

## HOUSE BILL No. 2271

By Committee on Legislative Modernization

Requested by Representative Penn

2-5

1 AN ACT concerning cybersecurity; removing the expiration provisions of  
2 cybersecurity legislation; consolidating cybersecurity services under  
3 the chief information security officer of each branch; amending K.S.A.  
4 2024 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7203, 75-  
5 7206a, 75-7208a, 75-7245 and 75-7246 and repealing the existing  
6 sections; also repealing K.S.A. 2023 Supp. 45-229, as amended by  
7 section 11 of chapter 95 of the 2024 Session Laws of Kansas, 75-7201,  
8 as amended by section 17 of chapter 95 of the 2024 Session Laws of  
9 Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024  
10 Session Laws of Kansas, 75-7203, as amended by section 21 of chapter  
11 95 of the 2024 Session Laws of Kansas, 75-7205, as amended by  
12 section 23 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206,  
13 as amended by section 25 of chapter 95 of the 2024 Session Laws of  
14 Kansas, 75-7208, as amended by section 27 of chapter 95 of the 2024  
15 Session Laws of Kansas, 75-7209, as amended by section 29 of chapter  
16 95 of the 2024 Session Laws of Kansas, 75-7237, as amended by  
17 section 31 of chapter 95 of the 2024 Session Laws of Kansas, 75-7238,  
18 as amended by section 33 of chapter 95 of the 2024 Session Laws of  
19 Kansas, 75-7239, as amended by section 35 of chapter 95 of the 2024  
20 Session Laws of Kansas, 75-7240, as amended by section 37 of chapter  
21 95 of the 2024 Session Laws of Kansas.  
22

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

24 Section 1. K.S.A. 2024 Supp. 40-110 is hereby amended to read as  
25 follows: 40-110. (a) The commissioner of insurance is hereby authorized  
26 to appoint an assistant commissioner of insurance, actuaries, two special  
27 attorneys who shall have been regularly admitted to practice, an executive  
28 secretary, policy examiners, two field representatives, and a secretary to  
29 the commissioner. Such appointees shall each receive an annual salary to  
30 be determined by the commissioner of insurance, within the limits of  
31 available appropriations. The commissioner is also authorized to appoint,  
32 within the provisions of the civil service law, and available appropriations,  
33 other employees as necessary to administer the provisions of this act. The  
34 field representatives authorized by this section may be empowered to  
35 conduct inquiries, investigations or to receive complaints. Such field

1 representatives shall not be empowered to make, or direct to be made, an  
2 examination of the affairs and financial condition of any insurance  
3 company in the process of organization, or applying for admission or  
4 doing business in this state.

5 (b) The appointees authorized by this section shall take the proper  
6 official oath and shall be in no way interested, except as policyholders, in  
7 any insurance company. In the absence of the commissioner of insurance  
8 the assistant commissioner shall perform the duties of the commissioner of  
9 insurance, but shall in all cases execute papers in the name of the  
10 commissioner of insurance, as assistant. The commissioner of insurance  
11 shall be responsible for all acts of an official nature done and performed by  
12 the commissioner's assistant or any person employed in such office. All the  
13 appointees authorized by this section shall hold their office at the will and  
14 pleasure of the commissioner of insurance.

15 (c)-(4) The commissioner shall appoint a chief information security  
16 officer who shall be responsible for establishing security standards and  
17 policies to protect the department's information technology systems and  
18 infrastructure. The chief information security officer shall:

19 (A)(1) Develop a cybersecurity program for the department that  
20 complies with the national institute of standards and technology  
21 cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief  
22 information security officer shall ensure that such programs achieve a CSF  
23 tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

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

28 (C)-(i)-(a)(3) (A) (i) coordinate with the United States cybersecurity  
29 and infrastructure security agency to perform annual audits of the  
30 department for compliance with applicable state and federal laws, rules  
31 and regulations and department policies and standards; and

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

35 (ii)(B) Results of audits conducted pursuant to this paragraph shall be  
36 confidential and shall not be subject to discovery or disclosure pursuant to  
37 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

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

39 Sec. 2. K.S.A. 2024 Supp. 75-413 is hereby amended to read as  
40 follows: 75-413. (a) The secretary of state may appoint such other  
41 assistants and clerks as may be authorized by law, but the secretary of state  
42 shall be responsible for the proper discharge of the duties of all assistants  
43 and clerks, and they shall hold their offices at the will and pleasure of the

1 secretary and shall do and perform such general duties as the secretary  
2 may require.

