

**HOUSE BILL No. 2842**

By Committee on Appropriations

Requested by Representative B. Carpenter

3-15

Proposed Amendments to HB 2842 - executive branch  
House Legislative Modernization Committee  
Prepared by the Office of Revisor of Statutes  
March 19, 2024

3

1 AN ACT concerning information technology; relating to transferring  
2 information technology employees under the chief information  
3 technology officer of each branch; creating a chief information security  
4 officer within the judicial and legislative branches; requiring the  
5 attorney general, secretary of state, state treasurer and insurance  
6 commissioner to appoint chief information technology officers; placing  
7 the duty of cybersecurity under the chief information technology  
8 officer; requiring state agencies to comply with certain minimum  
9 cybersecurity standards; exempting certain audit reports from the open  
10 records act and eliminating the five-year review of such exemption;  
11 making and concerning appropriations for the fiscal years ending June  
12 30, 2025, and June 30, 2026, for the office of information technology,  
13 Kansas information security office and the adjutant general; authorizing  
14 certain transfers and imposing certain limitations and restrictions, and  
15 directing or authorizing certain disbursements and procedures for all  
16 state agencies; legislative review of state agencies not in compliance  
17 with this act; amending K.S.A. 40-110, 75-413, 75-623, 75-710 and 75-  
18 7203 and K.S.A. 2023 Supp. 45-229, 75-7205, 75-7206, 75-7208, 75-  
19 7238, 75-7239 and 75-7240 and repealing the existing sections.  
20

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

22 Section 1. (a) On and after July 1, 2027, all information technology  
23 services, including cybersecurity services, for each branch of state  
24 government shall be administered by the chief information technology  
25 officer and the chief information security officer of such branch. All  
26 information technology employees within each branch of state government  
27 shall work at the direction of the chief information technology officer of  
28 the branch, except that each state agency that maintains confidential  
29 information, including, but not limited to, legal, healthcare or tax  
30 information may maintain one employee to assist with the information  
31 technology related to such information.

32 (b) Prior to January 1, 2026:

33 (1) The executive chief information technology officer shall develop  
34 a plan to integrate all information technology services into the office of  
35 information technology services. The executive chief information

and excluding enterprise services offered by the  
office of information technology services

strike

1 technology officer shall consult with each ~~senior~~-agency head when  
2 developing such plan.

3 (2) The judicial chief information technology officer shall develop a  
4 plan to integrate all information technology services into the office of the  
5 state judicial administrator. The judicial chief information technology  
6 officer shall develop an estimated project cost to provide information  
7 technology hardware to state and county employees in each judicial  
8 district who access applications administered by the judicial branch. Such  
9 employees shall be required to use such state issued information  
10 technology hardware to access such applications. The judicial chief  
11 information technology officer shall consult with the executive chief  
12 information technology officer to develop a plan to allow each piece of  
13 information technology hardware that is used to access an application  
14 administered by the judicial branch to be part of the KANWIN network  
15 prior to July 1, 2027.

16 (3) The legislative chief information technology officer shall develop  
17 a plan to integrate all information technology services under the legislative  
18 chief information technology officer. The legislative chief information  
19 technology officer shall consult with each legislative agency head when  
20 developing such plan.

21 (c) Each chief information technology officer shall report the plan  
22 developed pursuant to subsection (b) to the senate standing committee on  
23 ways and means and the house standing committee on legislative  
24 modernization or its successor committee prior to January 15, 2026.

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

27 (e) On July 1, 2025, and each year thereafter, moneys appropriated  
28 from the state general fund to or any special revenue fund of any state  
29 agency for information technology and cybersecurity expenditures shall be  
30 appropriated as a separate line item and shall not be merged with other  
31 items of appropriation for such state agency to allow for detailed review  
32 by the senate committee on ways and means and the house of  
33 representatives committee on appropriations during each regular  
34 legislative session.

35 Sec. 2. (a) There is hereby established the position of judicial branch  
36 chief information security officer. The judicial chief information security  
37 officer shall be in the unclassified service under the Kansas civil service  
38 act, shall be appointed by the judicial administrator, subject to approval by  
39 the chief justice and shall receive compensation determined by the judicial  
40 administrator, subject to approval of the chief justice.

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

- 42 (1) Report to the judicial branch chief information technology officer;
- 43 (2) establish security standards and policies to protect the branch's

1 information technology systems and infrastructure in accordance with  
2 subsection (c);

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

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

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

10 (6) be responsible for the ~~security~~ of all judicial branch data and  
11 information resources;

12 (7) ~~create a database of all electronic devices within the branch and~~  
13 ~~ensure that each device is inventoried, cataloged and tagged with an~~  
14 ~~inventory device;~~

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

19 (9) ~~maintain all third-party data centers at locations within the United~~  
20 ~~States or with companies that are based in the United States;~~

21 (10) review all contracts related to information technology entered  
22 into by a person or entity within the judicial branch to ensure that there are  
23 no security vulnerabilities within the supply chain or product and each  
24 contract contains standard security language; and

25 (11) coordinate with the United States cybersecurity and  
26 infrastructure security agency to perform annual audits of judicial branch  
27 agencies for compliance with applicable state and federal laws, rules and  
28 regulations and judicial branch policies and standards. The judicial chief  
29 information security officer shall make an audit request to such agency  
30 annually, regardless of whether or not such agency has the capacity to  
31 perform the requested audit.

32 (c) The judicial chief information security officer shall develop a  
33 cybersecurity program of each judicial agency that complies with the  
34 national institute of standards and technology cybersecurity framework  
35 (CSF) 2.0, as in effect on July 1, 2024. The judicial chief information  
36 security officer shall ensure that such programs achieve a national institute  
37 of standards and technology score of 3.0 prior to July 1, 2028, and a score  
38 of 4.0 prior to July 1, 2030. The agency head of each judicial agency shall  
39 coordinate with the executive chief information security officer to achieve  
40 such standards.

41 (d) (1) If an audit conducted pursuant to subsection (b)(11) results in  
42 a failure, the judicial chief information security officer shall report such  
43 failure to the speaker of the house of representatives and the president of

cybersecurity

collaborate with the chief information security officers of  
the other branches of state government to respond to  
cybersecurity incidents

strike  
Redesignate paragraphs

CSF tier

1 the senate within 30 days of receiving notice of such failure. Such report  
 2 shall contain a plan to mitigate any security risks identified in the audit.  
 3 The judicial chief information security officer shall coordinate for an  
 4 additional audit after the mitigation plan is implemented and report the  
 5 results of such audit to the speaker of the house of representatives and the  
 6 president of the senate.

7 (2) Results of audits conducted pursuant to subsection (b)(11) and the  
 8 reports described in subsection (d)(1) shall be confidential and shall not be  
 9 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
 10 45-215 et seq., and amendments thereto.

