State of Kansas
Office of Judicial Administration
Kansas Judicial Center
301 SW 10th
Topeka, Kansas 66612-1507 (785)296-2256

August 27, 2024

Joint Committee on Information Technology

Chairman Peterson and members of the joint committee, my name is Anne Madden Johnson and I am the Acting Chief Information Technology Officer at the Office of Judicial Administration. Thank you for the opportunity to provide this update on our recent IT security efforts, key initiatives related to House Sub. for SB 291, as well as other significant developments within our IT operations.

Update on IT Security Efforts

Since the cybersecurity incident, our information systems have been successfully restored and are fully operational, though we are still addressing a few remaining district court business processes to ensure they return to their pre-October status. Security remains at the forefront of our efforts, and we have taken substantial steps to protect our systems from future threats.

One of the significant developments has been the hiring in February of a Chief Information Security Officer (CISO), Evan Burt, who is now leading our security team. We are also in the process of staffing our security team, who will play a critical role in bolstering our defenses by reviewing security measures, implementing and supporting advanced threat detection systems, managing incident response protocols, and monitoring our network for vulnerabilities. Their expertise will be instrumental in enhancing our ability to protect ourselves against evolving cyber risks. Along with this critical staff expansion, we continue to review and update our policies and procedures, aligning them with the best practices in the industry and ensuring our staff are following them.

A key aspect of our security strategy is the adoption of a Zero Trust policy, which includes strict requirements for using VPN and multi-factor authentication (MFA) when accessing Judicial Branch accounts and systems. Additionally, we have implemented security measures on Judicial Branch and relevant district court endpoints, such as encryption and stringent password policies. These steps are part of a broader initiative to ensure that our network remains secure from both external and internal threats.

Our information system backups were key to our successful restoration and recovery. Even when something works as intended, opportunities to improve may be found. We are taking steps to augment our backup solutions, which will improve our resilience against the many threats and risks we face today.

We have taken significant steps to enhance the security of our environment by fortifying, isolating, or decommissioning systems to reduce vulnerabilities. For example, we recently upgraded the eFiling system to a more modern and secure platform, and we isolated legacy systems before updating them as well. Additionally, we have significantly strengthened our firewall protections and deployed advanced endpoint protection and monitoring across all systems to safeguard against potential threats.

We are committed to supporting the district courts in the event of cyberattacks or other incidents within their counties, ensuring they have the resources and expertise needed to respond effectively and minimize disruption. Additionally, we have acquired advanced identity management licenses for our staff, which will allow us to leverage enhanced compliance and security features. This investment is crucial to ensuring that we remain protected and compliant with regulatory requirements.

House Sub. for SB 291 Efforts

In addition to our IT security initiatives, we have made progress on efforts related to House Sub. for SB 291. One of the major undertakings is the migration to the .gov domain, which will enhance the security and credibility of our online presence. We are in a good position to complete this migration before the deadline of February 1, 2025.

Our new CISO is leading the design and implementation of a comprehensive cybersecurity program, with active involvement from executive leadership in planning and shaping the necessary policies and procedures. This collaborative approach is vital for addressing the cybersecurity challenges specific to the Judicial Branch, aligning with our strategic goals, and ensuring the program's long-term sustainability and success.

We are also strengthening the cybersecurity awareness training program for all Judicial Branch employees and ensuring its timely completion. This enhancement aims to improve overall security awareness and compliance across the organization.

As part of this initiative, we are also developing project costs related to the ownership, management, and protection of district court endpoints, as well as for securing access to the KANWIN network. Additionally, we are reviewing all of our IT contracts to incorporate standard security language ensuring that all our vendors and suppliers meet our security requirements and comply with our protocols.

Other Topics

Beyond our security and legislative efforts, in June, we successfully completed the migration of the Appellate courts to our centralized case management system (CCMS).. Looking ahead, we are preparing for the final district court, Johnson County, to go live on the CCMS in November 2024. This will mark the completion of our statewide CCMS migration efforts.

As we look to the future, several key initiatives are on the horizon. We are preparing to upgrade the CCMS system to enhance its capabilities, exploring cloud options for our data center to boost scalability and resilience, and planning to introduce additional tools to further strengthen our security and compliance posture. Additionally, we are planning to migrate some video conferencing tools to government optimized platforms, which provide additional security for our video conferencing needs.

Thank you for the opportunity to provide an update on IT and security efforts in the judicial branch.