.S.A. 45-215 et seq., and amendments thereto. *The*
19 *provisions of this subparagraph shall expire on July 1, 2030, unless the*
20 *legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,*
21 *and amendments thereto.*

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

23 Sec. 3. K.S.A. 2025 Supp. 75-413 is hereby amended to read as
24 follows: 75-413. (a) The secretary of state may appoint such other
25 assistants and clerks as may be authorized by law, but the secretary of state
26 shall be responsible for the proper discharge of the duties of all assistants
27 and clerks, and they shall hold their offices at the will and pleasure of the
28 secretary and shall do and perform such general duties as the secretary
29 may require.

30 (b) ~~(1)~~ The secretary of state shall appoint a chief information
31 security officer who shall be responsible for establishing security standards
32 and policies to protect the office's information technology systems and
33 infrastructure. The chief information security officer shall:

34 (A)(1) Develop a cybersecurity program for the office ~~that complies~~
35 ~~with based on~~ the national institute of standards and technology
36 cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ 2026.
37 ~~Beginning in 2027 and every two years thereafter, the chief information~~
38 ~~security officer shall ensure that such programs achieve a CSF tier of 3.0~~
39 ~~prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030 report to~~
40 ~~the joint committee on information technology, the house of~~
41 ~~representatives standing committee on appropriations and the senate~~
42 ~~standing committee on ways and means on the maturity level of the~~
43 *program;*

1 (B)(2) ensure that the secretary of state and all employees complete
2 cybersecurity awareness training annually and that if an employee does not
3 complete the required training, such employee's access to any state-issued
4 hardware or the state network is revoked; and

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

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

13 (iii)(B) Results of audits conducted pursuant to this paragraph shall be
14 confidential and shall not be subject to discovery or disclosure pursuant to
15 the open records act, K.S.A. 45-215 et seq., and amendments thereto. *The
16 provisions of this subparagraph shall expire on July 1, 2030, unless the
17 legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,
18 and amendments thereto.*

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

20 Sec. 4. K.S.A. 2025 Supp. 75-623 is hereby amended to read as
21 follows: 75-623. (a) The treasurer shall appoint such other assistants,
22 clerks, bookkeepers, accountants and stenographers as may be authorized
23 by law, each of which persons shall take the oath of office required of
24 public officers. Such persons shall hold their offices at the will and
25 pleasure of the state treasurer.

26 (b) (1) The treasurer shall appoint a chief information security officer
27 who shall be responsible for establishing security standards and policies to
28 protect the office's information technology systems and infrastructure. The
29 chief information security officer shall:

30 (A)(1) Develop a cybersecurity program for the office that complies
31 with based on the national institute of standards and technology
32 cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024 2026.
33 *Beginning in 2027 and every two years thereafter, the chief information*
34 *security officer shall ensure that such programs achieve a CSF tier of 3.0*
35 *prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030 report to*
36 *the joint committee on information technology, the house of*
37 *representatives standing committee on appropriations and the senate*
38 *standing committee on ways and means on the maturity level of the*
39 *program;*

40 (B)(2) ensure that the treasurer and all employees complete
41 cybersecurity awareness training annually and that if an employee does not
42 complete the required training, such employee's access to any state-issued
43 hardware or the state network is revoked; and

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

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

9 (ii)(B) Results of audits conducted pursuant to this paragraph shall be
10 confidential and shall not be subject to discovery or disclosure pursuant to
11 the open records act, K.S.A. 45-215 et seq., and amendments thereto. *The*
12 *provisions of this subparagraph shall expire on July 1, 2030, unless the*
13 *legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,*
14 *and amendments thereto.*

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

16 Sec. 5. K.S.A. 2025 Supp. 75-710 is hereby amended to read as
17 follows: 75-710. (a) The attorney general shall appoint such assistants,
18 clerks, and stenographers as shall be authorized by law, and who shall hold
19 their office at the will and pleasure of the attorney general. All fees and
20 allowances earned by said assistants or any of them, or allowed to them by
21 any statute or order of court in any civil or criminal case whatsoever, shall
22 be turned into the general revenue fund of the state treasury, and the
23 vouchers for their monthly salaries shall not be honored by the director of
24 accounts and reports until a verified account of the fees collected by them,
25 or either of them, during the preceding month, has been filed in the
26 director of accounts and reports' office. Assistants appointed by the
27 attorney general shall perform the duties and exercise the powers as
28 prescribed by law and shall perform other duties as prescribed by the
29 attorney general. Assistants shall act for and exercise the power of the
30 attorney general to the extent the attorney general delegates them the
31 authority to do so.

