

**As Amended by House Committee**

---

*Session of 2026*

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

31  
32 *Be it enacted by the Legislature of the State of Kansas:*  
33 **New Section 1. There is hereby established the legislative branch**  
34 **information technology oversight council. The membership of the**  
35 **council shall be determined by the legislative coordinating council.**  
36 **The legislative branch information technology oversight council shall:**

- 1       (a) Set standards for legislative branch information technology;
- 2       (b) establish information technology policies for the legislative
- 3       branch;
- 4       (c) approve strategic information technology plans;
- 5       (d) oversee information technology projects to ensure alignment
- 6       with legislative branch goals;
- 7       (e) evaluate information technology and cybersecurity programs;
- 8       and
- 9       (f) support the legislative chief information technology officer and
- 10      the legislative chief information security officer.

11      New Section 1. **Sec. 2.** There is hereby established the judicial branch  
12      technology oversight council. The membership of the council shall be  
13      determined by the chief justice. The council shall:

- 14       (a) Set standards for judicial branch information technology;
- 15       (b) establish information technology policies for the judicial branch;
- 16       (c) approve strategic information technology plans;
- 17       (d) oversee information technology projects to ensure alignment with
- 18      judicial branch goals;
- 19       (e) evaluate information technology and cybersecurity programs; and
- 20       (f) support the judicial chief information technology officer and the
- 21      judicial branch chief information security officer.

22      **Sec. 2.** K.S.A. 2025 Supp. 40-110 is hereby amended to read as  
23      follows: 40-110. (a) The commissioner of insurance is hereby authorized  
24      to appoint an assistant commissioner of insurance, actuaries, two special  
25      attorneys who shall have been regularly admitted to practice, an executive  
26      secretary, policy examiners, two field representatives, and a secretary to  
27      the commissioner. Such appointees shall each receive an annual salary to  
28      be determined by the commissioner of insurance, within the limits of  
29      available appropriations. The commissioner is also authorized to appoint,  
30      within the provisions of the civil service law, and available appropriations,  
31      other employees as necessary to administer the provisions of this act. The  
32      field representatives authorized by this section may be empowered to  
33      conduct inquiries, investigations or to receive complaints. Such field  
34      representatives shall not be empowered to make, or direct to be made, an  
35      examination of the affairs and financial condition of any insurance  
36      company in the process of organization, or applying for admission or  
37      doing business in this state.

38      (b) The appointees authorized by this section shall take the proper  
39      official oath and shall be in no way interested, except as policyholders, in  
40      any insurance company. In the absence of the commissioner of insurance  
41      the assistant commissioner shall perform the duties of the commissioner of  
42      insurance, but shall in all cases execute papers in the name of the  
43      commissioner of insurance, as assistant. The commissioner of insurance

1 shall be responsible for all acts of an official nature done and performed by  
2 the commissioner's assistant or any person employed in such office. All the  
3 appointees authorized by this section shall hold their office at the will and  
4 pleasure of the commissioner of insurance.

5 (c)(1) The commissioner shall appoint a chief information security  
6 officer who shall be responsible for establishing security standards and  
7 policies to protect the department's information technology systems and  
8 infrastructure. The chief information security officer shall:

9 (A)(1) Develop a cybersecurity program for the department—that  
10 ~~complies with based on the national institute of standards and technology~~  
11 ~~cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024 2026 a~~  
12 ~~nationally recognized standard for governmental entities. Beginning in~~  
13 ~~2027 and every two years thereafter, the chief information security officer~~  
14 ~~shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1,~~  
15 ~~2028, and a CSF tier of 4.0 prior to July 1, 2030 report to the joint~~  
16 ~~committee on information technology, the house of representatives~~  
17 ~~standing committee on appropriations and the senate standing committee~~  
18 ~~on ways and means on the maturity level of the program;~~

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

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

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

31 (ii)(B) Results of audits conducted pursuant to this paragraph shall be  
32 confidential and shall not be subject to discovery or disclosure pursuant to  
33 the open records act, K.S.A. 45-215 et seq., and amendments thereto. The  
34 provisions of this subparagraph shall expire on July 1, 2030, unless the  
35 legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,  
36 and amendments thereto.

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

38 Sec. 3. 4. K.S.A. 2025 Supp. 75-413 is hereby amended to read as  
39 follows: 75-413. (a) The secretary of state may appoint such other  
40 assistants and clerks as may be authorized by law, but the secretary of state  
41 shall be responsible for the proper discharge of the duties of all assistants  
42 and clerks, and they shall hold their offices at the will and pleasure of the  
43 secretary and shall do and perform such general duties as the secretary

1 may require.