11 Sec. 3. (a) There is hereby established the position of legislative  
 12 branch chief information security officer. The legislative chief information  
 13 security officer shall be in the unclassified service under the Kansas civil  
 14 service act, shall be appointed by the legislative coordinating council and  
 15 shall receive compensation determined by the legislative coordinating  
 16 council.

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

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

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

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

25 (4) develop a centralized cybersecurity protocol for protecting and  
 26 managing legislative branch information technology assets and  
 27 infrastructure;

28 (5) detect and respond to security incidents consistent with  
 29 information security standards and policies;

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

34 (7) ~~create a database of all electronic devices within the branch and~~  
 35 ~~ensure that each device is inventoried, cataloged and tagged with an~~  
 36 ~~inventory device;~~

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

41 (9) ~~maintain all third party data centers at locations within the United~~  
 42 ~~States or with companies that are based in the United States;~~

43 (10) review all contracts related to information technology entered

cybersecurity

collaborate with the chief information security officers of  
 the other branches of state government to respond to  
 cybersecurity incidents

strike  
 Redesignate paragraphs

1 into by a person or entity within the legislative branch to ensure that there  
2 are no security vulnerabilities within the supply chain or product and each  
3 contract contains standard security language; and

4 (11) coordinate with the United States cybersecurity and  
5 infrastructure security agency to perform annual audits of legislative  
6 branch agencies for compliance with applicable state and federal laws,  
7 rules and regulations and legislative branch policies and standards. The  
8 legislative chief information security officer shall make an audit request to  
9 such agency annually, regardless of whether or not such agency has the  
10 capacity to perform the requested audit.

11 (c) The legislative chief information security officer shall develop a  
12 cybersecurity program of each legislative agency that complies with the  
13 national institute of standards and technology cybersecurity framework  
14 (CSF) 2.0, as in effect on July 1, 2024. The legislative chief information  
15 security officer shall ensure that such programs achieve a ~~national institute~~  
16 ~~of standards and technology score of 3.0~~ prior to July 1, 2028, and a score  
17 of 4.0 prior to July 1, 2030. The agency head of each legislative agency  
18 shall coordinate with the legislative chief information security officer to  
19 achieve such standards.

20 (d) (1) If an audit conducted pursuant to subsection (b)(11) results in  
21 a failure, the legislative chief information security officer shall report such  
22 failure to the speaker of the house of representatives and the president of  
23 the senate within 30 days of receiving notice of such failure. Such report  
24 shall contain a plan to mitigate any security risks identified in the audit.  
25 The legislative chief information security officer shall coordinate for an  
26 additional audit after the mitigation plan is implemented and report the  
27 results of such audit to the speaker of the house of representatives and the  
28 president of the senate.

29 (2) Results of audits conducted pursuant to subsection (b)(11) and the  
30 reports described in subsection (d)(1) shall be confidential and shall not be  
31 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
32 45-215 et seq, and amendments thereto.

33 Sec. 4. (a) On July 1, 2028, and each year thereafter, the director of  
34 the budget, in consultation with the legislative, executive and judicial chief  
35 information technology officers as appropriate, shall determine if each  
36 state agency is in compliance with the provisions of this act for the  
37 previous fiscal year. If the director of the budget determines that a state  
38 agency is not in compliance with the provisions of this act for such fiscal  
39 year, the director shall certify an amount equal to 5% of the amount:

- 40 (1) Appropriated and reappropriated from the state general fund for  
41 such state agency for such fiscal year; and
- 42 (2) credited to and available in each special revenue fund for such  
43 state agency in such fiscal year. If during any fiscal year, a special revenue

CSF tier

1 fund has no expenditure limitation, then an expenditure limitation shall be  
2 established for such fiscal year on such special revenue fund by the  
3 director of the budget in an amount that is 5% less than the amount of  
4 moneys credited to and available in such special revenue fund for such  
5 fiscal year.

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

11 (c) During the regular session of the legislature, the senate committee  
12 on ways and means and the house of representatives committee on  
13 appropriations shall consider such compliance determinations and whether  
14 to lapse amounts appropriated and reappropriated and decrease the  
15 expenditure limitations of special revenue funds for such state agencies  
16 during the budget committee hearings for such noncomplying agency.

17 Sec. 5.

18 OFFICE OF INFORMATION TECHNOLOGY SERVICES

19 (a) There is appropriated for the above agency from the state general  
20 fund for the fiscal year ending June 30, 2026, the following:

21 Kansas information  
22 technology office (335-00-1000).....\$65,000,000

23 (b) During fiscal year 2026, the director of the budget, in consultation  
24 with the executive branch chief information technology officer and  
25 executive branch chief information security officer, shall determine the  
26 amount of moneys from the state general fund and each special revenue  
27 fund that each executive branch agency has expended during fiscal years  
28 2021 through 2025 for services performed by the office of information  
29 technology services or the Kansas information security office for such  
30 state agency: *Provided*, That the director of the budget shall determine  
31 such five-year average of each state agency's expenditures from the state  
32 general fund and each special revenue fund: *Provided further*, That during  
33 fiscal year 2026, the director of the budget shall certify the amount so  
34 determined to the director of accounts and reports and, at the same time as  
35 such certification is transmitted to the director of accounts and reports,  
36 shall transmit a copy of such certification to the director of legislative  
37 research: *And provided further*, That upon receipt of each such  
38 certification, the director of accounts and reports shall: (1) For the amounts  
39 from the state general fund, lapse such funds; and (2) for each special  
40 revenue fund, transfer the amount from the special revenue fund of the  
41 state agency to the information technology fund established in K.S.A. 75-  
42 4715, and amendments thereto.

43 Sec. 6.

KANSAS INFORMATION SECURITY OFFICE

(a) There is appropriated for the above agency from the following special revenue fund or funds for the fiscal year ending June 30, 2025, all moneys now or hereafter lawfully credited to and available in such fund or funds, except that expenditures other than refunds authorized by law shall not exceed the following:  
Information technology security fund.....No limit  
Sec. 7.

KANSAS INFORMATION SECURITY OFFICE

(a) There is appropriated for the above agency from the following special revenue fund or funds for the fiscal year ending June 30, 2026, all moneys now or hereafter lawfully credited to and available in such fund or funds, except that expenditures other than refunds authorized by law shall not exceed the following:  
Information technology security fund.....No limit  
Sec. 8.

ADJUTANT GENERAL

(a) There is appropriated for the above agency from the state general fund for the fiscal year ending June 30, 2025, the following:  
Operating expenditures (034-00-1000-0053).....\$250,000  
*Provided*, That expenditures shall be made by the above agency from such account for two full-time employees in the Kansas intelligence fusion center to assist in monitoring state information technology systems:  
*Provided further*, That such employees shall be in the unclassified service of the civil service act and shall be in addition to the positions of the above agency as authorized pursuant to K.S.A. 2023 Supp. 48-3706, and amendments thereto.