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

36 (A)(1) Develop a cybersecurity program for the office ~~that complies~~
37 ~~with~~ based on the national institute of standards and technology
38 cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ 2026.
39 *Beginning in 2027 and every two years thereafter,* the chief information
40 security officer shall ensure that such programs achieve a CSF tier of 3.0
41 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030 report to
42 the joint committee on information technology, the house of
43 representatives standing committee on appropriations and the senate

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

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

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

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

15 (H)(B) Results of audits conducted pursuant to this paragraph shall be
16 confidential and shall not be subject to discovery or disclosure pursuant to
17 the open records act, K.S.A. 45-215 et seq., and amendments thereto. *The*
18 *provisions of this subparagraph shall expire on July 1, 2030, unless the*
19 *legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,*
20 *and amendments thereto.*

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

22 Sec. 6. K.S.A. 2025 Supp. 75-711 is hereby amended to read as
23 follows: 75-711. (a) There is hereby established, under the jurisdiction of
24 the attorney general, a division to be known as the Kansas bureau of
25 investigation. The director of the bureau shall be appointed by the attorney
26 general, subject to confirmation by the senate as provided in K.S.A. 75-
27 4315b, and amendments thereto, and shall have special training and
28 qualifications for such position. Except as provided by K.S.A. 46-2601,
29 and amendments thereto, no person appointed as director shall exercise
30 any power, duty or function as director until confirmed by the senate. In
31 accordance with appropriation acts, the director shall appoint agents who
32 shall be trained in the detection and apprehension of criminals. The
33 director shall appoint an associate director, and any such assistant directors
34 from within the agency as are necessary for the efficient operation of the
35 bureau, who shall have the qualifications and employee benefits, including
36 longevity, of an agent. The director also may appoint a deputy director
37 and, in accordance with appropriation acts, such administrative employees
38 as are necessary for the efficient operation of the bureau. No person shall
39 be appointed to a position within the Kansas bureau of investigation if the
40 person has been convicted of a felony.

41 (b) The director, associate director, deputy director, assistant directors
42 and any assistant attorneys general assigned to the bureau shall be within
43 the unclassified service under the Kansas civil service act. All other agents

1 and employees of the bureau shall be in the classified service under the
2 Kansas civil service act and their compensation shall be determined as
3 provided in the Kansas civil service act and shall receive actual and
4 necessary expenses.

5 (c) Any person who was a member of the bureau at the time of
6 appointment as director, associate director or assistant director, upon the
7 expiration of their appointment, shall be returned to an unclassified or
8 regular classified position under the Kansas civil service act with
9 compensation comparable to and not lower than compensation being
10 received at the time of appointment to the unclassified service. If all such
11 possible positions are filled at that time, a temporary additional position
12 shall be created for the person until a vacancy exists in the position. While
13 serving in the temporary additional position, the person shall continue to
14 be a contributing member of the retirement system for the agents of the
15 Kansas bureau of investigation.

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

19 (e)(1) The director shall appoint a chief information security officer
20 who shall be responsible for establishing security standards and policies to
21 protect the bureau's information technology systems and infrastructure.
22 The chief information security officer shall:

23 (A)(1) Develop a cybersecurity program for the bureau ~~that complies~~
24 ~~with~~ *based on* the national institute of standards and technology
25 cybersecurity framework (CSF) 2.0, as in effect on July 1, ~~2024~~ 2026.
26 *Beginning in 2027 and every two years thereafter*, the chief information
27 security officer shall ~~ensure that such programs achieve a CSF tier of 3.0~~
28 ~~prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030~~ *report to*
29 *the joint committee on information technology, the house of*
30 *representatives standing committee on appropriations and the senate*
31 *standing committee on ways and means on the maturity level of the*
32 *program*;

33 (B)(2) ensure that the director and all employees complete
34 cybersecurity awareness training annually and that if an employee does not
35 complete the required training, such employee's access to any state-issued
36 hardware or the state network is revoked; and

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

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

1 audit.