2 (b) (1) The secretary of state shall appoint a chief information  
3 security officer who shall be responsible for establishing security standards  
4 and policies to protect the office's information technology systems and  
5 infrastructure. The chief information security officer shall:

6 (A)(1) Develop a cybersecurity program for the office that complies  
7 with ~~based on the national institute of standards and technology~~  
8 ~~cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024-2026 a~~  
9 ~~nationally recognized standard for governmental entities. Beginning in~~  
10 ~~2027 and every two years thereafter, the chief information security officer~~  
11 ~~shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1,~~  
12 ~~2028, and a CSF tier of 4.0 prior to July 1, 2030 report to the joint~~  
13 ~~committee on information technology, the house of representatives~~  
14 ~~standing committee on appropriations and the senate standing committee~~  
15 ~~on ways and means on the maturity level of the program;~~

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

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

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

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

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

35 Sec. 4. 5. K.S.A. 2025 Supp. 75-623 is hereby amended to read as  
36 follows: 75-623. (a) The treasurer shall appoint such other assistants,  
37 clerks, bookkeepers, accountants and stenographers as may be authorized  
38 by law, each of which persons shall take the oath of office required of  
39 public officers. Such persons shall hold their offices at the will and  
40 pleasure of the state treasurer.

41 (b) (1) The treasurer shall appoint a chief information security officer  
42 who shall be responsible for establishing security standards and policies to  
43 protect the office's information technology systems and infrastructure. The

1 chief information security officer shall:

2     (A)(1) Develop a cybersecurity program for the office ~~that complies~~  
3 ~~with and the Kansas public employees retirement system based on the~~  
4 ~~national institute of standards and technology cybersecurity framework~~  
5 ~~(CSF) 2.0, as in effect on July 1, 2024 2026 a nationally recognized~~  
6 ~~standard for governmental entities. Beginning in 2027 and every two~~  
7 ~~years thereafter, the chief information security officer shall ensure that~~  
8 ~~such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF~~  
9 ~~tier of 4.0 prior to July 1, 2030 report to the joint committee on~~  
10 ~~information technology, the house of representatives standing committee~~  
11 ~~on appropriations and the senate standing committee on ways and means~~  
12 ~~on the maturity level of the program;~~

13     (B)(2) ensure that the treasurer and all employees **within the office of**  
14 **the treasurer and the Kansas public employees retirement system**  
15 complete cybersecurity awareness training annually and that if an  
16 employee does not complete the required training, such employee's access  
17 to any state-issued hardware or the state network is revoked; and

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

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

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

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

33     Sec. 5. 6. K.S.A. 2025 Supp. 75-710 is hereby amended to read as  
34 follows: 75-710. (a) The attorney general shall appoint such assistants,  
35 clerks, and stenographers as shall be authorized by law, and who shall hold  
36 their office at the will and pleasure of the attorney general. All fees and  
37 allowances earned by said assistants or any of them, or allowed to them by  
38 any statute or order of court in any civil or criminal case whatsoever, shall  
39 be turned into the general revenue fund of the state treasury, and the  
40 vouchers for their monthly salaries shall not be honored by the director of  
41 accounts and reports until a verified account of the fees collected by them,  
42 or either of them, during the preceding month, has been filed in the  
43 director of accounts and reports' office. Assistants appointed by the

1 attorney general shall perform the duties and exercise the powers as  
2 prescribed by law and shall perform other duties as prescribed by the  
3 attorney general. Assistants shall act for and exercise the power of the  
4 attorney general to the extent the attorney general delegates them the  
5 authority to do so.

6 (b)(1) The attorney general shall appoint a chief information security  
7 officer who shall be responsible for establishing security standards and  
8 policies to protect the office's information technology systems and  
9 infrastructure. The chief information security officer shall:

10 (A)(1) Develop a cybersecurity program for the office that complies  
11 with ~~based on the national institute of standards and technology~~  
12 ~~cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024-2026 a~~  
13 **nationally recognized standard for governmental entities. Beginning in**  
14 *2027 and every two years thereafter, the chief information security officer*  
15 *shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1,*  
16 *2028, and a CSF tier of 4.0 prior to July 1, 2030 report to the joint*  
17 *committee on information technology, the house of representatives*  
18 *standing committee on appropriations and the senate standing committee*  
19 *on ways and means on the maturity level of the program;*