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

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

11 (c) The commissioner shall appoint a chief information security  
 12 officer who shall be responsible for establishing security standards and  
 13 policies to protect the department's information technology systems and  
 14 infrastructure. The chief information security officer shall:

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

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

25 (3) (A) coordinate with the United States cybersecurity and  
 26 infrastructure security agency to perform annual audits of the department  
 27 for compliance with applicable state and federal laws, rules and  
 28 regulations and department policies and standards;

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; and

32 (C) 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.

35 Sec. 10. K.S.A. 2023 Supp. 45-229 is hereby amended to read as  
 36 follows: 45-229. (a) It is the intent of the legislature that exceptions to  
 37 disclosure under the open records act shall be created or maintained only  
 38 if:

39 (1) The public record is of a sensitive or personal nature concerning  
 40 individuals;

41 (2) the public record is necessary for the effective and efficient  
 42 administration of a governmental program; or

43 (3) the public record affects confidential information.

CSF tier



1 The maintenance or creation of an exception to disclosure must be  
2 compelled as measured by these criteria. Further, the legislature finds that  
3 the public has a right to have access to public records unless the criteria in  
4 this section for restricting such access to a public record are met and the  
5 criteria are considered during legislative review in connection with the  
6 particular exception to disclosure to be significant enough to override the  
7 strong public policy of open government. To strengthen the policy of open  
8 government, the legislature shall consider the criteria in this section before  
9 enacting an exception to disclosure.

10 (b) Subject to the provisions of subsections (g) and (h), any new  
11 exception to disclosure or substantial amendment of an existing exception  
12 shall expire on July 1 of the fifth year after enactment of the new  
13 exception or substantial amendment, unless the legislature acts to continue  
14 the exception. A law that enacts a new exception or substantially amends  
15 an existing exception shall state that the exception expires at the end of  
16 five years and that the exception shall be reviewed by the legislature  
17 before the scheduled date.

18 (c) For purposes of this section, an exception is substantially  
19 amended if the amendment expands the scope of the exception to include  
20 more records or information. An exception is not substantially amended if  
21 the amendment narrows the scope of the exception.

22 (d) This section is not intended to repeal an exception that has been  
23 amended following legislative review before the scheduled repeal of the  
24 exception if the exception is not substantially amended as a result of the  
25 review.

26 (e) In the year before the expiration of an exception, the revisor of  
27 statutes shall certify to the president of the senate and the speaker of the  
28 house of representatives, by July 15, the language and statutory citation of  
29 each exception that will expire in the following year that meets the criteria  
30 of an exception as defined in this section. Any exception that is not  
31 identified and certified to the president of the senate and the speaker of the  
32 house of representatives is not subject to legislative review and shall not  
33 expire. If the revisor of statutes fails to certify an exception that the revisor  
34 subsequently determines should have been certified, the revisor shall  
35 include the exception in the following year's certification after that  
36 determination.

37 (f) "Exception" means any provision of law that creates an exception  
38 to disclosure or limits disclosure under the open records act pursuant to  
39 K.S.A. 45-221, and amendments thereto, or pursuant to any other  
40 provision of law.

41 (g) A provision of law that creates or amends an exception to  
42 disclosure under the open records law shall not be subject to review and  
43 expiration under this act if such provision:

- 1 (1) Is required by federal law;  
2 (2) applies solely to the legislature or to the state court system;  
3 (3) has been reviewed and continued in existence twice by the  
4 legislature;~~or~~  
5 (4) has been reviewed and continued in existence by the legislature  
6 during the 2013 legislative session and thereafter; *or*  
7 (5) *is a report of the results of an audit conducted by the United*  
8 *States cybersecurity and infrastructure security agency.*  
9 (h) (1) The legislature shall review the exception before its scheduled  
10 expiration and consider as part of the review process the following:  
11 (A) What specific records are affected by the exception;  
12 (B) whom does the exception uniquely affect, as opposed to the  
13 general public;  
14 (C) what is the identifiable public purpose or goal of the exception;  
15 (D) whether the information contained in the records may be obtained  
16 readily by alternative means and how it may be obtained;  
17 (2) an exception may be created or maintained only if it serves an  
18 identifiable public purpose and may be no broader than is necessary to  
19 meet the public purpose it serves. An identifiable public purpose is served  
20 if the legislature finds that the purpose is sufficiently compelling to  
21 override the strong public policy of open government and cannot be  
22 accomplished without the exception and if the exception:  
23 (A) Allows the effective and efficient administration of a  
24 governmental program that would be significantly impaired without the  
25 exception;  
26 (B) protects information of a sensitive personal nature concerning  
27 individuals, the release of such information would be defamatory to such  
28 individuals or cause unwarranted damage to the good name or reputation  
29 of such individuals or would jeopardize the safety of such individuals.  
30 Only information that would identify the individuals may be excepted  
31 under this paragraph; or  
32 (C) protects information of a confidential nature concerning entities,  
33 including, but not limited to, a formula, pattern, device, combination of  
34 devices, or compilation of information that is used to protect or further a  
35 business advantage over those who do not know or use it, if the disclosure  
36 of such information would injure the affected entity in the marketplace.  
37 (3) Records made before the date of the expiration of an exception  
38 shall be subject to disclosure as otherwise provided by law. In deciding  
39 whether the records shall be made public, the legislature shall consider  
40 whether the damage or loss to persons or entities uniquely affected by the  
41 exception of the type specified in paragraph (2)(B) or (2)(C) would occur  
42 if the records were made public.  
43 (i) (1) Exceptions contained in the following statutes as continued in