2 (ii)(B) Results of audits conducted pursuant to this paragraph shall be
3 confidential and shall not be subject to discovery or disclosure pursuant to
4 the open records act, K.S.A. 45-215 et seq., and amendments thereto. *The
5 provisions of this subparagraph shall expire on July 1, 2030, unless the
6 legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,
7 and amendments thereto.*

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

9 Sec. 7. K.S.A. 2025 Supp. 75-7202 is hereby amended to read as
10 follows: 75-7202. (a) There is hereby established the information
11 technology executive council which shall be attached to the office of
12 information technology services for purposes of administrative functions.

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

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

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

17 (C) the executive chief information technology officer;

18 (D) *the executive chief information security officer;*

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

21 (E)(F) one representative of cities;

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

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

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

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

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

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

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

40 (N) two information technology employees from state board of
41 regents institutions appointed by the board of regents.

42 (2) The chief information technology architect, the legislative chief
43 information technology officer; *and* the judicial chief information

1 technology officer, one member of the senate appointed by the president of
2 the senate, one member of the senate appointed by the minority leader of
3 the senate, one member of the house of representatives appointed by the
4 speaker of the house of representatives and one member of the house of
5 representatives appointed by the minority leader of the house of
6 representatives shall be nonvoting members of the council.

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

19 (c) The chairperson of the council shall be the executive chief
20 information technology officer.

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

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

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

34 Sec. 8. K.S.A. 2025 Supp. 75-7203 is hereby amended to read as
35 follows: 75-7203. (a) The information technology executive council is
36 hereby authorized to adopt such policies and rules and regulations as
37 necessary to implement, administer and enforce the provisions of this act.

38 (b) The council shall:

39 (1) Adopt:

40 (A) Information technology resource policies and procedures and
41 project management methodologies for all executive branch agencies;

42 (B) an information technology architecture, including
43 telecommunications systems, networks and equipment, that covers all state

1 agencies;

2 (C) standards for data management for all executive branch agencies;

3 and

4 (D) a strategic information technology management plan for the

5 executive branch;

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

7 executive branch's information technology resources;

8 (3) designate the ownership of information resource processes and the

9 lead executive branch agency for implementation of new technologies and

10 networks shared by multiple agencies within the executive branch of state

11 government; *and*

12 (4) develop a plan to integrate all information technology services for

13 the executive branch into the office of information technology services and

14 all cybersecurity services for state educational institutions as defined in

15 K.S.A. 76-711, and amendments thereto, into the office of information

16 technology services and the Kansas information security office; *and*

17 (5) perform such other functions and duties as necessary to carry out

18 the provisions of this act.

19 (e) The information technology executive council shall report the

20 plan developed under subsection (b)(4) to the senate standing committee

21 on ways and means and the house standing committee on legislative

22 modernization or its successor committee prior to January 15, 2026, in

23 accordance with K.S.A. 2025 Supp. 75-7245, and amendments thereto.

24 Sec. 9. K.S.A. 2025 Supp. 75-7206a is hereby amended to read as

25 follows: 75-7206a. (a) There is hereby established the position of judicial

26 branch chief information security officer. The judicial chief information

27 security officer shall be in the unclassified service under the Kansas civil

28 service act, shall be appointed by the judicial administrator, subject to

29 approval by the chief justice and shall receive compensation determined

30 by the judicial administrator, subject to approval of the chief justice.

31 (b) The judicial chief information security officer, *in coordination*

32 *with the judicial technology oversight council*, shall:

- 33 (1) Report to the judicial administrator;
- 34 (2) establish security standards and policies to protect the branch's
- 35 information technology systems and infrastructure in accordance with
- 36 subsection (c);
- 37 (3) ensure the confidentiality, availability and integrity of the
- 38 information transacted, stored or processed in the branch's information
- 39 technology systems and infrastructure;
- 40 (4) develop a centralized cybersecurity protocol for protecting and
- 41 managing judicial branch information technology assets and infrastructure;
- 42 (5) detect and respond to security incidents consistent with
- 43 information security standards and policies;

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

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

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

9 (9) ~~review ensure that~~ all contracts related to information technology
10 entered into by a person or entity within the judicial branch ~~to make efforts~~
11 *contain provisions* to reduce the risk of security vulnerabilities within the
12 supply chain or product and~~—ensure~~ each contract contains standard
13 security language; and