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

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

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

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

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

39 Sec.-6. 7. K.S.A. 2025 Supp. 75-711 is hereby amended to read as  
40 follows: 75-711. (a) There is hereby established, under the jurisdiction of  
41 the attorney general, a division to be known as the Kansas bureau of  
42 investigation. The director of the bureau shall be appointed by the attorney  
43 general, subject to confirmation by the senate as provided in K.S.A. 75-

1 4315b, and amendments thereto, and shall have special training and  
2 qualifications for such position. Except as provided by K.S.A. 46-2601,  
3 and amendments thereto, no person appointed as director shall exercise  
4 any power, duty or function as director until confirmed by the senate. In  
5 accordance with appropriation acts, the director shall appoint agents who  
6 shall be trained in the detection and apprehension of criminals. The  
7 director shall appoint an associate director, and any such assistant directors  
8 from within the agency as are necessary for the efficient operation of the  
9 bureau, who shall have the qualifications and employee benefits, including  
10 longevity, of an agent. The director also may appoint a deputy director  
11 and, in accordance with appropriation acts, such administrative employees  
12 as are necessary for the efficient operation of the bureau. No person shall  
13 be appointed to a position within the Kansas bureau of investigation if the  
14 person has been convicted of a felony.

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

22 (c) Any person who was a member of the bureau at the time of  
23 appointment as director, associate director or assistant director, upon the  
24 expiration of their appointment, shall be returned to an unclassified or  
25 regular classified position under the Kansas civil service act with  
26 compensation comparable to and not lower than compensation being  
27 received at the time of appointment to the unclassified service. If all such  
28 possible positions are filled at that time, a temporary additional position  
29 shall be created for the person until a vacancy exists in the position. While  
30 serving in the temporary additional position, the person shall continue to  
31 be a contributing member of the retirement system for the agents of the  
32 Kansas bureau of investigation.

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

36 (e)-(1) The director shall appoint a chief information security officer  
37 who shall be responsible for establishing security standards and policies to  
38 protect the bureau's information technology systems and infrastructure.  
39 The chief information security officer shall:

40 (A)(1) Develop a cybersecurity program for the bureau that complies  
41 with ~~based on the national institute of standards and technology~~  
42 ~~cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024-2026 a~~  
43 ~~nationally recognized standard for governmental entities. Beginning in~~

1    2027 and every two years thereafter, the chief information security officer  
2    shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1,  
3    2028, and a CSF tier of 4.0 prior to July 1, 2030 report to the joint  
4    committee on information technology, the house of representatives  
5    standing committee on appropriations and the senate standing committee  
6    on ways and means on the maturity level of the program;

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

11   (C) (i) (a)(3) (4) coordinate with the United States cybersecurity and  
12   infrastructure security agency to perform annual audits of the department  
13   for periodic audits of the bureau's compliance with the cybersecurity  
14   program for compliance with and applicable state and federal laws, rules  
15   and regulations and department policies and standards; and

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

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

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

26   Sec. 7. 8. K.S.A. 2025 Supp. 75-7202 is hereby amended to read as  
27   follows: 75-7202. (a) There is hereby established the information  
28   technology executive council which shall be attached to the office of  
29   information technology services for purposes of administrative functions.

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

32   (A) Two cabinet agency heads or such persons' designees;  
33   (B) two noncabinet agency heads or such persons' designees;  
34   (C) the executive chief information technology officer;  
35   (D) the executive chief information security officer;  
36   (E) the chief executive officer of the state board of regents or such  
37   person's designee;

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

39   (F)(G) one representative of counties; the network manager of the  
40   information network of Kansas (INK);

41   (G)(H) one representative with background and knowledge in  
42   technology and cybersecurity from the private sector, except that such  
43   representative or such representative's employer shall not be an

1 information technology or cybersecurity vendor that does business with  
2 the state of Kansas;

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

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

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

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

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

14 ~~(N)~~ two information technology employees from state board of  
15 regents institutions appointed by the board of regents.

16 (2) The chief information technology architect, the legislative chief  
17 information technology officer; and the judicial chief information  
18 technology officer, ~~one member of the senate appointed by the president of~~  
19 ~~the senate, one member of the senate appointed by the minority leader of~~  
20 ~~the senate, one member of the house of representatives appointed by the~~  
21 ~~speaker of the house of representatives and one member of the house of~~  
22 ~~representatives appointed by the minority leader of the house of~~  
23 ~~representatives~~ shall be nonvoting members of the council.