1 existence in section 2 of chapter 126 of the 2005 Session Laws of Kansas  
2 and that have been reviewed and continued in existence twice by the  
3 legislature as provided in subsection (g) are hereby continued in existence:  
4 1-401, 2-1202, 5-512, 9-1137, 9-1712, 9-22217, 10-630, 12-189, 12-1,108,  
5 12-1694, 12-1698, 12-2819, 12-4516, 16-715, 16a-2-304, 17-1312e, 17-  
6 2227, 17-5832, 17-7511, 17-76139, 19-4321, 21-2511, 22-3711, 22-4707,  
7 22-4909, 22a-243, 22a-244, 23-605, 23-9-312, 25-4161, 25-4165, 31-405,  
8 34-251, 38-2212, 39-709b, 39-719e, 39-934, 39-1434, 39-1704, 40-222,  
9 40-2,156, 40-2c20, 40-2c21, 40-2d20, 40-2d21, 40-409, 40-956, 40-1128,  
10 40-2807, 40-3012, 40-3304, 40-3308, 40-3403b, 40-3421, 40-3613, 40-  
11 3805, 40-4205, 44-510j, 44-550b, 44-594, 44-635, 44-714, 44-817, 44-  
12 1005, 44-1019, 45-221(a)(1) through (43), 46-256, 46-259, 46-2201, 47-  
13 839, 47-844, 47-849, 47-1709, 48-1614, 49-406, 49-427, 55-1,102, 58-  
14 4114, 59-2135, 59-2802, 59-2979, 59-29b79, 60-3333, 60-3336, 65-102b,  
15 65-118, 65-119, 65-153f, 65-170g, 65-177, 65-1,106, 65-1,113, 65-1,116,  
16 65-1,157a, 65-1,163, 65-1,165, 65-1,168, 65-1,169, 65-1,171, 65-1,172,  
17 65-436, 65-445, 65-507, 65-525, 65-531, 65-657, 65-1135, 65-1467, 65-  
18 1627, 65-1831, 65-2422d, 65-2438, 65-2836, 65-2839a, 65-2898a, 65-  
19 3015, 65-3447, 65-34,108, 65-34,126, 65-4019, 65-4922, 65-4925, 65-  
20 5602, 65-5603, 65-6002, 65-6003, 65-6004, 65-6010, 65-67a05, 65-6803,  
21 65-6804, 66-101c, 66-117, 66-151, 66-1,190, 66-1,203, 66-1220a, 66-  
22 2010, 72-2232, 72-3438, 72-6116, 72-6267, 72-9934, 73-1228, 74-2424,  
23 74-2433f, 74-32,419, 74-4905, 74-4909, 74-50,131, 74-5515, 74-7308, 74-  
24 7338, 74-8104, 74-8307, 74-8705, 74-8804, 74-9805, 75-104, 75-712, 75-  
25 7b15, 75-1267, 75-2943, 75-4332, 75-4362, 75-5133, 75-5266, 75-5665,  
26 75-5666, 75-7310, 76-355, 76-359, 76-493, 76-12b11, 76-12c03, 76-3305,  
27 79-1119, 79-1437f, 79-3234, 79-3395, 79-3420, 79-3499, 79-34,113, 79-  
28 3614, 79-3657, 79-4301 and 79-5206.

29 (2) Exceptions contained in the following statutes as certified by the  
30 revisor of statutes to the president of the senate and the speaker of the  
31 house of representatives pursuant to subsection (e) and that have been  
32 reviewed during the 2015 legislative session and continued in existence by  
33 the legislature as provided in subsection (g) are hereby continued in  
34 existence: 17-2036, 40-5301, 45-221(a)(45), (46) and (49), 48-16a10, 58-  
35 4616, 60-3351, 72-3415, 74-50,217 and 75-53,105.

36 (i) (1) Exceptions contained in the following statutes as continued in  
37 existence in section 1 of chapter 87 of the 2006 Session Laws of Kansas  
38 and that have been reviewed and continued in existence twice by the  
39 legislature as provided in subsection (g) are hereby continued in existence:  
40 1-501, 9-1303, 12-4516a, 39-970, 65-525, 65-5117, 65-6016, 65-6017 and  
41 74-7508.

42 (2) Exceptions contained in the following statutes as certified by the  
43 revisor of statutes to the president of the senate and the speaker of the

1 house of representatives pursuant to subsection (e) during 2015 and that  
2 have been reviewed during the 2016 legislative session are hereby  
3 continued in existence: 12-5611, 22-4906, 22-4909, 38-2310, 38-2311, 38-  
4 2326, 40-955, 44-1132, 45-221(a)(10)(F) and (a)(50), 60-3333, 65-4a05,  
5 65-445(g), 65-6154, 71-218, 75-457, 75-712c, 75-723 and 75-7c06.

6 (k) Exceptions contained in the following statutes as certified by the  
7 revisor of statutes to the president of the senate and the speaker of the  
8 house of representatives pursuant to subsection (e) and that have been  
9 reviewed during the 2014 legislative session and continued in existence by  
10 the legislature as provided in subsection (g) are hereby continued in  
11 existence: 1-205, 2-2204, 8-240, 8-247, 8-255c, 8-1324, 8-1325, 12-  
12 17,150, 12-2001, 17-12a607, 38-1008, 38-2209, 40-5006, 40-5108, 41-  
13 2905, 41-2906, 44-706, 44-1518, 45-221(a)(44), (45), (46), (47) and (48),  
14 50-6a11, 65-1,243, 65-16,104, 65-3239, 74-50,184, 74-8134, 74-99b06,  
15 77-503a and 82a-2210.

16 (l) Exceptions contained in the following statutes as certified by the  
17 revisor of statutes to the president of the senate and the speaker of the  
18 house of representatives pursuant to subsection (e) during 2016 and that  
19 have been reviewed during the 2017 legislative session are hereby  
20 continued in existence: 12-5711, 21-2511, 22-4909, 38-2313, 45-221(a)  
21 (51) and (52), 65-516, 65-1505, 74-2012, 74-5607, 74-8745, 74-8752, 74-  
22 8772, 75-7d01, 75-7d05, 75-5133, 75-7427 and 79-3234.

23 (m) Exceptions contained in the following statutes as certified by the  
24 revisor of statutes to the president of the senate and the speaker of the  
25 house of representatives pursuant to subsection (e) during 2012 and that  
26 have been reviewed during the 2013 legislative session and continued in  
27 existence by the legislature as provided in subsection (g) are hereby  
28 continued in existence: 12-5811, 40-222, 40-223j, 40-5007a, 40-5009a,  
29 40-5012a, 65-1685, 65-1695, 65-2838a, 66-1251, 66-1805, 72-8268, 75-  
30 712 and 75-5366.

31 (n) Exceptions contained in the following statutes as certified by the  
32 revisor of statutes to the president of the senate and the speaker of the  
33 house of representatives pursuant to subsection (e) and that have been  
34 reviewed during the 2018 legislative session are hereby continued in  
35 existence: 9-513c(c)(2), 39-709, 45-221(a)(26), (53) and (54), 65-6832,  
36 65-6834, 75-7c06 and 75-7c20.

37 (o) Exceptions contained in the following statutes as certified by the  
38 revisor of statutes to the president of the senate and the speaker of the  
39 house of representatives pursuant to subsection (e) that have been  
40 reviewed during the 2019 legislative session are hereby continued in  
41 existence: 21-2511(h)(2), 21-5905(a)(7), 22-2302(b) and (c), 22-2502(d)  
42 and (e), 40-222(k)(7), 44-714(e), 45-221(a)(55), 46-1106(g) regarding 46-  
43 1106(i), 65-2836(i), 65-2839a(c), 65-2842(d), 65-28a05(n), article 6(d) of

1 65-6230, 72-6314(a) and 74-7047(b),  
 2 (p) Exceptions contained in the following statutes as certified by the  
 3 revisor of statutes to the president of the senate and the speaker of the  
 4 house of representatives pursuant to subsection (e) that have been  
 5 reviewed during the 2020 legislative session are hereby continued in  
 6 existence: 38-2310(c), 40-409(j)(2), 40-6007(a), 45-221(a)(52), 46-1129,  
 7 59-29a22(b)(10) and 65-6747.