14 (10) coordinate with the United States cybersecurity and
15 infrastructure security agency to perform annual *periodic* audits of judicial
16 branch agencies *the cybersecurity program* for compliance with applicable
17 state and federal laws, rules and regulations and judicial branch policies
18 and standards. ~~The judicial chief information security officer shall make an~~
19 ~~audit request to such agency annually, regardless of whether or not such~~
20 ~~agency has the capacity to perform the requested audit.~~

21 (c) The judicial chief information security officer shall develop a
22 cybersecurity program of each judicial agency ~~that complies with~~ *based on*
23 the national institute of standards and technology cybersecurity framework
24 (CSF) 2.0, as in effect on July 1, ~~2024~~, 2026. *Beginning in 2027 and every*
25 *two years thereafter*, the judicial chief information security officer shall
26 ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028,
27 and a CSF tier of 4.0 prior to July 1, 2030 *report to the joint committee on*
28 *information technology, the house of representatives standing committee*
29 *on appropriations and the senate standing committee on ways and means*
30 *on the maturity level of the program.*

31 (d)(1) If an audit conducted pursuant to subsection (b)(10) results in
32 a failure, the judicial chief information security officer shall report such
33 failure to the speaker and minority leader of the house of representatives
34 and the president and minority leader of the senate within 30 days of
35 receiving notice of such failure. Such report shall contain a plan to
36 mitigate any security risks identified in the audit. The judicial chief
37 information security officer shall coordinate for an additional audit after
38 the mitigation plan is implemented and report the results of such audit to
39 the speaker and minority leader of the house of representatives and the
40 president and minority leader of the senate.

41 (2) Results of audits conducted pursuant to subsection (b)(10) and the
42 reports described in subsection (d)(1) shall be confidential and shall not be
43 subject to discovery or disclosure pursuant to the open records act, K.S.A.

1 45-215 et seq., and amendments thereto. *The provisions of this subsection*
2 *shall expire on July 1, 2030, unless the legislature reviews and reenacts*
3 *this provision pursuant to K.S.A. 45-229, and amendments thereto.*

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

5 Sec. 10. K.S.A. 2025 Supp. 75-7208a is hereby amended to read as
6 follows: 75-7208a. (a) There is hereby established the position of
7 legislative branch chief information security officer. The legislative chief
8 information security officer shall be in the unclassified service under the
9 Kansas civil service act, shall be appointed by the legislative coordinating
10 council and shall receive compensation determined by the legislative
11 coordinating council.

12 (b) The legislative chief information security officer shall:

13 (1) Report to the legislative chief information technology officer;
14 (2) establish security standards and policies to protect the branch's
15 information technology systems and infrastructure in accordance with
16 subsection (e);

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

20 (4) develop a centralized cybersecurity protocol for protecting and
21 managing legislative branch information technology assets and
22 infrastructure;

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

25 (6) be responsible for the cybersecurity of all legislative branch data
26 and information resources and obtain approval from the revisor of statutes
27 prior to taking any action on any matter that involves a legal issue related
28 to the security of information technology;

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

31 (8) ensure that all legislators and legislative branch employees
32 complete cybersecurity awareness training annually and if an employee
33 does not complete the required training, such employee's access to any
34 state-issued hardware or the state network is revoked;

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

39 (10) coordinate with the United States cybersecurity and
40 infrastructure security agency to perform annual audits of legislative
41 branch agencies for compliance with applicable state and federal laws,
42 rules and regulations and legislative branch policies and standards. The
43 legislative chief information security officer shall make an audit request to

1 such agency annually, regardless of whether or not such agency has the
2 capacity to perform the requested audit.

3 (e) *The legislative chief information technology officer shall appoint*
4 *a legislative chief information security officer. The legislative chief*
5 *information security officer shall develop a cybersecurity program of each*
6 *legislative agency that complies with based on the national institute of*
7 *standards and technology cybersecurity framework (CSF) 2.0, as in effect*
8 *on July 1, 2024 2026. Beginning in 2027 and every two years thereafter,*
9 *the legislative chief information security officer shall ensure that such*
10 *programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of*
11 *4.0 prior to July 1, 2030. The agency head of each legislative agency shall*
12 *coordinate with the legislative chief information security officer to achieve*
13 *such standards report to the joint committee on information technology,*
14 *the house of representatives standing committee on appropriations and the*
15 *senate standing committee on ways and means on the maturity level of the*
16 *program.*

