

Report of the Joint Committee on Kansas Security to the 2021 Kansas Legislature

CHAIRPERSON: Senator Dan Goddard

VICE-CHAIRPERSON: Representative Eric Smith

OTHER MEMBERS: Senators Kevin Braun, Mike Petersen, Pat Pettey, and Mary Ware; Representatives Dave Baker, Michael Houser, Jarrod Ousley, and Louis Ruiz

CHARGE

Review Various Security Matters

KSA 46-3301 directs the Joint Committee to study, monitor, review, and make recommendations on matters related to the security of state officers or employees, state and other public buildings and other property and infrastructure in the state, and to consider measures for the improvement of security for the state. In addition, the Committee is authorized to address additional topics:

- State capabilities in the areas of:
 - Cybersecurity; and
 - Implementation of updates to emergency communications capabilities across the state; and
- The safety of students and state employees.

Joint Committee on Kansas Security

ANNUAL REPORT

Conclusions and Recommendations

The Joint Committee on Kansas Security notes the increasing importance of security for the information assets of the State and therefore strongly encourages cybersecurity training for all legislators and those who work in state government. The State of Kansas and individuals are at risk of fraud and abuse of information systems and the data they contain. The State cannot afford a lax approach to cybersecurity training that has occurred over the past several years by various state agencies as pointed out in reports of the Legislative Division of Post Audit.

- The Committee recommends the Kansas Legislative Office of Information Services offer cybersecurity training to legislators and strongly encourages legislators to participate.
- The Committee commends the Department of Health and Environment (KDHE) for its requirement that each employee receive annual information security training and its emphasis on keeping Kansans' health information confidential.
- The Committee encourages other agencies to review the KDHE training requirements and implement similar protocols. Additionally, there is a need for a thorough and comprehensive review of agency training programs to ensure compliance with information security guidelines by all employees.
- The Committee suggests members of the House Committee on Appropriations and the Senate Committee on Ways and Means, during the budget process, ask each agency to provide information on its security training protocols.
- It became apparent during the Committee meetings a major problem exists with the age and efficiency of the information security systems currently in place in state agencies. The Committee recommends legislative consideration of agency budget enhancements for updating and securing agency information systems.

The Committee notes the increased role of Internet-based conferencing for legislative meetings and needed upgrades to the Statehouse in response and the continuing requirement to provide funding to maintain the added equipment.

The Committee commends the Department of Agriculture for its emphasis on education for food preparation and service businesses and its interactions with licensees using Internet-based conferencing under certain circumstances.

The Committee recognizes changes in business practices by agencies in response to the COVID-19 pandemic. It encourages agencies to evaluate those practices for efficacy and efficiency to determine which practices should be continued when in-person contact is no longer curtailed.

The Committee commends agencies that quickly respond to identified information security weaknesses and the Legislative Division of Post Audit (LPA) for its work on evaluating agency information technology security.

The Committee recommends the LPA recommend to the Legislative Post Audit Committee to schedule a follow-up cybersecurity audit of the Judicial Branch in calendar year 2021.

The Committee recommends the Kansas Highway Patrol, through its Troop K (Capitol Police), develop and implement drills with regard to demonstrations within and near the Statehouse to prevent future interruptions of official legislative proceedings such as committee meetings and meetings in the chambers.

The Committee recommends the 2021 Legislature review and update the Kansas Emergency Management Act to incorporate lessons learned during the COVID-19 pandemic. Specifically, the Committee recommends examination of statutory language including but not limited to KSA 48-924(b) that affects mobilization of the Kansas Division of Emergency Management and the Kansas National Guard. It notes demobilization tied to expiration of a formal declaration of emergency creates inefficiencies when an emergency is reasonably expected to be ongoing.

The Committee supports and commends the collaborative efforts of the Kansas Bureau of Investigation (KBI) and the Department for Children and Families (DCF) to assist youth in foster care who may be or become victims of human trafficking or sexual violence. It expresses its hope such efforts can be extended statewide.