8 (q) Exceptions contained in the following statutes as certified by the  
 9 revisor of statutes to the president of the senate and the speaker of the  
 10 house of representatives pursuant to subsection (e) that have been  
 11 reviewed during the 2021 legislative session are hereby continued in  
 12 existence: 22-2302(c)(4)(J) and (c)(6)(B), 22-2502(e)(4)(J) and (e)(6)(B)  
 13 and 65-6111(d)(4).

14 (r) Exceptions contained in the following statutes as certified by the  
 15 revisor of statutes to the president of the senate and the speaker of the  
 16 house of representatives pursuant to subsection (e) that have been  
 17 reviewed during the 2023 legislative session are hereby continued in  
 18 existence: 2-3902 and 66-2020.

19 Sec. 11. K.S.A. 75-413 is hereby amended to read as follows: 75-413.  
 20 (a) The secretary of state may appoint such other assistants and clerks as  
 21 may be authorized by law; but the secretary of state shall be responsible  
 22 for the proper discharge of the duties of all assistants and clerks, and they  
 23 shall hold their offices at the will and pleasure of the secretary and shall do  
 24 and perform such general duties as the secretary may require.

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

29 (1) Develop a cybersecurity program for the office that complies with  
 30 the national institute of standards and technology cybersecurity  
 31 framework (CSF) 2.0, as in effect on July 1, 2024. The chief information  
 32 security officer shall ensure that such programs ~~achieve a national~~  
 33 ~~institute of standards and technology score of 3.0~~ prior to July 1, 2028,  
 34 and a score of 4.0 prior to July 1, 2030.

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

39 (3) (A) coordinate with the United States cybersecurity and  
 40 infrastructure security agency to perform annual audits of the office for  
 41 compliance with applicable state and federal laws, rules and regulations  
 42 and office policies and standards;

43 (B) make an audit request to such agency annually, regardless of

CSF tier

1 whether or not such agency has the capacity to perform the requested  
2 audit; and

3 (C) results of audits conducted pursuant to this paragraph shall be  
4 confidential and shall not be subject to discovery or disclosure pursuant to  
5 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

6 Sec. 12. K.S.A. 75-623 is hereby amended to read as follows: 75-623.

7 (a) The treasurer shall appoint such other assistants, clerks, bookkeepers,  
8 accountants and stenographers as may be authorized by law, each of which  
9 persons shall take the oath of office required of public officers. Such  
10 persons shall hold their offices at the will and pleasure of the state  
11 treasurer.

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

15 The chief information security officer shall:

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

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

26 (3) (A) coordinate with the United States cybersecurity and  
27 infrastructure security agency to perform annual audits of the office for  
28 compliance with applicable state and federal laws, rules and regulations  
29 and office policies and standards;

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

33 (C) results of audits conducted pursuant to this paragraph shall be  
34 confidential and shall not be subject to discovery or disclosure pursuant to  
35 the open records act, K.S.A. 45-215 et seq., and amendments thereto.

36 Sec. 13. K.S.A. 75-710 is hereby amended to read as follows: 75-710.

37 (a) The attorney general shall appoint such assistants, clerks, and  
38 stenographers as shall be authorized by law, and who shall hold their office  
39 at the will and pleasure of the attorney general. All fees and allowances  
40 earned by said assistants or any of them, or allowed to them by any statute  
41 or order of court in any civil or criminal case whatsoever, shall be turned  
42 into the general revenue fund of the state treasury, and the vouchers for  
43 their monthly salaries shall not be honored by the director of accounts and

CSF tier

1 reports until a verified account of the fees collected by them, or either of  
 2 them, during the preceding month, has been filed in the director of  
 3 accounts and reports' office. Assistants appointed by the attorney general  
 4 shall perform the duties and exercise the powers as prescribed by law and  
 5 shall perform other duties as prescribed by the attorney general. Assistants  
 6 shall act for and exercise the power of the attorney general to the extent  
 7 the attorney general delegates them the authority to do so.

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

12 (1) Develop a cybersecurity program for the office that complies with  
 13 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 national  
 16 institute of standards and technology score of 3.0 prior to July 1, 2028,  
 17 and a score of 4.0 prior to July 1, 2030;

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

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

26 (B) make an audit request to such agency annually, regardless of  
 27 whether or not such agency has the capacity to perform the requested  
 28 audit; and

29 (C) results of audits conducted pursuant to this paragraph shall be  
 30 confidential and shall not be subject to discovery or disclosure pursuant to  
 31 the open records act, K.S.A. 45-215 et seq, and amendments thereto.

32 Sec. 14. 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: (A) information technology resource policies and  
 38 procedures and project management methodologies for all state agencies;  
 39 (B) an information technology architecture, including telecommunications  
 40 systems, networks and equipment, that covers all state agencies; (C)  
 41 standards for data management for all state agencies; and (D) a strategic  
 42 information technology management plan for the state;

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

CSF tier

1 state's information technology resources;

2 ~~(2) designate the ownership of information resource processes and the~~  
3 ~~lead agency for implementation of new technologies and networks shared~~  
4 ~~by multiple agencies in different branches of state government; and~~  
5 ~~(4) perform such other functions and duties as necessary to carry out~~  
6 ~~the provisions of this act meet as the council deems necessary for the~~  
7 ~~purpose of discussing information technology policies and procedures.~~

8 Sec. 15. K.S.A. 2023 Supp. 75-7205 is hereby amended to read as  
9 follows: 75-7205. (a) There is hereby established within and as a part of  
10 the office of information technology services the position of executive  
11 chief of information technology officer. The executive chief of information  
12 technology officer shall be in the unclassified service under the Kansas  
13 civil service act, shall be appointed by the governor, and shall receive  
14 compensation in an amount fixed by the governor. The executive chief  
15 of information technology officer shall maintain a presence in any cabinet  
16 established by the governor and shall report to the governor.