17 (d)(b) (1) *If an audit conducted pursuant to subsection (b)(10) results*
18 *in a failure, the legislative chief information security officer shall report*
19 *such failure to the speaker and minority leader of the house of*
20 *representatives and the president and minority leader of the senate within*
21 *30 days of receiving notice of such failure. Such report shall contain a plan*
22 *to mitigate any security risks identified in the audit. The legislative chief*
23 *information security officer shall coordinate for an additional audit after*
24 *the mitigation plan is implemented and report the results of such audit to*
25 *the speaker and minority leader of the house of representatives and the*
26 *president and minority leader of the senate. The legislative chief*
27 *information security officer shall:*

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

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

36 (2) *Results of audits conducted pursuant to this subsection (b)(10)*
37 *and the reports described in subsection (d)(1) shall be confidential and*
38 *shall not be subject to discovery or disclosure pursuant to the open records*
39 *act, K.S.A. 45-215 et seq., and amendments thereto. The provisions of this*
40 *paragraph shall expire on July 1, 2030, unless the legislature reviews and*
41 *reenacts this provision pursuant to K.S.A. 45-229, and amendments*
42 *thereto.*

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

1 Sec. 11. K.S.A. 2025 Supp. 75-7237 is hereby amended to read as
2 follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and
3 amendments thereto:

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

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

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

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

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

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

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

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

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

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

31 (i) Social security number;

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

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

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

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

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

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

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

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

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

12 Sec. 12. K.S.A. 2025 Supp. 75-7238 is hereby amended to read as
13 follows: 75-7238. (a) There is hereby established the position of executive
14 branch chief information security officer (CISO). The executive CISO
15 shall be in the unclassified service under the Kansas civil service act, shall
16 be appointed by the governor and shall receive compensation in an amount
17 fixed by the governor.

18 (b) The executive CISO shall:

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

21 (2) establish security standards and policies to protect the branch's
22 information technology systems and infrastructure in accordance with
23 subsection (c);

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

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

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

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

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

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

40 (9) ~~review ensure that~~ all contracts related to information technology
41 entered into by a person or entity within the executive branch ~~to make~~
42 ~~efforts contain provisions~~ to reduce the risk of security vulnerabilities
43 within the supply chain or product and ~~ensure~~ each contract contains

1 standard security language; and
2 (10) *adopt statewide cybersecurity standards, controls, directives and*
3 *maturity and tier expectations for the executive branch and continually*
4 *evaluate standards and expectations to address evolving threats, federal*
5 *requirements, technological changes and statewide risk conditions.*

6 (c) The executive CISO shall develop a cybersecurity program for
7 each executive branch agency—that complies with *based on* the national
8 institute of standards and technology cybersecurity framework (CSF) 2.0,
9 as in effect on July 1, ~~2024~~ 2026. *Beginning in 2027 and every two years*
10 *thereafter, the executive CISO shall ensure that such programs achieve a*
11 *CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1,*
12 *2030 report to the joint committee on information technology, the house of*
13 *representatives standing committee on appropriations and the senate*
14 *standing committee on ways and means on the maturity level of the*
15 *program.* The agency head of each executive branch agency shall
16 coordinate with the executive CISO to achieve such standards.

17 Sec. 13. K.S.A. 2025 Supp. 75-7239 is hereby amended to read as
18 follows: 75-7239. (a) There is hereby established within and as a part of
19 the office of information technology services the Kansas information
20 security office. The Kansas information security office shall be
21 administered by the executive CISO and be staffed appropriately to effect
22 the provisions of the Kansas cybersecurity act.

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

33 (c) Under direction of the executive CISO, the KISO shall:
34 (1) Administer the Kansas cybersecurity act;
35 (2) develop, implement and monitor strategic and comprehensive
36 information security risk-management programs;
37 (3) facilitate a metrics, logging and reporting framework to measure
38 the efficiency and effectiveness of state information security programs;
39 (4) provide the executive branch strategic risk guidance for
40 information technology projects, including the evaluation and
41 recommendation of technical controls;
42 (5) ~~coordinate with the United States cybersecurity and infrastructure~~
43 ~~security agency to perform annual periodic audits of executive branch~~

1 ~~agencies the cybersecurity program for compliance with applicable state~~
2 ~~and federal laws, rules and regulations and executive branch policies and~~
3 ~~standards. The executive CISO shall make an audit request to such agency~~
4 ~~annually, regardless of whether or not such agency has the capacity to~~
5 ~~perform the requested audit;~~

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

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

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

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

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

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

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

26 (12)(13) perform such other functions and duties as provided by law
27 and as directed by the CISO.