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

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

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

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

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

8       Sec.-8. 9. K.S.A. 2025 Supp. 75-7203 is hereby amended to read as  
9 follows: 75-7203. (a) The information technology executive council is  
10 hereby authorized to adopt such policies and rules and regulations as  
11 necessary to implement, administer and enforce the provisions of this act.

12       (b) The council shall:

13           (1) Adopt:

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

16              (B) an information technology architecture, including  
17 telecommunications systems, networks and equipment, that covers all state  
18 agencies;

19              (C) standards for data management for all executive branch agencies;  
20 and

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

23              (2) provide direction and coordination for the application of the  
24 executive branch's information technology resources;

25              (3) designate the ownership of information resource processes and the  
26 lead executive branch agency for implementation of new technologies and  
27 networks shared by multiple agencies within the executive branch of state  
28 government; and

29              (4) ~~—develop a plan to integrate all information technology services for  
30 the executive branch into the office of information technology services and  
31 all cybersecurity services for state educational institutions as defined in  
32 K.S.A. 76-711, and amendments thereto, into the office of information  
33 technology services and the Kansas information security office; and~~

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

36              (e) ~~The information technology executive council shall report the  
37 plan developed under subsection (b)(4) to the senate standing committee  
38 on ways and means and the house standing committee on legislative  
39 modernization or its successor committee prior to January 15, 2026, in  
40 accordance with K.S.A. 2025 Supp. 75-7245, and amendments thereto.~~

41       Sec.-9. 10. K.S.A. 2025 Supp. 75-7206a is hereby amended to read as  
42 follows: 75-7206a. (a) There is hereby established the position of judicial  
43 branch chief information security officer. The judicial chief information

1 security officer shall be in the unclassified service under the Kansas civil  
2 service act, shall be appointed by the judicial administrator, subject to  
3 approval by the chief justice and shall receive compensation determined  
4 by the judicial administrator, subject to approval of the chief justice.

5 (b) The judicial chief information security officer, *in coordination*  
6 *with the judicial technology oversight council*, shall:

7 (1) Report to the judicial administrator;

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

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

14 (4) develop a centralized cybersecurity protocol for protecting and  
15 managing judicial branch information technology assets and infrastructure;

16 (5) detect and respond to security incidents consistent with  
17 information security standards and policies;

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

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

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

26 (9) ~~review ensure that~~ all contracts related to information technology  
27 entered into by a person or entity within the judicial branch ~~to make efforts~~  
28 ~~contain provisions~~ to reduce the risk of security vulnerabilities within the  
29 supply chain or product and ~~ensure~~ each contract contains standard  
30 security language; and

31 (10) coordinate with the United States cybersecurity and  
32 infrastructure security agency to perform annual ~~periodic~~ audits of judicial  
33 branch agencies **the branch's compliance with the cybersecurity**  
34 ~~program for compliance with and~~ applicable state and federal laws, rules  
35 and regulations and judicial branch policies and standards. ~~The judicial~~  
36 ~~chief information security officer shall make an audit request to such~~  
37 ~~agency annually, regardless of whether or not such agency has the capacity~~  
38 ~~to perform the requested audit.~~

39 (c) The judicial chief information security officer shall develop a  
40 cybersecurity program of each judicial agency ~~that complies with based on~~  
41 ~~the national institute of standards and technology cybersecurity framework~~  
42 ~~(CSF) 2.0, as in effect on July 1, 2024, 2026 a nationally recognized~~  
43 ~~standard for governmental entities. Beginning in 2027 and every two~~

1    *years thereafter, the judicial chief information security officer shall ensure*  
2    *that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a*  
3    *CSF tier of 4.0 prior to July 1, 2030 report to the joint committee on*  
4    *information technology, the house of representatives standing committee*  
5    *on appropriations and the senate standing committee on ways and means*  
6    *on the maturity level of the program.*

7    (d)(1) ~~If an audit conducted pursuant to subsection (b)(10) results in~~  
8    ~~a failure, the judicial chief information security officer shall report such~~  
9    ~~failure to the speaker and minority leader of the house of representatives~~  
10   ~~and the president and minority leader of the senate within 30 days of~~  
11   ~~receiving notice of such failure. Such report shall contain a plan to~~  
12   ~~mitigate any security risks identified in the audit. The judicial chief~~  
13   ~~information security officer shall coordinate for an additional audit after~~  
14   ~~the mitigation plan is implemented and report the results of such audit to~~  
15   ~~the speaker and minority leader of the house of representatives and the~~  
16   ~~president and minority leader of the senate.~~