17 (b) The executive chief of information technology officer shall:

18 (1) Review and consult with each executive agency regarding  
19 information technology plans, deviations from the state information  
20 technology architecture, information technology project estimates and  
21 information technology project changes and overruns submitted by such  
22 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine  
23 whether the agency has complied with:

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

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

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

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

33 (2) report to the chief of information technology architect all deviations  
34 from the state information architecture that are reported to the executive  
35 information technology officer by executive agencies;

36 (3) submit recommendations to the division of the budget as to the  
37 technical and management merit of information technology projects and  
38 information technology project changes and overruns submitted by  
39 executive agencies that are reportable pursuant to K.S.A. 75-7209, and  
40 amendments thereto;

41 (4) monitor executive agencies' compliance with:

42 (A) The information technology resource policies and procedures and  
43 project management methodologies adopted by the information technology



1 executive council;

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

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

6 (D) the strategic information technology management plan adopted  
7 by the information technology executive council;

8 (5) coordinate implementation of new information technology among  
9 executive agencies and with the judicial and legislative chief information  
10 technology officers;

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

14 (7) perform such other functions and duties as provided by law or as  
15 directed by the governor;

16 (8) ~~consult with the appropriate legal counsel on topics related to~~  
17 ~~confidentiality of information, the open records act, K.S.A. 45-215 et seq.,~~  
18 ~~and amendments thereto, the open meetings act, K.S.A. 75-4317 et seq.,~~  
19 ~~and amendments thereto, and any other legal matter related to~~  
20 ~~information technology; and~~

21 (9) ~~ensure that each executive agency has the necessary information~~  
22 ~~technology and cybersecurity staff imbedded within the agency to~~  
23 ~~accomplish the agency's duties.~~

24 (c) ~~An employee of the office of information technology services shall~~  
25 ~~not disclose confidential information of an executive agency. Violation of~~  
26 ~~this subsection is a severity level 5, nonperson felony.~~

27 (d) ~~The executive chief information technology officer may make a~~  
28 ~~request to the adjutant general to permit the 184<sup>th</sup> wing cyber operations~~  
29 ~~group to practice and white hat hack the branch for the purpose of~~  
30 ~~enhancing security. Such hack shall not harm or shutdown any critical~~  
31 ~~infrastructure. The executive chief information technology officer shall~~  
32 ~~notify the executive agency that owns the information that is hacked about~~  
33 ~~such white hat hack and coordinate to mitigate the security risk.~~

34 Sec. 16. K.S.A. 2023 Supp. 75-7206 is hereby amended to read as  
35 follows: 75-7206. (a) There is hereby established within and as a part of  
36 the office of the state judicial administrator the position of judicial chief  
37 information technology officer. The judicial chief information technology  
38 officer shall be appointed by the judicial administrator, subject to approval  
39 of the chief justice, and shall receive compensation determined by the  
40 judicial administrator, subject to approval of the chief justice.

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

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

(10) maintain all third-party data centers at locations within the United States or with companies that are based in the United States; and  
(11) create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged and tagged with an inventory device

Kansas national guard in a state active duty capacity

perform vulnerability assessments or other assessments

During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed

assessed  
assessment

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

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

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

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

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

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

17 (3) submit recommendations to the judicial administrator as to the  
18 technical and management merit of information technology projects and  
19 information technology project changes and overruns submitted by judicial  
20 agencies that are reportable pursuant to K.S.A. 75-7209, and amendments  
21 thereto;

22 (4) monitor judicial agencies' compliance with:

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

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

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

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

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

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

38 (7) perform such other functions and duties as provided by law or as  
39 directed by the judicial administrator; ~~and~~

40 (8) ensure that each judicial agency has the necessary information  
41 technology and cybersecurity staff imbedded ~~within the agency to~~  
42 accomplish the agency's duties;

43 (c) An employee of the office of the state judicial administrator shall

(9) maintain all third-party data centers at locations within the United States or with companies that are based in the United States; and  
(10) create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged and tagged with an inventory device

1 not disclose confidential information of a judicial agency. Violation of this  
2 subsection is a severity level 5, nonperson felony.

3 (d) The judicial chief information technology officer may make a  
4 request to the adjutant general to permit the 18<sup>th</sup> wing cyber operations  
5 group to practice and white hat hack the branch for the purpose of  
6 enhancing security. ~~Such hack shall not harm or shutdown any critical  
7 infrastructure. The judicial chief information technology officer shall  
8 notify the judicial agency that owns the information that is hacked about  
9 such white hat hack and coordinate to mitigate the security risk.~~

10 Sec. 17. K.S.A. 2023 Supp. 75-7208 is hereby amended to read as  
11 follows: 75-7208. (a) The legislative chief information technology officer  
12 shall:

13 (a)(1) Review and consult with each legislative agency regarding  
14 information technology plans, deviations from the state information  
15 technology architecture, information technology project estimates and  
16 information technology project changes and overruns submitted by such  
17 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine  
18 whether the agency has complied with the:

19 (A) Information technology resource policies and procedures and  
20 project management methodologies adopted by the information technology  
21 executive council;

22 (B) information technology architecture adopted by the  
23 information technology executive council;

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

26 (D) strategic information technology management plan adopted by  
27 the information technology executive council;

28 (2) report to the chief information technology architect all  
29 deviations from the state information architecture that are reported to the  
30 legislative information technology officer by legislative agencies;

31 (3) submit recommendations to the legislative coordinating council  
32 as to the technical and management merit of information technology  
33 projects and information technology project changes and overruns  
34 submitted by legislative agencies that are reportable pursuant to K.S.A. 75-  
35 7209, and amendments thereto;

36 (4) monitor legislative agencies' compliance with the:

37 (A) Information technology resource policies and procedures and  
38 project management methodologies adopted by the information technology  
39 executive council;

40 (B) information technology architecture adopted by the  
41 information technology executive council;

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

Kansas national guard in a state active duty capacity

perform vulnerability assessments or other assessments

During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed

assessed

assessment

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

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

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

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

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

(9) consult and obtain approval from the revisor of statutes prior to taking action on topics related to confidentiality of information, the open records act, K.S.A. 45-215 et seq., and amendments thereto, the open meetings act, K.S.A. 75-4317 et seq., and amendments thereto, and any other legal matter related to information technology; and

(10) ensure that each legislative agency has the necessary information technology and cybersecurity staff imbedded within the agency to accomplish the agency's duties.

(11) maintain all third-party data centers at locations within the United States or with companies that are based in the United States; and

(12) create a database of all electronic devices within the branch and ensure that each device is inventoried, cataloged and tagged with an inventory device

Kansas national guard in a state active duty capacity perform vulnerability assessments or other assessments

During such vulnerability assessments, members performing the assessment shall, to the extent possible, ensure that no harm is done to the systems being assessed

assessed

assessment

(b) An employee of the Kansas legislative office of information services or the division of legislative administrative services shall not disclose confidential information of a legislative agency. Violation of this subsection is a severity level 5, nonperson felony.

(c) The legislative chief information technology officer may make a request to the adjutant general to permit the 18<sup>th</sup> wing cyber operations group to practice and white hat hack the branch for the purpose of enhancing security. Such hack shall not harm or shutdown any critical infrastructure. The legislative chief information technology officer shall notify the legislative agency that owns the information that is hacked about such white hat hack and coordinate to mitigate the security risk.