28 (d)(1) ~~If an audit conducted pursuant to subsection (e)(5) results in a~~
29 ~~failure, the executive CISO shall report such failure to the speaker and~~
30 ~~minority leader of the house of representatives and the president and~~
31 ~~minority leader of the senate within 30 days of receiving notice of such~~
32 ~~failure. Such report shall contain a plan to mitigate any security risks~~
33 ~~identified in the audit. The executive CISO shall coordinate for an~~
34 ~~additional audit after the mitigation plan is implemented and report the~~
35 ~~results of such audit to the speaker and minority leader of the house of~~
36 ~~representatives and the president and minority leader of the senate.~~

37 (2) Results of audits conducted pursuant to subsection (c)(5) and the
38 reports described in subsection (d)(1) shall be confidential and shall not be
39 subject to discovery or disclosure pursuant to the open records act, K.S.A.
40 45-215 et seq., and amendments thereto. *The provisions of this subsection*
41 *shall expire on July 1, 2030, unless the legislature reviews and reenacts*
42 *this provision pursuant to K.S.A. 45-229, and amendments thereto.*

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

1 *the executive CISO may utilize KISO personnel, qualified third-party
2 assessors or a combination thereof. The CISO may establish an
3 assessment cycle that includes an initial baseline assessment for each
4 agency and periodic assessments thereafter. After conducting such
5 assessment, the executive CISO shall issue written findings,
6 recommendations and a timeline for any corrective action that is needed
7 based on the results of such assessments to be used in conjunction with
8 2025 Supp. K.S.A. 75-7246, and amendments thereto. After receiving such
9 written findings, recommendations and timeline, an agency shall develop
10 and maintain a written plan of action and milestones that details efforts to
11 remediate the findings from such assessment.*

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

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

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

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

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

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

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

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

40 (A) Comply with the notification requirements set out in K.S.A. 50-
41 7a01 et seq., and amendments thereto, and applicable federal laws and
42 rules and regulations, to the same extent as a person who conducts
43 business in this state; and

1 (B) not later than 12 hours after the discovery of the breach,
2 suspected breach or unauthorized exposure, notify:
3 (i) The CISO; and
4 (ii) if the breach, suspected breach or unauthorized exposure involves
5 election data, the secretary of state.
6 (b) The director or head of each state agency shall:
7 (1) Participate in annual agency leadership training to ensure
8 understanding of:
9 (A) The potential impact of common types of cyberattacks and data
10 breaches on the agency's operations and assets;
11 (B) how cyberattacks and data breaches on the agency's operations
12 and assets may impact the operations and assets of other governmental
13 entities on the state enterprise network;
14 (C) how cyberattacks and data breaches occur; and
15 (D) steps to be undertaken by the executive director or agency head
16 and agency employees to protect their information and information
17 systems; and
18 (2) coordinate with the executive CISO to implement the security
19 standard described in K.S.A. 75-7238, and amendments thereto.

20 Sec. 15. K.S.A. 2025 Supp. 75-7245 is hereby amended to read as
21 follows: 75-7245. (a) On and after July 1, 2027, all cybersecurity services
22 for each branch of state government shall be administered by the chief
23 information technology officer and the chief information security officer of
24 such branch. All cybersecurity employees within the legislative and
25 executive branches of state government shall work at the direction of the
26 chief information technology officer of the branch.

27 (b) ~~Prior to January 1, 2026:~~
28 (1) ~~The information technology executive council shall develop a~~
29 ~~plan to integrate all executive branch information technology services into~~
30 ~~the office of information technology services. The council shall consult~~
31 ~~with each agency head when developing such plan.~~
32 (2) ~~The judicial chief information technology officer shall develop an~~
33 ~~estimated project cost to provide information technology to judicial~~
34 ~~agencies and all employees of such agencies, including state and county-~~
35 ~~funded judicial branch district court employees. Such employees shall be~~
36 ~~required to use such state-issued information technology hardware. The~~
37 ~~project cost developed pursuant to this paragraph shall include, in~~
38 ~~consultation with the executive branch information technology officer, a~~
39 ~~plan to allow each piece of information technology hardware that is used~~
40 ~~by a judicial branch employee to access a judicial branch application to~~
41 ~~have access to the KANWIN network and an estimated project cost to~~
42 ~~develop a cybersecurity program for all judicial districts that complies~~
43 ~~with the national institute of standards and technology cybersecurity~~

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

2 (e) The information technology executive council shall report the
3 plan developed pursuant to subsection (b) to the senate standing committee
4 on ways and means and the house standing committee on legislative
5 modernization or its successor committee prior to January 15, 2026.