The Committee supports proposals of the KBI:

- To mandate the submission and testing of every sexual assault kit collected through a reported sexual offense; and
- To establish Child Victim Task Forces like that in the Northeast Region in other KBI regions of the state and work in cooperation with the DCF to protect vulnerable children.

Proposed Legislation: None.

BACKGROUND

The 2004 Legislature created the Joint Committee on Kansas Security (Committee) (KSA 2019 Supp. 46-3301) to study, monitor, review, and make recommendations for the following:

- Matters relating to the security of state officers and employees;
- Security of buildings and property under the ownership or control of the State;
- Matters relating to the security of a public body or agency, public building, or facility;

- Matters relating to the security of the infrastructure of Kansas, including any information system; and
- Measures for the improvement of security for the state.

COMMITTEE ACTIVITIES

Initially granted one meeting day by the Legislative Coordinating Council (LCC), the Committee met on November 16, 2020. At that meeting, Committee members agreed to request a second meeting day from the LCC. That request was granted, and the Committee met again on December 1, 2020. Both meetings were in the Statehouse, with limited participation *via* Zoom. The Committee heard presentations from representatives of the Adjutant General's

Department, Division of Emergency Management; Judicial Branch; Kansas Bureau of Investigation; Kansas Department of Agriculture; Kansas Department of Labor; Kansas Highway Patrol; Kansas Legislative Office of Information Services; and Legislative Division of Post Audit. Certain presentations and portions of presentations were closed under the provisions of KSA 75-4319(b) (12)(C). Staff were not present in the closed sessions.

Adjutant General's Department, Division of Emergency Management

At the meeting on November 16, the Assistant Director of the Kansas Division of Emergency Management (KDEM) reviewed the role of the agency in planning for disaster response and noted the State responds when the resources of the local government and those with whom the local government has mutual aid agreements are insufficient. She stated a local declaration of disaster, in writing or orally, starts the response, and a declaration of disaster from the Governor gives more authority for KDEM to respond.

The Assistant Director described the Kansas Response Plan, which was to be updated in January 2021. She noted the importance of planning, as the agency could be involved with responses to disasters as diverse as grassland fires, a foreign animal disease for which there is a stop-movement order, or a radiological incident at Wolf Creek Generating Station. She reported the agency reviews its response after each incident and described various assets that could be deployed.

The remainder of the Assistant Director's testimony on November 16 was provided in a closed session, with the Chief of Legislative Affairs for the Adjutant General's Department also present. The Assistant Director also gave testimony in a closed session at the December 1 meeting, with the Adjutant General, the Chief of Legislative Affairs, and the Branch Director for Planning and Mitigation, KDEM, also present.

Judicial Branch

Representatives of the Judicial Branch presented information in a closed session at the December 1 meeting. Also present was the

Information Technology (IT) Audit Manager, Legislative Division of Post Audit.

Kansas Bureau of Investigation

At the meeting on November 16, the Executive Officer of the Kansas Bureau of Investigation (KBI) provided information about crime trends, reporting in fiscal year (FY) 2019, overall violent crime (murder, rape, robbery, and aggravated assault and battery) was up 2.6 percent, with the rate for aggravated assault and battery up 6.1 percent. Property crime (burglary, theft, and motor vehicle theft) declined 6.8 percent from FY 2018 to FY 2019. He reported the top five threat concerns for the region that includes Kansas are violent crime with firearms, criminal gangs and crews, homicides, drug trafficking and proliferation, and drug user derivative crime.

To address issues identified regarding analysis of sexual assault kits associated with reported sexual offenses, the agency will seek legislation to compel law enforcement agencies to adopt policies requiring the submission of the kits to forensic laboratories within 14 days and the laboratories to examine those kits, the Executive Officer said.

The Executive Officer stated from calendar years 2015 to 2019, 7,447 children were victims of sexually motivated crimes in Kansas. He described a collaboration between the KBI and the Department for Children and Families (DCF) regarding KBI support to DCF staff with the investigation of violent crimes against children and the agency's activities with the Northeast Child Victims Task Force, activities he said the agency would like to expand to more areas of the state.