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

7 (A)(1) Develop a cybersecurity program for the office that complies  
8 with the national institute of standards and technology cybersecurity  
9 framework (CSF) 2.0, as in effect on July 1, 2024. The chief information  
10 security officer shall ensure that such programs achieve a CSF tier of 3.0  
11 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

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

16 (C)-(1)-(a)(3) (A) (i) coordinate with the United States cybersecurity  
17 and infrastructure security agency to perform annual audits of the office  
18 for compliance with applicable state and federal laws, rules and  
19 regulations and office policies and standards; and

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

23 (1)(B) Results of audits conducted pursuant to this paragraph shall be  
24 confidential and shall not be subject to discovery or disclosure pursuant to  
25 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

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

27 Sec. 3. K.S.A. 2024 Supp. 75-623 is hereby amended to read as  
28 follows: 75-623. (a) The treasurer shall appoint such other assistants,  
29 clerks, bookkeepers, accountants and stenographers as may be authorized  
30 by law, each of which persons shall take the oath of office required of  
31 public officers. Such persons shall hold their offices at the will and  
32 pleasure of the state treasurer.

33 (b)-(1) The treasurer shall appoint a chief information security officer  
34 who shall be responsible for establishing security standards and policies to  
35 protect the office's information technology systems and infrastructure. The  
36 chief information security officer shall:

37 (A)(1) Develop a cybersecurity program for the office that complies  
38 with the national institute of standards and technology cybersecurity  
39 framework (CSF) 2.0, as in effect on July 1, 2024. 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;

42 (B)(2) ensure that the treasurer and all employees complete  
43 cybersecurity awareness training annually and that if an employee does not

1 complete the required training, such employee's access to any state-issued  
2 hardware or the state network is revoked; and

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

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

10 ~~(ii)(B)~~ Results of audits conducted pursuant to this paragraph shall be  
11 confidential and shall not be subject to discovery or disclosure pursuant to  
12 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

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

14 Sec. 4. K.S.A. 2024 Supp. 75-710 is hereby amended to read as  
15 follows: 75-710. (a) The attorney general shall appoint such assistants,  
16 clerks, and stenographers as shall be authorized by law, and who shall hold  
17 their office at the will and pleasure of the attorney general. All fees and  
18 allowances earned by said assistants or any of them, or allowed to them by  
19 any statute or order of court in any civil or criminal case whatsoever, shall  
20 be turned into the general revenue fund of the state treasury, and the  
21 vouchers for their monthly salaries shall not be honored by the director of  
22 accounts and reports until a verified account of the fees collected by them,  
23 or either of them, during the preceding month, has been filed in the  
24 director of accounts and reports' office. Assistants appointed by the  
25 attorney general shall perform the duties and exercise the powers as  
26 prescribed by law and shall perform other duties as prescribed by the  
27 attorney general. Assistants shall act for and exercise the power of the  
28 attorney general to the extent the attorney general delegates them the  
29 authority to do so.

30 ~~(b)-(1)~~ The attorney general shall appoint a chief information security  
31 officer who shall be responsible for establishing security standards and  
32 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 the national institute of standards and technology cybersecurity  
36 framework (CSF) 2.0, as in effect on July 1, 2024. The chief information  
37 security officer shall ensure that such programs achieve a CSF tier of 3.0  
38 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

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

43 ~~(C)(i)-(a)(3)~~ (A) (i) coordinate with the United States cybersecurity

1 and infrastructure security agency to perform annual audits of the office  
2 for compliance with applicable state and federal laws, rules and  
3 regulations and office policies and standards; and

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

7 ~~(ii)(B)~~ Results of audits conducted pursuant to this paragraph shall be  
8 confidential and shall not be subject to discovery or disclosure pursuant to  
9 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

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

11 Sec. 5. K.S.A. 2024 Supp. 75-711 is hereby amended to read as  
12 follows: 75-711. (a) There is hereby established, under the jurisdiction of  
13 the attorney general, a division to be known as the Kansas bureau of  
14 investigation. The director of the bureau shall be appointed by the attorney  
15 general, subject to confirmation by the senate as provided in K.S.A. 75-  
16 4315b, and amendments thereto, and shall have special training and  
17 qualifications for such position. Except as provided by K.S.A. 46-2601,  
18 and amendments thereto, no person appointed as director shall exercise  
19 any power, duty or function as director until confirmed by the senate. In  
20 accordance with appropriation acts, the director shall appoint agents who  
21 shall be trained in the detection and apprehension of criminals. The  
22 director shall appoint an associate director, and any such assistant directors  
23 from within the agency as are necessary for the efficient operation of the  
24 bureau, who shall have the qualifications and employee benefits, including  
25 longevity, of an agent. The director also may appoint a deputy director  
26 and, in accordance with appropriation acts, such administrative employees  
27 as are necessary for the efficient operation of the bureau. No person shall  
28 be appointed to a position within the Kansas bureau of investigation if the  
29 person has been convicted of a felony.

