

## **Substitute for HOUSE BILL No. 2060**

By Committee on Legislative Modernization

2-18

1 AN ACT concerning cybersecurity; relating to the judicial branch;  
2 replacing references to judicial agencies with references to the office of  
3 judicial administration; amending K.S.A. 2024 Supp. 75-7206 and 75-  
4 7206a and repealing the existing sections.

5  
6 *Be it enacted by the Legislature of the State of Kansas:*

7 Section 1. K.S.A. 2024 Supp. 75-7206 is hereby amended to read as  
8 follows: 75-7206. (a) There is hereby established within and as a part of  
9 the office of the state judicial administrator the position of judicial chief  
10 information technology officer. The judicial chief information technology  
11 officer shall be appointed by the judicial administrator, subject to approval  
12 of the chief justice, and shall receive compensation determined by the  
13 judicial administrator, subject to approval of the chief justice.

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

15 (1) Review and consult with each judicial agency regarding  
16 information technology plans, deviations from the state information  
17 technology architecture, information technology project estimates and  
18 information technology project changes and overruns to determine  
19 whether the agency has complied with policies and procedures adopted by  
20 the judicial branch;

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

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

29 (4) coordinate implementation of new information technology among  
30 judicial agencies and with the executive and legislative chief information  
31 technology officers;

32 (5) designate the ownership of information resource processes and the  
33 lead agency for implementation of new technologies and networks shared  
34 by multiple agencies within the judicial branch of state government;

35 (6) perform such other functions and duties as provided by law or as  
36 directed by the judicial administrator;

1 (7) ensure that ~~each~~ *the office of* judicial ~~agency~~ *administration* has  
2 the necessary information technology and cybersecurity staff imbedded  
3 within the ~~agency~~ *office* to accomplish the ~~agency's~~ *office's* duties;

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

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

9 (c) An employee of the office of the state judicial administrator shall  
10 not disclose confidential information of a judicial agency.

11 (d) The judicial chief information technology officer may make a  
12 request to the adjutant general to permit the Kansas national guard in a  
13 state active duty capacity to perform vulnerability assessments or other  
14 assessments of the branch for the purpose of enhancing security. During  
15 such vulnerability assessments, members performing the assessment shall,  
16 to the extent possible, ensure that no harm is done to the systems being  
17 assessed. The judicial chief information technology officer shall notify the  
18 judicial agency that owns the information systems being assessed about  
19 such assessment and coordinate to mitigate the security risk.

20 Sec. 2. K.S.A. 2024 Supp. 75-7206a is hereby amended to read as  
21 follows: 75-7206a. (a) There is hereby established the position of judicial  
22 branch chief information security officer. The judicial chief information  
23 security officer shall be in the unclassified service under the Kansas civil  
24 service act, shall be appointed by the judicial administrator, subject to  
25 approval by the chief justice and shall receive compensation determined  
26 by the judicial administrator, subject to approval of the chief justice.

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

28 (1) Report to the judicial administrator;

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

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

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

37 (5) detect and respond to security incidents consistent with  
38 information security standards and policies;

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

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

43 (8) ensure that all justices, judges and judicial branch employees

1 complete cybersecurity awareness training annually and if an employee  
2 does not complete the required training, such employee's access to any  
3 state-issued hardware or the state network is revoked;

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

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

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

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

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

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

37 Sec. 3. K.S.A. 2024 Supp. 75-7206 and 75-7206a are hereby  
38 repealed.

39 Sec. 4. This act shall take effect and be in force from and after its  
40 publication in the statute book.