Sec. 18. K.S.A. 2023 Supp. 75-7238 is hereby amended to read as follows: 75-7238. (a) There is hereby established the position of executive branch chief information security officer (CISO). The executive CISO shall be in the unclassified service under the Kansas civil service act, shall be appointed by the governor and shall receive compensation in an amount fixed by the governor.

(b) The executive CISO shall:

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

(2) serve as the state's CISO;

(3) serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance and technologies

1 impairing executive branch cybersecurity programs;

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

5 ~~(5) coordinate cybersecurity efforts between executive branch~~  
6 ~~agencies;~~

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

10 ~~(7) set cybersecurity policy and standards for executive branch~~  
11 ~~agencies; and~~

12 ~~(8) perform such other functions and duties as provided by law and as~~  
13 ~~directed by the executive chief information technology officer establish~~  
14 ~~security standards and policies to protect the branch's information~~  
15 ~~technology systems and infrastructure in accordance with subsection (c);~~

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

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

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

24 (6) be responsible for the ~~security of~~ all executive branch data and  
25 information resources;

26 ~~(7) create a database of all electronic devices within the branch and~~  
27 ~~ensure that each device is inventoried, cataloged and tagged with an~~  
28 ~~inventory device;~~

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

33 ~~(9) maintain all third-party data centers at locations within the~~  
34 ~~United States or with companies that are based in the United States; and~~

35 (10) review all contracts related to information technology entered  
36 into by a person or entity within the executive branch to ensure that there  
37 are no security vulnerabilities within the supply chain or product and each  
38 contract contains standard security language.

39 (c) The executive CISO shall develop a cybersecurity program for  
40 each executive agency that complies with the national institute of  
41 standards and technology cybersecurity framework (CSF) 2.0, as in effect  
42 on July 1, 2024. The executive CISO shall ensure that such programs  
43 achieve a national institute of standards and technology score of 3.0 prior

cybersecurity

collaborate with the chief information security officers of  
the other branches of state government to respond to  
cybersecurity incidents

strike  
Redesignate paragraphs

1 to July 1, 2028, and a score of 4.0 prior to July 1, 2030. The agency head  
2 of each executive agency shall coordinate with the executive CISO to  
3 achieve such standards.

4 Sec. 19. K.S.A. 2023 Supp. 75-7239 is hereby amended to read as  
5 follows: 75-7239. (a) There is hereby established within and as a part of  
6 the office of information technology services the Kansas information  
7 security office. The Kansas information security office shall be  
8 administered by the executive CISO and be staffed appropriately to effect  
9 the provisions of the Kansas cybersecurity act.

10 (b) For the purpose of preparing the governor's budget report and  
11 related legislative measures submitted to the legislature, the Kansas  
12 information security office, established in this section, shall be considered  
13 a separate state agency and shall be titled for such purpose as the "Kansas  
14 information security office." The budget estimates and requests of such  
15 office shall be presented as from a state agency separate from the office of  
16 information technology services, and such separation shall be maintained  
17 in the budget documents and reports prepared by the director of the budget  
18 and the governor, or either of them, including all related legislative reports  
19 and measures submitted to the legislature.

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

21 (1) Administer the Kansas cybersecurity act;  
22 (2) assist the executive branch in developing, implementing and  
23 monitoring/develop, implement and monitor strategic and comprehensive  
24 information security risk-management programs;

25 (3) facilitate executive branch information security governance,  
26 including the consistent application of information security programs,  
27 plans and procedures;

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

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

34 (6)(4) provide the executive branch strategic risk guidance for  
35 information technology projects, including the evaluation and  
36 recommendation of technical controls;

37 (7) assist in the development of executive branch agency  
38 cybersecurity programs to ensure compliance with applicable state and  
39 federal laws, rules and regulations, executive branch policies and standards  
40 and policies and standards adopted by the information technology  
41 executive council;

42 (8)(5) coordinate with the United States cybersecurity and  
43 infrastructure security agency to perform annual audits of executive

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

7 ~~(9)(6)~~ coordinate the use of external resources involved in  
 8 information security programs, including, but not limited to, interviewing  
 9 and negotiating contracts and fees;

10 ~~(10)(7)~~ liaise with external agencies, such as law enforcement and  
 11 other advisory bodies as necessary, to ensure a strong security posture;

12 ~~(11)(8)~~ assist in the development of plans and procedures to manage  
 13 and recover business-critical services in the event of a cyberattack or other  
 14 disaster;

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

18 ~~(13)(9)~~ coordinate with executive branch agencies to provide  
 19 cybersecurity staff to such agencies as necessary;

20 (10) ensure a cybersecurity awareness training program is made  
 21 available to all branches of state government; and

22 ~~(14)(11)~~ perform such other functions and duties as provided by law  
 23 and as directed by the CISO.

24 (d) (1) *If an audit conducted pursuant to subsection (c)(5) results in a*  
 25 *failure, the executive CISO shall report such failure to the speaker of the*  
 26 *house of representatives and the president of the senate within 30 days of*  
 27 *receiving notice of such failure. Such report shall contain a plan to*  
 28 *mitigate any security risks identified in the audit. The executive CISO shall*  
 29 *coordinate for an additional audit after the mitigation plan is implemented*  
 30 *and report the results of such audit to the speaker of the house of*  
 31 *representatives and the president of the senate.*

32 (2) Results of audits conducted pursuant to subsection ~~(9)(8)~~ (c)(5)  
 33 and the reports described in subsection (d)(1) shall be confidential and  
 34 shall not be subject to discovery or disclosure pursuant to the open records  
 35 act, K.S.A. 45-215 et seq., and amendments thereto. ~~The provisions of this~~  
 36 ~~subsection shall expire on July 1, 2028, unless the legislature reviews and~~  
 37 ~~acts to continue such provision pursuant to K.S.A. 45-229, and~~  
 38 ~~amendments thereto, prior to July 1, 2028.~~

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

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

1 Sec. 20. K.S.A. 2023 Supp. 75-7240 is hereby amended to read as  
2 follows: 75-7240. (a) The executive branch agency heads shall:

3 (1) Be solely responsible for security of all data and information  
4 technology resources under such agency's purview, irrespective of the  
5 location of the data or resources. Locations of data may include:

6 (A) Agency sites;

7 (B) Agency real property;

8 (C) Infrastructure in state data centers;

9 (D) Third-party locations; and

10 (E) In transit between locations;

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

13 (3) ~~Designate an information security officer to administer the  
14 agency's information security program that reports directly to executive  
15 leadership;~~

16 (4) ~~(2) participate in CISO-sponsored statewide cybersecurity program  
17 initiatives and services;~~