17    (2) ~~Results of audits conducted pursuant to subsection (b)(10) and the~~  
18    ~~reports described in subsection (d)(1) shall be confidential and shall not be~~  
19    ~~subject to discovery or disclosure pursuant to the open records act, K.S.A.~~  
20    ~~45-215 et seq., and amendments thereto. The provisions of this subsection~~  
21    ~~shall expire on July 1, 2030, unless the legislature reviews and reenacts~~  
22    ~~this provision pursuant to K.S.A. 45-229, and amendments thereto.~~

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

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

31    (b) ~~The legislative chief information security officer shall:~~

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

33      (2) ~~establish security standards and policies to protect the branch's~~  
34      ~~information technology systems and infrastructure in accordance with~~  
35      ~~subsection (e);~~

36      (3) ~~ensure the confidentiality, availability and integrity of the~~  
37      ~~information transacted, stored or processed in the branch's information~~  
38      ~~technology systems and infrastructure;~~

39      (4) ~~develop a centralized cybersecurity protocol for protecting and~~  
40      ~~managing legislative branch information technology assets and~~  
41      ~~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 legislative branch data  
2 and information resources and obtain approval from the revisor of statutes  
3 prior to taking any action on any matter that involves a legal issue related  
4 to the security of information technology;

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

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

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

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

22       (e) *The legislative chief information technology officer shall appoint  
23 a legislative chief information security officer. The legislative chief  
24 information security officer shall develop a cybersecurity program of for  
25 each legislative agency that complies with based on the national institute  
26 of standards and technology cybersecurity framework (CSF) 2.0, as in  
27 effect on July 1, 2024 2026 a nationally recognized standard for  
28 governmental entities. Beginning in 2027 and every two years thereafter,  
29 the legislative chief information security officer shall ensure that such  
30 programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of  
31 4.0 prior to July 1, 2030. The agency head of each legislative agency shall  
32 coordinate with the legislative chief information security officer to achieve  
33 such standards report to the joint committee on information technology,  
34 the house of representatives standing committee on appropriations and the  
35 senate standing committee on ways and means on the maturity level of the  
36 program.*

37       (d)(b) (1) If an audit conducted pursuant to subsection (b)(10) results  
38 in a failure, the legislative chief information security officer shall report  
39 such failure to the speaker and minority leader of the house of  
40 representatives and the president and minority leader of the senate within  
41 30 days of receiving notice of such failure. Such report shall contain a plan  
42 to mitigate any security risks identified in the audit. The legislative chief  
43 information security officer shall coordinate for an additional audit after

1 the mitigation plan is implemented and report the results of such audit to  
2 the speaker and minority leader of the house of representatives and the  
3 president and minority leader of the senate. *The legislative chief*  
4 *information security officer shall:*

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

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

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

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

21 Sec. 11. 12. K.S.A. 2025 Supp. 75-7237 is hereby amended to read as  
22 follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and  
23 amendments thereto:

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

25 (b) "Breach" or "breach of security" means unauthorized access of  
26 data in electronic form containing personal information. Good faith access  
27 of personal information by an employee or agent of an executive branch  
28 agency does not constitute a breach of security, provided that the  
29 information is not used for a purpose unrelated to the business or subject to  
30 further unauthorized use.

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

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

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

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

41 (g) "Executive branch agency" means any agency in the executive  
42 branch of the state of Kansas, including the judicial council but not the  
43 elected office agencies, the adjutant general's department, *the Kansas*

1   *public employees retirement system, regents' institutions, or the board of*  
2   *regents.*

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

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

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

8           (i) Social security number;

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

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

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

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

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

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

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

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

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

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

38       (b) The executive CISO shall:

39           (1) Report to the executive branch chief information technology  
40           officer;

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

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

4       (4) develop a centralized cybersecurity protocol for protecting and  
5 managing executive branch information technology assets and  
6 infrastructure;

7       (5) detect and respond to security incidents consistent with  
8 information security standards and policies;

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

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

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

17       (9) ~~review~~ ensure that all contracts related to information technology  
18 entered into by a person or entity within the executive branch ~~to make~~  
19 ~~efforts~~ contain provisions to reduce the risk of security vulnerabilities  
20 within the supply chain or product and ~~ensure~~ each contract contains  
21 standard security language; ~~and~~