The Executive Officer discussed KBI investigation of officer use of force incidents in Kansas (approximately 25 so far in FY 2021, 18 of them investigated by the KBI) and how the planned replacement for the Kansas Incident Based Response System will provide more data on that topic. He also noted the replacement of the Automated Fingerprint Identification System with the Automated Biometric Identification System was underway. He reported the new KBI Cyber Crimes Unit is receiving training and procuring needed hardware and software.

The Executive Officer reviewed additional agency efforts to reduce and track criminal activity in Kansas.

Kansas Department of Agriculture

The Animal Health Commissioner and the Program Managers of Plant Protection and Weed Control and of Food Safety and Lodging presented information to the Committee on behalf of the Kansas Department of Agriculture (KDA) at the November 16 meeting.

The Animal Health Commissioner stated the KDA cooperates with the U.S. Department of Agriculture and a network of more than 1,700 veterinarians in Kansas to monitor for outbreaks of foreign animal diseases, and he reported an increase in the number of outbreak investigations from 22 in federal fiscal year (FFY) 2019 to 57 in FFY 2020. He noted the agency performs exercises regarding stop-movement orders in case of a disease outbreak and an outbreak of foot-and-mouth disease could affect the entire country. He noted KDA focuses on stopping movements of animals infected or exposed to foreign animal diseases, implementing operational biosecurity, increasing traceability, and, when feasible, vaccination. The Animal Health Commissioner mentioned the agency had done some planning for euthanasia and disposal of animal carcasses that could not be processed in a timely manner due to outbreaks of COVID-19 among workers at meat processing plants, but carrying out such plans had not been necessary.

The Program Manager for Plant Protection and Weed Control stated the main pathways of introduction of plant diseases into Kansas are untreated wood packing material, live plants, seed, and firewood. He noted KDA works to prevent problems through licensing, permitting, inspections, surveys, and investigations. The Program Manager provided information on the Secretary of Agriculture's statutory authority to respond to an outbreak of plant pests or disease with quarantine, including disposing of plants infested with pests; making an emergency declaration of a noxious weed; and taking whatever action is necessary specifically to destroy plants affected with or hosting black stem rust disease. The Program Manager briefly discussed recent instances that required a response

that included live plant disease and unsolicited seed shipments.

The Program Manager noted the work of the State Noxious Weed Advisory Committee to address concerns with cedar trees.

The Program Manager for Food Safety and Lodging stated the program's 46 inspectors perform an average of 21,000 inspections a year of the state's more than 17,000 licensed food establishments, food processors, and lodging establishments. He reviewed inspection priorities, noting all inspections of new facilities are scheduled but that other inspections are unannounced; agency procedures to mitigate risks of unintentional or intentional food-borne illness; and investigations of food-borne illness. In response to questions about the effect of the COVID-19 pandemic on this work, he stated some inspections and work to educate licensed businesses have been done *via* videoconferencing, and the agency anticipated using videoconferencing for certain types of interactions with licensees into the future, saving inspector travel time and increasing efficiency.

The Deputy Secretary of Agriculture stated the agency has sufficient authority to mitigate the risks discussed.

Kansas Department of Health and Environment

At the Committee's November 16 meeting, information regarding Kansas Department of Health and Environment (KDHE) information security and agency systems and contact tracing with regard to COVID-19 was provided by the agency's Chief Information Officer (CIO) and the Deputy State Epidemiologist. The State Epidemiologist also answered a question from a Committee member.

The CIO reported on annual cybersecurity training required of all KDHE associates and contractor staff members and said network access is denied for noncompliance. The CIO noted new associates are required to complete the training within 30 days of their start date. He provided general information on technical security components used for protection of data, data encryption, and authentication of users.