30 (b) The director, associate director, deputy director, assistant directors  
31 and any assistant attorneys general assigned to the bureau shall be within  
32 the unclassified service under the Kansas civil service act. All other agents  
33 and employees of the bureau shall be in the classified service under the  
34 Kansas civil service act and their compensation shall be determined as  
35 provided in the Kansas civil service act and shall receive actual and  
36 necessary expenses.

37 (c) Any person who was a member of the bureau at the time of  
38 appointment as director, associate director or assistant director, upon the  
39 expiration of their appointment, shall be returned to an unclassified or  
40 regular classified position under the Kansas civil service act with  
41 compensation comparable to and not lower than compensation being  
42 received at the time of appointment to the unclassified service. If all such  
43 possible positions are filled at that time, a temporary additional position

1 shall be created for the person until a vacancy exists in the position. While  
2 serving in the temporary additional position, the person shall continue to  
3 be a contributing member of the retirement system for the agents of the  
4 Kansas bureau of investigation.

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

8 (e)-(f) The director shall appoint a chief information security officer  
9 who shall be responsible for establishing security standards and policies to  
10 protect the bureau's information technology systems and infrastructure.  
11 The chief information security officer shall:

12 (A)(1) Develop a cybersecurity program for the bureau that complies  
13 with the national institute of standards and technology cybersecurity  
14 framework (CSF) 2.0, as in effect on July 1, 2024. The chief information  
15 security officer shall ensure that such programs achieve a CSF tier of 3.0  
16 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

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

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

25 (b)(ii) 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.

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

32 Sec. 6. K.S.A. 75-7203 is hereby amended to read as follows: 75-  
33 7203. (a) The information technology executive council is hereby  
34 authorized to adopt such policies and rules and regulations as necessary to  
35 implement, administer and enforce the provisions of this act.

36 (b) The council shall:

37 (1) Adopt:

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

40 (B) an information technology architecture, including  
41 telecommunications systems, networks and equipment, that covers all state  
42 agencies;

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

1 and

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

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

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

10 (4) develop a plan to integrate all information technology services for  
11 the executive branch into the office of information technology services and  
12 all cybersecurity services for state educational institutions as defined in  
13 K.S.A. 76-711, and amendments thereto, into the office of information  
14 technology services and the Kansas information security office; and

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

17 (c) The information technology executive council shall report the  
18 plan developed under subsection (b)(4) to the senate standing committee  
19 on ways and means ~~and~~, the house standing committee on legislative  
20 modernization or its successor committee *and the joint committee on*  
21 *information technology* prior to January 15, 2026, in accordance with  
22 K.S.A. 2024 Supp. 75-7245, and amendments thereto.

23 Sec. 7. K.S.A. 2024 Supp. 75-7206a is hereby amended to read as  
24 follows: 75-7206a. (a) There is hereby established the position of judicial  
25 branch chief information security officer. The judicial chief information  
26 security officer shall be in the unclassified service under the Kansas civil  
27 service act, shall be appointed by the judicial administrator, subject to  
28 approval by the chief justice and shall receive compensation determined  
29 by the judicial administrator, subject to approval of the chief justice.

30 (b) The judicial chief information security officer shall:

31 (1) Report to the judicial administrator;

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

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

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

40 (5) detect and respond to security incidents consistent with  
41 information security standards and policies;

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

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

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

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

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

18 (c) The judicial chief information security officer shall develop a  
19 cybersecurity program of each judicial agency that complies with the  
20 national institute of standards and technology cybersecurity framework  
21 (CSF) 2.0, as in effect on July 1, 2024. The judicial chief information  
22 security officer shall ensure that such programs achieve a CSF tier of 3.0  
23 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030.

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

34 (2) Results of audits conducted pursuant to subsection (b)(10) and the  
35 reports described in subsection (d)(1) shall be confidential and shall not be  
36 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
37 45-215 et seq., and amendments thereto.

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

39 Sec. 8. K.S.A. 2024 Supp. 75-7208a is hereby amended to read as  
40 follows: 75-7208a. (a) There is hereby established the position of  
41 legislative branch chief information security officer. The legislative chief  
42 information security officer shall be in the unclassified service under the  
43 Kansas civil service act, shall be appointed by the legislative coordinating

1 council and shall receive compensation determined by the legislative  
2 coordinating council.

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

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

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

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

11 (4) develop a centralized cybersecurity protocol for protecting and  
12 managing legislative branch information technology assets and  
13 infrastructure;

14 (5) detect and respond to security incidents consistent with  
15 information security standards and policies;

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

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 legislators and legislative 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 all contracts related to information technology entered into  
27 by a person or entity within the legislative branch to make efforts to reduce  
28 the risk of security vulnerabilities within the supply chain or product and  
29 ensure each contract contains standard security language; and

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

37 (c) The legislative chief information security officer shall develop a  
38 cybersecurity program of each legislative agency that complies with the  
39 national institute of standards and technology cybersecurity framework  
40 (CSF) 2.0, as in effect on July 1, 2024. The legislative 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. The  
43 agency head of each legislative agency shall coordinate with the legislative

1 chief information security officer to achieve such standards.