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

26       (c) The executive CISO shall develop a cybersecurity program for  
27 each executive branch agency ~~that complies with based on the national~~  
28 ~~institute of standards and technology cybersecurity framework (CSF) 2.0,~~  
29 ~~as in effect on July 1, 2024 2026 a nationally recognized standard for~~  
30 ~~governmental entities. Beginning in 2027 and every two years thereafter,~~  
31 ~~the executive CISO shall ensure that such programs achieve a CSF tier of~~  
32 ~~3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030 report~~  
33 ~~to the joint committee on information technology, the house of~~  
34 ~~representatives standing committee on appropriations and the senate~~  
35 ~~standing committee on ways and means on the maturity level of the~~  
36 ~~program. The agency head of each executive branch agency shall~~  
37 ~~coordinate with the executive CISO to achieve such standards.~~

38       Sec. ~~13.~~ **14.** K.S.A. 2025 Supp. 75-7239 is hereby amended to read as  
39 follows: 75-7239. (a) There is hereby established within and as a part of  
40 the office of information technology services the Kansas information  
41 security office. The Kansas information security office shall be  
42 administered by the executive CISO and be staffed appropriately to effect  
43 the provisions of the Kansas cybersecurity act.

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

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

12           (1) Administer the Kansas cybersecurity act;

13           (2) develop, implement and monitor strategic and comprehensive  
14 information security risk-management programs;

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

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

20           (5) coordinate with the United States cybersecurity and infrastructure  
21 security agency to perform annual *periodic* audits of executive branch  
22 agencies **the branch's compliance with the cybersecurity program for**  
23 ~~compliance with and~~ applicable state and federal laws, rules and  
24 regulations and executive branch policies and standards. ~~The executive~~  
25 ~~CISO shall make an audit request to such agency annually, regardless of~~  
26 ~~whether or not such agency has the capaeity to perform the requested~~  
27 ~~audit;~~

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

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

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

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

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

42           (11) *conduct periodic cybersecurity assessments of each executive*  
43 *branch agency that may include a review of controls, processes,*

1   *technologies, governance, incident preparedness, operational security and*  
2   *compliance with statewide policies and standards;*

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

5       (12)(13) perform such other functions and duties as provided by law  
6       and as directed by the CISO.

7       (d)(1) ~~If an audit conducted pursuant to subsection (e)(5) results in a~~  
8       ~~failure, the executive CISO shall report such failure to the speaker and~~  
9       ~~minority leader of the house of representatives and the president and~~  
10       ~~minority leader of the senate within 30 days of receiving notice of such~~  
11       ~~failure. Such report shall contain a plan to mitigate any security risks~~  
12       ~~identified in the audit. The executive CISO shall coordinate for an~~  
13       ~~additional audit after the mitigation plan is implemented and report the~~  
14       ~~results of such audit to the speaker and minority leader of the house of~~  
15       ~~representatives and the president and minority leader of the senate.~~

16       (2) Results of audits conducted pursuant to subsection (c)(5) and the  
17       ~~reports described in subsection (d)(1) and the assessments conducted~~  
18       ~~pursuant to subsection (c)(11)~~ shall be confidential and shall not be  
19       subject to discovery or disclosure pursuant to the open records act, K.S.A.  
20       45-215 et seq., and amendments thereto. *The provisions of this subsection*  
21       *shall expire on July 1, 2030, unless the legislature reviews and reenacts*  
22       *this provision pursuant to K.S.A. 45-229, and amendments thereto.*

23       (e) *When conducting the assessments required by subsection (c)(11),*  
24       *the executive CISO may utilize KISO personnel, qualified third-party*  
25       *assessors or a combination thereof. The CISO—may shall establish an*  
26       *assessment cycle that includes an initial baseline assessment for each*  
27       *agency and periodic assessments thereafter. After conducting such*  
28       *assessment, the executive CISO shall issue written findings,*  
29       *recommendations and a timeline for any corrective action that is needed*  
30       *based on the results of such assessments to be used in conjunction with*  
31       *2025 Supp. K.S.A. 75-7246, and amendments thereto. After receiving such*  
32       *written findings, recommendations and timeline, an agency shall develop*  
33       *and maintain a written plan of action and milestones that details efforts to*  
34       *remediate the findings from such assessment.*