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

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

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

27 (8) ~~(A) submit a cybersecurity self-assessment report to the CISO by  
28 October 16 of each even-numbered year, including an executive summary  
29 of the findings, that assesses the extent to which the agency is vulnerable  
30 to unauthorized access or harm, including the extent to which the agency's  
31 or contractor's electronically stored information is vulnerable to alteration,  
32 damage, erasure or inappropriate use;~~

33 (B) ~~ensure that the agency conducts annual internal assessments of its  
34 security program. Internal assessment results shall be considered  
35 confidential and shall not be subject to discovery by or release to any  
36 person or agency, outside of the KISO or CISO, without authorization  
37 from the executive branch agency director or head; and~~

38 (C) ~~prepare or have prepared a financial summary identifying  
39 cybersecurity expenditures addressing the findings of the cybersecurity  
40 self-assessment report required in subparagraph (A), excluding  
41 information that might put the data or information resources of the agency  
42 or its contractors at risk and submit such report to the house of  
43 representatives committee on appropriations and the senate committee on~~

Be responsible for security of all data and information  
technology resources under such agency's purview,  
irrespective of the location of the data or resources  
(2)  
Redesignate paragraphs



~~ways and means; and~~  
 2 ~~(9)(3)~~ ensure that if an agency owns, licenses or maintains  
 3 computerized data that includes personal information, confidential  
 4 information or information, the disclosure of which is regulated by law,  
 5 such agency shall, in the event of a breach or suspected breach of system  
 6 security or an unauthorized exposure of that information:

7 (A) Comply with the notification requirements set out in K.S.A. 2023  
 8 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal  
 9 laws and rules and regulations, to the same extent as a person who  
 10 conducts business in this state; and

11 (B) not later than ~~48~~ hours after the discovery of the breach,  
 12 suspected breach or unauthorized exposure, notify: (i) The CISO; and (ii)  
 13 if the breach, suspected breach or unauthorized exposure involves election  
 14 data, the secretary of state.

15 (b) The director or head of each state agency shall:  
 16 (1) Participate in annual agency leadership training to ensure  
 17 understanding of:

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

20 (B) how cyberattacks and data breaches on the agency's operations  
 21 and assets may impact the operations and assets of other governmental  
 22 entities on the state enterprise network;

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

24 (D) steps to be undertaken by the executive director or agency head  
 25 and agency employees to protect their information and information  
 26 systems; *and*

27 (2) ~~ensure that all information technology login credentials are~~  
 28 ~~disabled the same day that any employee ends their employment with the~~  
 29 ~~state; and~~

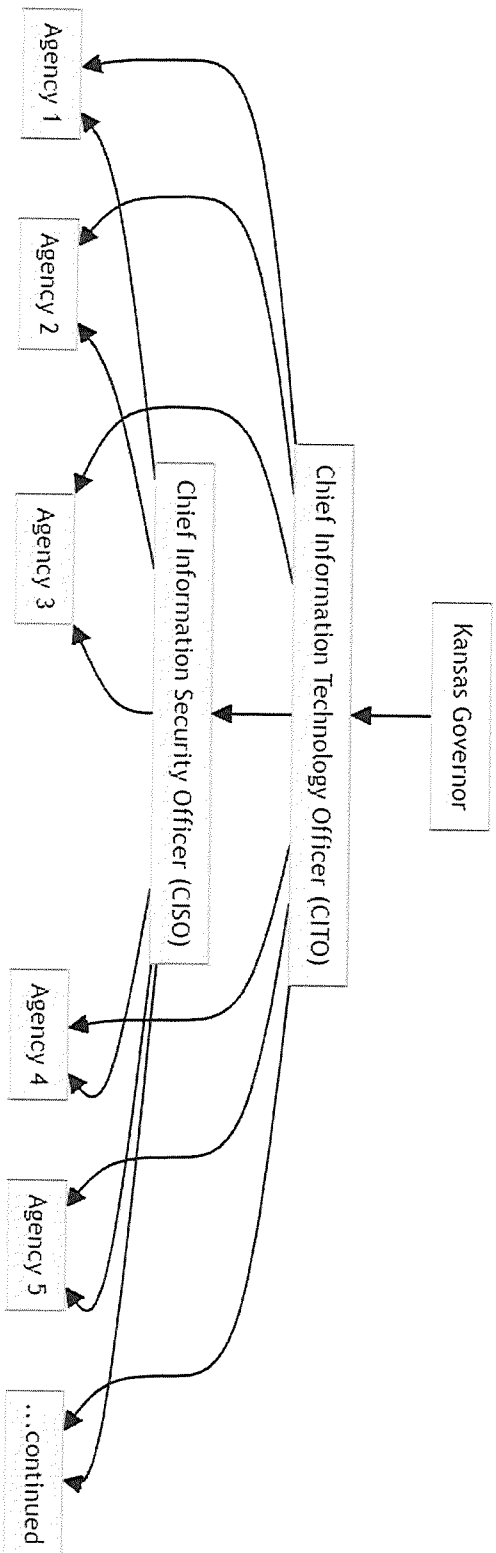
30 (3) ~~require that all employees with access to information technology~~  
 31 ~~receive a minimum of one hour of information technology security~~  
 32 ~~training per year coordinate with the executive CISO to implement the~~  
 33 ~~security standard described in K.S.A. 75-7238, and amendments thereto.~~

34 (e) (1) The CISO, with input from the joint committee on information  
 35 technology and the joint committee on Kansas security, shall develop a  
 36 self-assessment report template for use under subsection (a)(8)(A). The  
 37 most recent version of such template shall be made available to state  
 38 agencies prior to July 1 of each even numbered year. The CISO shall  
 39 aggregate data from the self-assessments received under subsection (a)(8)  
 40 (A) and provide a summary of such data to the joint committee on  
 41 information technology and the joint committee on Kansas security.

42 (2) Self-assessment reports made to the CISO pursuant to subsection  
 43 (a)(8)(A) shall be confidential and shall not be subject to the provisions of

1 the Kansas open records act, K.S.A. 45-215 et seq, and amendments  
2 thereto. The provisions of this paragraph shall expire on July 1, 2028,  
3 unless the legislature reviews and reenacts this provision pursuant to  
4 K.S.A. 45-229, and amendments thereto prior to July 1, 2028.  
5 Sec. 21. K.S.A. 40-110, 75-413, 75-623, 75-710 and 75-7203 and  
6 K.S.A. 2023 Supp. 45-229, 75-7205, 75-7206, 75-7208, 75-7238, 75-7239  
7 and 75-7240 are hereby repealed.  
8 Sec. 22. This act shall take effect and be in force from and after its  
9 publication in the statute book.

# New Proposed Executive Structure for IT and Cyber



Computer  
experiments 3