6 (d) Prior to February 1, 2025, Every website that is maintained by a
7 branch of government or state agency shall be moved to *hosted on a ".gov"*
8 domain.

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

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

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

20 Sec. 16. K.S.A. 2025 Supp. 75-7246 is hereby amended to read as
21 follows: 75-7246. (a) On ~~July~~ October 1, 2028, and each year thereafter,
22 the ~~director of the budget~~ in consultation with the legislative, executive
23 and judicial chief information technology officers as appropriate,
24 *executive CISO* shall determine if each state agency is in compliance with
25 the provisions of this act* for the previous fiscal year. If the director of the
26 budget determines that a state agency is not in compliance with the
27 provisions of this act for such fiscal year, The director shall certify an
28 amount equal to 5% of the amount:

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

31 (2) credited to and available in each special revenue fund for such
32 state agency in such fiscal year. If during any fiscal year, a special revenue
33 fund has no expenditure limitation, then an expenditure limitation shall be
34 established for such fiscal year on such special revenue fund by the
35 director of the budget in an amount that is 5% less than the amount of
36 moneys credited to and available in such special revenue fund for such
37 fiscal year *report to the legislative budget committee any executive branch*
38 *agency that is not making progress on a written plan of action and*
39 *milestones based on the assessment of such agency conducted pursuant to*
40 *K.S.A. 75-7240, and amendments thereto. Each such agency shall present*
41 *to the legislative budget committee such agency's plan to make progress*
42 *on the written plan of action and milestones.*

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

1 written report to the ~~legislature~~ senate committee on ways and means and
2 the ~~house of representatives~~ committee on appropriations on or before the
3 first day of the regular session of the legislature concerning—such
4 compliance determinations, including factors considered by the director
5 when making such determination, and the amounts certified for each state
6 agency for such fiscal year each agency that continues to fail to make
7 progress on a written plan of action and milestones after the presentation
8 made to the legislative budget committee pursuant to subsection (a).~~(e)~~
9 During the regular session of the legislature, the senate committee on ways
10 and means and the house of representatives committee on appropriations
11 shall consider such compliance determinations and whether to lapse
12 amounts appropriated and reappropriated and decrease the expenditure
13 limitations of special revenue funds *for information technology and*
14 *cybersecurity expenditures* for such state agencies by 10% during the
15 budget committee hearings for such noncomplying agency.

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

17 Sec. 17. K.S.A. 75-7203, as amended by section 21 of chapter 95 of
18 the 2024 Session Laws of Kansas, and 75-7205, as amended by section 23
19 of chapter 95 of the 2024 Session Laws of Kansas and K.S.A. 2023 Supp.
20 75-7201, as amended by section 17 of chapter 95 of the 2024 Session
21 Laws of Kansas, 75-7202, as amended by section 19 of chapter 95 of the
22 2024 Session Laws of Kansas, 75-7206, as amended by section 25 of
23 chapter 95 of the 2024 Session Laws of Kansas, 75-7208, as amended by
24 section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209, as
25 amended by section 29 of chapter 95 of the 2024 Session Laws of Kansas,
26 75-7237, as amended by section 31 of chapter 95 of the 2024 Session
27 Laws of Kansas, 75-7238, as amended by section 33 of chapter 95 of the
28 2024 Session Laws of Kansas, 75-7239, as amended by section 35 of
29 chapter 95 of the 2024 Session Laws of Kansas, and 75-7240, as amended
30 by section 37 of chapter 95 of the 2024 Session Laws of Kansas, and
31 K.S.A. 2025 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7202, 75-
32 7203, 75-7206a, 75-7208a, 75-7237, 75-7238, 75-7239, 75-7240, 75-7245
33 and 75-7246 are hereby repealed.

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