Report of the Joint Committee on Kansas Security to the 2022 Kansas Legislature

CHAIRPERSON: Representative Eric Smith

VICE-CHAIRPERSON: Senator Mike Petersen

OTHER MEMBERS: Senators Rick Kloos, Virgil Peck, Jeff Pittman, and Mary Ware; Representatives Dave Baker, Michael Houser, Jarrod Ousley, and Louis Ruiz

CHARGE

Review Various Security Matters

KSA 2020 Supp. 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:

- Hear testimony and formulate recommendations on state capabilities in the areas of:
  - Cybersecurity;
  - Implementation of updates to emergency communications capabilities across the state; and
- Address the safety of students and state employees.

Joint Committee on Kansas Security

Annual Report

Conclusions and Recommendations

The Joint Committee on Kansas Security recommends several measures related to cybersecurity, cybercrime, and Capitol security:

- The Committee recommends increased attention to cybersecurity statewide. It notes increases in crimes related to cybersecurity, the personal information held by taxpayer-supported entities, and testimony it heard regarding specific vulnerabilities in state systems and needs for additional cybersecurity personnel and other capabilities. The Committee recommends the Legislature, particularly the House Committee on Appropriations and the Senate Committee on Ways and Means, consider recommendations of the Kansas Cybersecurity Task Force and other entities, such as the Kansas Information Security Office, that are reviewing cybersecurity in the state and the input of agencies, including those that presented testimony to this committee in determining legislative priorities to add cybersecurity capability in state agencies.

- The Committee recommends the House Committee on Judiciary and the Senate Committee on Judiciary review the penalties for crimes related to identity theft or fraud and determine whether penalties for those types of crimes should be increased.

- The Committee recommends the Kansas Bureau of Investigation develop and distribute protocols for documenting cybercrime for use by state agencies and encourages agency involvement with entities in the state working to address cybersecurity concerns.

- The Committee recommends emergency response training for legislators and legislative staff, coordinated through the Capitol Police, to include but not be limited to, active shooter response training. A drill also could be considered.

- The Committee recommends the Capitol Police evaluate the adequacy of security measures in the lower level of the Capitol Parking Garage.

Proposed Legislation: None.

Background

The 2004 Legislature created the Joint Committee on Kansas Security (Committee) (KSA 2020 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.

The statute also directs the Committee to review and monitor federal moneys received by the State for the purposes of homeland security and other related security matters.

Committee Activities

Granted two meeting days by the Legislative Coordinating Council (LCC), the Committee met on October 12 and 13, 2021. The meeting was held in the Statehouse, with limited participation via Webex.

The Committee heard presentations from representatives of the Kansas Highway Patrol (KHP) on Capitol security, license plate readers, and U.S. Department of Homeland Security funds received by the State; the Department of Administration, on state facility security; the Kansas Information Security Office within the Office of Information Technology Services, on activities of the Governor's Cybersecurity Task Force; the Office of the Secretary of State, on election security; the Adjutant General's Department, on emergency communications; the Legislative Division of Post Audit, on various recent information-security-related audits; the Kansas Department of Labor, on security and fraud prevention; and the Kansas Bureau of Investigation (KBI), on Kansas crime statistics and agency activities.

Some of those presentations were closed under the provisions of KSA 75-4319(b)(12)(C). Legislative staff were not present in the closed sessions.

Kansas Highway Patrol

Capitol Security

Information on security in and near the Capitol was presented by the captain of KHP Troop K, the Capitol Police, in a closed session. Additional KHP personnel were present.

Automated License Plate Readers

The captain of KHP Troop G, which is assigned to the Kansas Turnpike, provided information on automated license plate readers (ALPRs). He described how ALPRs work and how they are used by law enforcement agencies. ALPRs take images of license plates and vehicles, those images of license plates are converted to license plate numbers, and the numbers are compared with license plate numbers of vehicles being sought by law enforcement agencies. The captain described, in general terms, how data are shared based on memoranda of understanding and how the data are protected on servers meeting law enforcement security standards. He also described, in general terms, how access to the data is restricted, based on the user's identity and role within the law enforcement agency and the purpose of the request, and how that access is monitored and audited. He stated the data are held for six months and then deleted in such a way that they cannot be retrieved.

The captain also described how ALPRs can assist law enforcement and three cases in which ALPR information was crucial to identifying the suspect's vehicle. In two of those cases, ALPR data helped locate crime victims; in the third, ALPR data were used to confirm an alibi in a homicide case.

It was noted 2021 SB 305 would require each law enforcement agency that deals with ALPR data to adopt and maintain written policy related to use of ALPR systems; prescribe requirements related to the collection, storage, and sharing of ALPR data; and create criminal penalties for unlawful acts related to ALPR-related data.