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

40       Sec. 14. 15. K.S.A. 2025 Supp. 75-7240 is hereby amended to read as  
41       follows: 75-7240. (a) The executive branch agency heads shall:

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

1 data or resources;

2 (2) designate an information security officer to administer the

3 agency's information security program that reports directly to executive

4 leadership;

5 (3) participate in CISO-sponsored statewide cybersecurity program

6 initiatives and services;

7 (4) *continuously work toward improving cybersecurity maturity*

8 *consistent with statewide standards and expectations adopted by the*

9 *executive CISO pursuant to K.S.A. 75-7238, and amendments thereto;*

10 (5) *prior to acquiring any cybersecurity-related product, service or*

11 *platform that may materially affect state systems, data or cybersecurity*

12 *risks, consult with the executive CISO and obtain a written certificate from*

13 *the executive CISO that such acquisition does not create a cybersecurity*

14 *risk; and*

15 (6) ensure that if an agency owns, licenses or maintains computerized

16 data that includes personal information, confidential information or

17 information, the disclosure of which is regulated by law, such agency

18 shall, in the event of a breach or suspected breach of system security or an

19 unauthorized exposure of that information:

20 (A) Comply with the notification requirements set out in K.S.A. 50-

21 7a01 et seq., and amendments thereto, and applicable federal laws and

22 rules and regulations, to the same extent as a person who conducts

23 business in this state; and

24 (B) not later than 12 hours after the discovery of the breach,

25 suspected breach or unauthorized exposure, notify:

26 (i) The CISO; and

27 (ii) if the breach, suspected breach or unauthorized exposure involves

28 election data, the secretary of state.

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

30 (1) Participate in annual agency leadership training to ensure

31 understanding of:

32 (A) The potential impact of common types of cyberattacks and data

33 breaches on the agency's operations and assets;

34 (B) how cyberattacks and data breaches on the agency's operations

35 and assets may impact the operations and assets of other governmental

36 entities on the state enterprise network;

37 (C) how cyberattacks and data breaches occur; and

38 (D) steps to be undertaken by the executive director or agency head

39 and agency employees to protect their information and information

40 systems; and

41 (2) coordinate with the executive CISO to implement the security

42 standard described in K.S.A. 75-7238, and amendments thereto.

43 Sec. 16. K.S.A. 2025 Supp. 75-7245 is hereby amended to read as

1 follows: 75-7245. (a) (1) **Except as provided in paragraph (2)**, on and  
2 after July 1, 2027, all cybersecurity services for each branch of state  
3 government shall be administered by the chief information technology  
4 officer and the chief information security officer of such branch. All  
5 cybersecurity employees within the legislative and executive branches of  
6 state government shall work at the direction of the chief information  
7 technology officer of the branch.

8 (2) All cybersecurity services for the Kansas public employees  
9 retirement system shall be administered by the chief information  
10 security officer within the office of the state treasurer. All  
11 cybersecurity employees within the Kansas public employees  
12 retirement system shall work at the direction of the chief information  
13 security officer within the office of the state treasurer.

14 (b) ~~Prior to January 1, 2026:~~

15 (1) ~~The information technology executive council shall develop a~~  
16 ~~plan to integrate all executive branch information technology services into~~  
17 ~~the office of information technology services. The council shall consult~~  
18 ~~with each agency head when developing such plan.~~

19 (2) ~~The judicial chief information technology officer shall develop an~~  
20 ~~estimated project cost to provide information technology to judicial~~  
21 ~~agencies and all employees of such agencies, including state and county-~~  
22 ~~funded judicial branch district court employees. Such employees shall be~~  
23 ~~required to use such state-issued information technology hardware. The~~  
24 ~~project cost developed pursuant to this paragraph shall include, in~~  
25 ~~consultation with the executive branch information technology officer, a~~  
26 ~~plan to allow each piece of information technology hardware that is used~~  
27 ~~by a judicial branch employee to access a judicial branch application to~~  
28 ~~have access to the KANWIN network and an estimated project cost to~~  
29 ~~develop a cybersecurity program for all judicial districts that complies~~  
30 ~~with the national institute of standards and technology cybersecurity~~  
31 ~~framework (CSF) 2.0, as in effect on July 1, 2024.~~

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

36 (d) ~~Prior to February 1, 2025, Every website that is maintained by a~~  
37 ~~branch of government or state agency shall be moved to hosted on a ".gov"~~  
38 ~~domain.~~

39 (e)(c) On July 1, 2025, and each year thereafter, moneys appropriated  
40 from the state general fund to or any special revenue fund of any state  
41 agency for information technology and cybersecurity expenditures shall be  
42 appropriated as a separate line item and shall not be merged with other  
43 items of appropriation for such state agency to allow for detailed review

1 by the senate committee on ways and means and the house of  
2 representatives committee on appropriations during each regular  
3 legislative session.

