State of Kansas

Office of Special Counsel

Kansas Judicial Center
301 SW 10th
Topeka, Kansas 66612-1507 **(785) 506-7145**

March 18, 2024

House Legislative Modernization Committee

Marisa Bayless
Special Counsel to the Chief Justice

Chairwoman Wasinger and members of the committee, thank you for allowing me to provide testimony on behalf of the judicial branch on HB 2842. I first would like to acknowledge and thank Chairwoman Wasinger and Speaker Pro Tem Carpenter for their dedication to the issue of cybersecurity and their work with all the branches of government on this topic.

Bettering the cybersecurity infrastructure and processes of all branches of government is an important and necessary goal. With that in mind, the judicial branch seeks to be a helpful and willing partner to better our state security in this sector. We have made great strides in the past few months but there is more work to be done.

Our IT and cybersecurity experts in the judicial branch took the weekend to review and analyze the requirements in HB 2842. We provide this initial review to pose questions to ensure that the judicial branch achieves the intentions of the bill and to see if there are possibilities for clarification or changes that could advance our system.

Below are considerations and questions from the judicial branch's initial review.

Section 1: Requires the judicial branch to administer all information technology services through the chief information technology officer (CITO) and chief information security officer (CISO) by July 1, 2027. Prior to January 1, 2026, the bill requires a plan for integration of all information technology services into the Office of Judicial Administration (OJA), including estimated project costs to provide information technology hardware to state and county employees in each judicial district who access applications administered by the judicial branch. By July 1, 2027, all information technology hardware that is used to access an application administered by the judicial branch is to be part of the KANWIN network.

Considerations

- Currently, each county is responsible for providing the hardware and information technology assets and tools to judicial branch employees, except those who are

considered under the Office of Judicial Administration (OJA) or appellate courts. Additionally, the county or a vendor supports the endpoints and network. The judicial branch has a little over 2,000 employees, but only approximately 300 of those employees are OJA and appellate court employees within the Kansas Judicial Center that are already supported by the State. Providing the hardware and necessary infrastructure to district courts statewide will require extensive logistical planning and deployment of those assets in addition to the initial cost and ongoing expense of hardware and software. The ultimate number of endpoint devices will be greater than the total number of employees due to the number of computers, laptops, and tablets that are utilized in different areas of a courthouse, like self-help centers, on the bench, and at court reporter tables.

- We want to ensure the KANWIN network would be able to support all the traffic that would now be added to it by adding all endpoints across the state, in addition to all the integrations that connect to our programs like the case management system and efiling system. District and county attorneys, state agencies like the Department of Revenue and the Department for Children and Families, and local sheriffs' departments and the Kansas Highway Patrol all have integrations into our system.

    - Would the requirement for KANWIN network integration extend to remote workers? If so, would a VPN connection that routes traffic across the KANWIN be sufficient?
    - Is the KANWIN intended to be the primary network used for data transmission, or would it be acceptable for the KANWIN to function as a secondary connection?

- The network security architecture must be carefully planned and will likely be different for each of the 105 counties. While all counties have a KANWIN connection point, our courthouses may not physically be near those connections and network architectural changes would be needed. Many of our courthouses do not house all the judicial employees in those counties because they do not have enough office space and they are scattered through different county offices. We would need to ensure KANWIN access to those employees, and we would have to respond if a county ever decided to move or transfer employees to different office spaces in the future.

- The timeline for achieving this transfer to KANWIN and all information technology operations under the administration of the Office of Judicial Administration is July 1, 2027. Our fiscal note provides our initial estimate of the cost for network equipment to provide managed network connectivity to the computer assets proposed. However, even with the appropriate funding, the process to complete this may not be achievable by July 1, 2027. Additionally, we would need assurance that the executive branch would be sufficiently supported to handle the proposed load to the KANWIN network.

- The judicial branch is part of the Kansas Criminal Justice Information System (KCJIS) – a system of connected data sources within a secure environment that exchanges information for local, state, and national criminal justice interests. As part of KCJIS, the

judicial branch must follow the policies and procedures of the system including, but not limited to, transferring of data, encryption protocols, and configuration management. Should the judicial branch network be completely under the KANWIN network, the executive branch would then theoretically be able to see the traffic of the judicial branch network. We must ensure that this transfer does not interfere with KCJIS polices and the confidentiality and ethical duties of the judicial branch to protect its information as required.