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

12 (2) Results of audits conducted pursuant to subsection (b)(10) and the  
13 reports described in subsection (d)(1) shall be confidential and shall not be  
14 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
15 45-215 et seq., and amendments thereto.

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

17 Sec. 9. K.S.A. 2024 Supp. 75-7245 is hereby amended to read as  
18 follows: 75-7245. (a) On and after July 1, 2027, all cybersecurity services  
19 for each branch of state government shall be administered by the chief  
20 information technology officer and the chief information security officer of  
21 such branch. All cybersecurity employees within the legislative and  
22 executive branches of state government shall work at the direction of the  
23 chief information technology officer of the branch.

24 (b) Prior to January 1, 2026:

25 (1) The information technology executive council shall develop a  
26 plan to integrate all executive branch information technology services into  
27 the office of information technology services. The council shall consult  
28 with each agency head when developing such plan.

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

42 (c) The information technology executive council shall report the  
43 plan developed pursuant to subsection (b) to the senate standing committee

1 on ways and means—and, the house standing committee on legislative  
2 modernization or its successor committee *and the joint committee on*  
3 *information technology*, prior to January 15, 2026.

4 (d) Prior to February 1, 2025, every website that is maintained by a  
5 branch of government or state agency shall be moved to a ".gov" domain.

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

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

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

17 Sec. 10. K.S.A. 2024 Supp. 75-7246 is hereby amended to read as  
18 follows: 75-7246. (a) On July 1, 2028, and each year thereafter, the  
19 director of the budget, in consultation with the legislative, executive and  
20 judicial chief information technology officers as appropriate, shall  
21 determine if each state agency is in compliance with the provisions of this  
22 act\* for the previous fiscal year. If the director of the budget determines  
23 that a state agency is not in compliance with the provisions of this act for  
24 such fiscal year, the director shall certify an amount equal to 5% of the  
25 amount:

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

28 (2) credited to and available in each special revenue fund for such  
29 state agency in such fiscal year. If during any fiscal year, a special revenue  
30 fund has no expenditure limitation, then an expenditure limitation shall be  
31 established for such fiscal year on such special revenue fund by the  
32 director of the budget in an amount that is 5% less than the amount of  
33 moneys credited to and available in such special revenue fund for such  
34 fiscal year.

35 (b) The director of the budget shall submit a detailed written report to  
36 the legislature on or before the first day of the regular session of the  
37 legislature concerning such compliance determinations, including factors  
38 considered by the director when making such determination, and the  
39 amounts certified for each state agency for such fiscal year.

40 (c) During the regular session of the legislature, the senate committee  
41 on ways and means and the house of representatives committee on  
42 appropriations shall consider such compliance determinations and whether  
43 to lapse amounts appropriated and reappropriated and decrease the

1 expenditure limitations of special revenue funds for such state agencies  
2 during the budget committee hearings for such noncomplying agency.

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

4 Sec. 11. K.S.A. 2024 Supp. 40-110, 45-229, as amended by section  
5 11 of chapter 95 of the 2024 Session Laws of Kansas, 75-413, 75-623, 75-  
6 710, 75-711, 75-7201, as amended by section 17 of chapter 95 of the 2024  
7 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95  
8 of the 2024 Session Laws of Kansas, 75-7203, 75-7203, as amended by  
9 section 21 of chapter 95 of the 2024 Session Laws of Kansas, 75-7205, as  
10 amended by section 23 of chapter 95 of the 2024 Session Laws of Kansas,  
11 75-7206, as amended by section 25 of chapter 95 of the 2024 Session  
12 Laws of Kansas, 75-7206a, 75-7208, as amended by section 27 of chapter  
13 95 of the 2024 Session Laws of Kansas, 75-7208a, 75-7209, as amended  
14 by section 29 of chapter 95 of the 2024 Session Laws of Kansas, 75-7237,  
15 as amended by section 31 of chapter 95 of the 2024 Session Laws of  
16 Kansas, 75-7238, as amended by section 33 of chapter 95 of the 2024  
17 Session Laws of Kansas, 75-7239, as amended by section 35 of chapter 95  
18 of the 2024 Session Laws of Kansas, 75-7240, as amended by section 37  
19 of chapter 95 of the 2024 Session Laws of Kansas, 75-7245 and 75-7246  
20 are hereby repealed.

21 Sec. 12. This act shall take effect and be in force from and after its  
22 publication in the statute book.