Session of 2025

Substitute for HOUSE BILL No. 2060

By Committee on Legislative Modernization

2-18

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

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

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

(b) The judicial chief information technology officer shall:

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

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

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

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

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

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

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

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

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

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

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

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

(b) The judicial chief information security officer shall:

(1) Report to the judicial administrator;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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