The Deputy State Epidemiologist reviewed processes for its contract tracing system, which was developed by Accenture (a state technology vendor) using the Salesforce platform. She noted explicit data-sharing rules apply to this system, there are operational separations of duties, and staff and systems meet statutory and regulatory requirements. Included in staff training is training on confidentiality requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Deputy State Epidemiologist also reviewed the KDHE disease surveillance and reporting system, EpiTrax. She noted all states and U.S. territories use electronic disease surveillance systems, but information crosses state lines only in very rare circumstances (described by the State Epidemiologist); in those cases only information that is not personally identifiable is transferred. The CIO noted staff and systems meet statutory and regulatory requirements, and the systems are compliant with requirements of the federal Centers for Disease Control and Prevention. He provided an overview of the security protocols used to protect the systems data

The KDHE officials stated Coronavirus Aid, Relief, and Economic Security (CARES) Act moneys are being used for these efforts and state support may be required when those moneys are no longer available, including for disease surveillance and laboratory staff. They said the agency is learning new practices and is investing in technology to leverage its capabilities.

Kansas Department of Labor

At the Committee's November 16 meeting, a Deputy Secretary of Labor, accompanied by the Kansas Department of Labor's (KDOL's) Director of Government Affairs and its Information Security Officer, provided an overview of the layers of security for the agency as a whole and for the unemployment compensation system specifically. The Deputy Secretary described, in general terms, approaches the agency takes to guard against threat vectors both internal (*e.g.*, disgruntled employees, employee mistakes) and external (*e.g.*, hackers, fraudsters). He reviewed controls on physical access to KDOL offices and systems. He stated agency attorneys had extensively overhauled data-sharing agreements related to unemployment compensation data and had developed a standard memorandum of

understanding that incorporates state and federal Treasury Offset Program requirements for data security.

The Deputy Secretary stated there has been an "epidemic" of identity theft but no evidence of a data breach for KDOL; he noted there are clear reporting requirements for data breaches. He also stated unemployment compensation fraud had been at a very low level before the COVID-19 pandemic. He noted the agency was collaborating with law enforcement agencies and used its own law enforcement staff members with regard to unemployment compensation fraud and the agency faced daily challenges related to identity theft.

Committee members requested additional information; the Deputy Secretary stated some of the information could be provided only in a closed session. A closed presentation on KDOL cybersecurity was provided at the Committee's December 1 meeting. Participating remotely, the Acting Secretary of Labor, two Deputy Secretaries of Labor, the Secretary of Administration, and the Chief Information Security Officer of the Kansas Information Security Office were authorized to be present.

Kansas Highway Patrol

Two representatives of the Kansas Highway Patrol presented information to the Committee in a closed session at the November 16 meeting. Two officials of the Department of Administration also were present in the closed session.

Kansas Legislative Office of Information Services

At the November 16 meeting, the Legislative Chief Information Technology Officer (LCITO) presented information regarding the Kansas Legislative Office of Information Services (KLOIS), including experience and current cybersecurity activities of staff, a general description of the Statehouse Secure Data Center and updates to software and hardware, and information on legislative meetings using videoconferencing.

The LCITO noted top KLOIS staff have many years of IT experience and described their involvement in the Information Technology

Executive Council (KSA 75-7202) and the Task Force on Cybersecurity of the National Conference of State Legislatures. He stated KLOIS staff have attended or participated in cyber range incident response training, Windows 10, Windows Server 2019, and active directory training.

The LCITO described, in general terms, security measures utilized to protect legislative data. This includes multiple levels of physical security for entry to the Statehouse Secure Data Center, in a subbasement of the Statehouse, and off-site backup systems used to protect legislative data.

The LCITO stated KLOIS staff continually update software and update or replace hardware to keep legislative systems secure, and he described cybersecurity tools KLOIS staff use and upgrades to capacity for legislative interfaces. He noted KLOIS maintains a strict change control process including management approval for updating systems. He stated screening systems block an average of 35,000-40,000 emails each day from coming into the legislative email inboxes, preventing phishing, computer viruses, and malware.

The LCITO stated the Legislature has used Zoom for meetings since March, first with all attendees participating remotely and in hybrid remote and in-person meetings since June. The system allowed simultaneous access to the meetings for the public using the Legislature's YouTube channels and the Legislature's website audio archive system (Harmony). KLOIS and other legislative agency staff monitored remote and hybrid meetings to ensure security. He noted limitations of this system.