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

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

7 Sec. 16. 17. K.S.A. 2025 Supp. 75-7246 is hereby amended to read as  
8 follows: 75-7246. (a) On ~~July~~ October 1, 2028, and each year thereafter,  
9 the ~~director of the budget, in consultation with the legislative, executive~~  
10 ~~and judicial chief information technology officers as appropriate,~~  
11 ~~executive CISO shall determine if each state agency is in compliance with~~  
12 ~~the provisions of this act\* for the previous fiscal year. If the director of the~~  
13 ~~budget determines that a state agency is not in compliance with the~~  
14 ~~provisions of this act for such fiscal year, The director shall certify an~~  
15 ~~amount equal to 5% of the amount:~~

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

18 (2) ~~credited to and available in each special revenue fund for such~~  
19 ~~state agency in such fiscal year. If during any fiscal year, a special revenue~~  
20 ~~fund has no expenditure limitation, then an expenditure limitation shall be~~  
21 ~~established for such fiscal year on such special revenue fund by the~~  
22 ~~director of the budget in an amount that is 5% less than the amount of~~  
23 ~~moneys credited to and available in such special revenue fund for such~~  
24 ~~fiscal year report to the legislative budget committee and the joint~~  
25 ~~committee on information technology any executive branch agency that~~  
26 ~~is not making progress on a written plan of action and milestones based~~  
27 ~~on the assessment of such agency conducted pursuant to K.S.A. 75-7240,~~  
28 ~~and amendments thereto. Each such agency shall present to the legislative~~  
29 ~~budget committee such agency's plan to make progress on the written plan~~  
30 ~~of action and milestones.~~

31 (b) The ~~director of the budget executive CISO shall submit a detailed~~  
32 ~~written report to the legislature joint committee on information~~  
33 ~~technology, the senate committee on ways and means and the house of~~  
34 ~~representatives committee on appropriations on or before the first day of~~  
35 ~~the regular session of the legislature concerning such compliance~~  
36 ~~determinations, including factors considered by the director when making~~  
37 ~~such determination, and the amounts certified for each state agency for~~  
38 ~~such fiscal year each agency that continues to fail to make progress on a~~  
39 ~~written plan of action and milestones after the presentation made to the~~  
40 ~~legislative budget committee pursuant to subsection (a).(e) During the~~  
41 ~~regular session of the legislature, the senate committee on ways and means~~  
42 ~~and the house of representatives committee on appropriations shall~~  
43 ~~consider such compliance determinations and whether to lapse amounts~~

1 appropriated and reappropriated and decrease the expenditure limitations  
2 of special revenue funds *for information technology and cybersecurity*  
3 *expenditures* for such state agencies *by 10%* during the budget committee  
4 hearings for such noncomplying agency.

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

6 Sec. ~~17~~ **18.** K.S.A. 75-7203, as amended by section 21 of chapter 95  
7 of the 2024 Session Laws of Kansas, and 75-7205, as amended by section  
8 23 of chapter 95 of the 2024 Session Laws of Kansas and K.S.A. 2023  
9 Supp. 75-7201, as amended by section 17 of chapter 95 of the 2024  
10 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95  
11 of the 2024 Session Laws of Kansas, 75-7206, as amended by section 25  
12 of chapter 95 of the 2024 Session Laws of Kansas, 75-7208, as amended  
13 by section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209,  
14 as amended by section 29 of chapter 95 of the 2024 Session Laws of  
15 Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024  
16 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter 95  
17 of the 2024 Session Laws of Kansas, 75-7239, as amended by section 35  
18 of chapter 95 of the 2024 Session Laws of Kansas, and 75-7240, as  
19 amended by section 37 of chapter 95 of the 2024 Session Laws of Kansas,  
20 and K.S.A. 2025 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7202,  
21 75-7203, 75-7206a, 75-7208a, 75-7237, 75-7238, 75-7239, 75-7240, 75-  
22 7245 and 75-7246 are hereby repealed.

23 Sec. ~~18~~ **19.** This act shall take effect and be in force from and after  
24 its publication in the statute book.