- The judicial branch has many statutory and rule-based confidentiality requirements, as well as federal mandates, relating to the records that are stored within our systems. In order to satisfy these requirements, there would need to be assurance that the substantive content of network traffic to our systems would not be monitored by OITS and other branches.

- Subsection (d) requires every website maintained by a branch of government or state agency to be moved to a ".gov" domain by January 1, 2025. We currently are in the initial planning process of doing that, but our initial estimate is the transition is expected to take 6 to 8 months in total. Due to the current workload and staffing, it may not be possible to complete that transition by January 1, 2025.

Section 2: Establishes the position of judicial branch chief information security officer and duties. Requires the judicial chief information security officer to develop a cybersecurity program that aligns with specific National Institute of Standards and Technology (NIST) standards and the timeline for that adherence. Audit provisions and reporting requirements are also provided.

Considerations

- Currently, our CISO reports directly to the judicial administrator. The bill would change this parameter to have the CISO report to the CITO. Part of the inherent duties of the Judicial Branch's Chief Information Security Officer is to ensure that cybersecurity controls are the best they can be for our information technology systems. At times that may conflict with the efficiency sought to be achieved by information technology. An equal reporting relationship within the Judicial Branch achieves the equilibrium that must occur when a conflict arises between the needs of the information technology and cybersecurity departments. We believe that the reporting structure we've established is in the best interests of the Judicial Branch and request that the bill be amended to reflect our current reporting structure, including all cybersecurity positions reporting to the CISO.

- Under subsection 2(b)(10) we request clarification on this duty of the CISO. This language likely mirrors Department of Defense Security Technical Implementation Guides, but the current commercial offerings of software like Microsoft would fail this examination and the hardware we utilize for workstations, servers, and networking would also fail. This may not be a realistic goal and we would request revised language.

- Subsection 2(b)(11) requires the CISO to coordinate with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to perform annual audits. We request revised language that explicitly states that we meet the requirements of this subsection when we request the audit. Additionally, this requirement to enter into audit agreements may require the branch to become a member of a federal group and to share data with the federal government in order to qualify for the auditing services based on CISA requirements. We would encourage further investigation on the requirements to receive a CISA audit.

General Considerations

- We work with our county partners on various aspects of judicial branch operations and this relationship is crucial to ensure judicial branch services are provided. The counties have not weighed in to give their perspective on this significant operational change proposed in the bill and the branch believes it necessary to hear their perspective and any concerns. Counties may have existing contracts with IT vendors that potentially would continue post-transition even though they are no longer supporting and managing those employees assigned IT assets.

- Several times the bill refers to "judicial agencies". We would request clarification about what a judicial agency means (*i.e.* the district court in each county, a judicial district, etc.)

    - Judicial Council is defined in K.S.A. 20-2201 as "an independent agency in the judicial branch of government," that has separate governance from the Supreme Court and OJA and currently receives all IT support from OITS. We ask for clarification if the intention is to also bring the Judicial Council under the judicial branch for IT and network support and services.

- Expanding the scope of branch's responsibility for all information technology across the state for judicial branch employees will have an initial cost and ongoing expenses and require additional FTE positions. Our fiscal note reflects our best estimate in the time provided for submission, but we ask the committee to consider that this number is still an estimate and may change greatly as we progress.

- In Section 4, the director of the budget makes the ultimate determination if each state agency is in compliance with the provisions of the act for the previous fiscal year. We respectfully pose the question of whether the director of the budget is the appropriate decision maker in this context.

- In regard to the penalty provision in Section 4, we would request additional guidance regarding any exceptions to the potential lapse in funding. For example, no lapse would occur if a deviation occurred because of a nonfeasance or malfeasance of a vendor, inability to obtain cooperation from an essential vendor, supply chain issues, or for other good cause reasons.

- We understand the impetus behind a penalty provision but must make the committee aware that currently the judicial branch budget is 92% salaries. Any cut could jeopardize important services should we be penalized with a lapse in funding.

- In several places in the bill the term “agency” is used. There is ambiguity here when speaking about a separate branch of government and we would request clarification on the use of “agency” or “state agency”.