The Kansas Virtual Statehouse Project, which the LCITO described, is designed to implement video conference systems in Statehouse committee rooms and the House and Senate chambers. These systems include cameras and monitors mounted to walls, room and centralized system controls, room audio integration, calendar integration, closed captioning, and audio/video streaming. He stated the project, begun in July 2020, is using moneys provided under the federal CARES Act, and the goal was system operation before the start of the

2021 Legislative Session. The security of Legislative meetings is a major requirement of the systems.

Legislative Division of Post Audit

In a closed session at the November 16 meeting, the Legislative Division of Post Audit (LPA) IT Audit Manager, accompanied by the Post Auditor, presented the results of IT audits of the Kansas Department of Transportation (KDOT) and the Judicial Branch. KDOT and Judicial Branch representatives were present when the audit relevant to them was presented.

In a closed session at the December 1 meeting, the IT Audit Manager presented the results of audits of the State Board of Regents and the Kansas Department of Corrections. Agency representatives were present when the audit relevant to them was presented.

CONCLUSIONS AND RECOMMENDATIONS

At its meetings on November 16 and December 1, Committee members discussed their conclusions and recommendations to the 2021 Legislature and agreed to the following:

The Committee notes the increasing importance of security for the information assets of the State and therefore strongly encourages cybersecurity training for all legislators and those who work in state government. The State of Kansas and individuals are at risk of fraud and abuse of information systems and the data they contain. The State cannot afford a lax approach to cybersecurity training that has occurred over the past several years by various State agencies as pointed out in reports of the LPA.

- The Committee recommends the KLOIS offer cybersecurity training to legislators and strongly encourages legislators to participate.
- The Committee commends KDHE for its requirement that each employee receive annual information security training and its emphasis on keeping Kansans' health information confidential.

- The Committee encourages other agencies to review the KDHE training requirements and implement similar protocols. Additionally, there is a need for a thorough and comprehensive review of agency training programs to ensure compliance with information security guidelines by all employees.
- The Committee suggests members of the House Committee on Appropriations and the Senate Committee on Ways and Means, during the budget process, ask each agency to provide information on its security training protocols.
- It became apparent during the Committee meetings a major problem exists with the age and efficiency of the information security systems currently in place in State agencies. The Committee recommends legislative consideration of agency budget enhancements for updating and securing agency information systems.

The Committee notes the increased role for Internet-based conferencing for legislative meetings and needed upgrades to the Statehouse in response, and the continuing requirement to provide funding to maintain the added equipment.

The Committee commends the KDA for its emphasis on education for food preparation and service businesses and its interactions with licensees using Internet-based conferencing under certain circumstances.

The Committee recognizes changes in business practices by agencies in response to the COVID-19 pandemic. It encourages agencies to evaluate those practices for efficacy and efficiency to determine which practices should be continued when in-person contacts are no longer curtailed.

The Committee commends agencies that quickly respond to identified information security

weaknesses and LPA for its work on evaluating agency information technology security.

The Committee recommends the LPA recommend to the Legislative Post Audit Committee to schedule a follow-up cybersecurity audit of the Judicial Branch in calendar year 2021.

The Committee recommends the Kansas Highway Patrol, through its Troop K (Capitol Police), develop and implement drills with regard to demonstrations within and near the Statehouse to prevent future interruptions of official legislative proceedings such as committee meetings and meetings in the chambers.

The Committee recommends the 2021 Legislature review and update the Kansas Emergency Management Act to incorporate lessons learned during the COVID-19 pandemic. Specifically, the Committee recommends examination of statutory language including but not limited to KSA 48-924(b) that affects mobilization of the Kansas Division of Emergency Management and the Kansas National Guard. It notes demobilization tied to expiration of a formal declaration of emergency creates inefficiencies when an emergency is reasonably expected to be ongoing.

The Committee supports and commends the collaborative efforts of the KBI and the DCF to assist youth in foster care who may be or become victims of human trafficking or sexual violence. It expresses its hope such efforts can be extended statewide.

The Committee supports proposals of the KBI:

- To mandate the submission and testing of every sexual assault kit collected through a reported sexual offense; and
- To establish Child Victim Task Forces like that in the Northeast Region in other KBI regions of the state and work in cooperation with the DCF to protect vulnerable children.