Federal Homeland Security Moneys

A KHP executive commander, a major, provided information on federal moneys directed to Kansas under the federal Homeland Security Grant Program and the Nonprofit Security Grant Program; the KHP is the governor-appointed state administrative agency for both.

The major stated the State receives approximately $4.0 million a year through these grants. The KHP major provided information on projects currently funded, amounts provided to each region by type of project in FY 2020 and FY 2021, and equipment resources purchased. He stated that because some projects are multi-year, at the time of the meeting, the KHP was managing eight open programs totaling approximately $25.5 million.

The KHP major described the process by which grant money projects or purchases are approved. The process includes priority-setting by local volunteer coordinating councils in the state's seven Homeland Security regions. Membership in those councils includes representatives of emergency response entities and other community partners. Regional projects are selected based on the Threat and Hazard Identification and Risk Assessment (THIRA) Stakeholder Preparedness Review process to address gaps in capabilities to reach targets that reflect preparedness goals in five areas: planning, organization, equipment, training, and exercises.

The KHP, in its role as state administrative agency, reviews the proposals for their fit with national THIRA priorities, and a senior advisory council further reviews the proposed projects. Once federal grant moneys are received, the KHP is responsible for oversight, program management, and communication among the entities, and it passes-through funds.

The major explained various constraints are placed on the uses. Federal requirements include that at least 25 percent must support law enforcement activities, 80 percent must be directed to local actions and purchases, and 20 percent may go to state agencies, and certain percentages are to address cybersecurity, protect soft targets, enhance information and intelligence sharing, combat domestic violent extremism, and address emergent threats. The Kansas target for funds to address cybersecurity is 25 percent, and additional Kansas priorities as defined by the Adjutant General, as the signing authority for the agreement, include enhancing the protection of soft targets, enhancing information and intelligence sharing, and addressing emergent threats and deployable resources.

He answered questions on topics including project selection, maintenance of equipment purchased, and protection of food-related assets.

State Facility Security

The Secretary of Administration, representatives of Burns & McDonnell, and representatives of the Department of Administration and the KHP were present for a closed session related to state facility security.

Kansas Cybersecurity Task Force

The Chief Information Security Officer (CISO) of the Office of Information Technology Services provided information on the Governor's Cybersecurity Task Force (Task Force) created by Executive Order 21-25. He reviewed the membership of the Task Force, noting the various types of private entities and governmental agencies represented. The CISO noted the Task Force created subcommittees: strategic vision and planning, statewide coordination and collaboration, cyberincident and disruption response, and workforce development and education. He also reviewed the charges to the Task Force, which include facilitating cross-industry and cross-government collaboration to mitigate cybersecurity risks related to critical infrastructure and protected systems, developing a coordinated and collaborative cyberresponse plan, and recommending cost-effective safeguards and resources to accomplish Task Force recommendations. The Task Force focuses on system-level responses, the CISO stated.

The CISO stated a preliminary Task Force report was delivered to the Governor on October 5 and a final report was due December 5, 2021.

Election Security

The Director of Elections of the Office of the Secretary of State (Office) noted the U.S. Department of Homeland Security (DHS) had designated election infrastructure as critical infrastructure. He described security as both systems and processes, including processes in law regarding voting.

The Director of Elections described various actions taken at the state level regarding election

security. He stated the Office works with a vendor to install security safeguards in each county for accessing the statewide voter registration system and described that system as one that may be accessed by each county and used in transferring registration when a voter moves.

He stated the Office has designated an election security specialist to lead election security initiatives and educate county election officials about election security topics.

Additionally, the Office works with DHS and the Kansas Intelligence Fusion Center for ongoing security reviews. In general terms, he described training provided to local officials in all Kansas counties by the Multi-State Information Sharing and Analysis Center, in partnership with the Kansas National Guard, the federal Cybersecurity and Infrastructure Security Agency, DHS, the Federal Bureau of Investigation (FBI), and the Elections Security Initiative before the 2020 primary elections. He noted security measures will need to change with new challenges in subsequent elections

In discussing voting machines, the Director of Elections stated it has been Office policy, since 2005, that no election machine or tabulator may be connected to the internet, and the Office planned to seek legislation to place this requirement in the statutes. He noted voting machines are purchased by the counties, but each machine must meet Office requirements, including that it be certified at the national level through the U.S. Election Assistance Commission. All access to a machine must be documented.

The Director of Elections stated he welcomes questions from the public regarding election security as opportunities to explain measures in place.

Representatives of the Kansas Association of County Clerks and Election Officials who were present were asked about their perspectives. They noted election officials know they can always improve but that mistrust and misinformation were obstacles to effectively doing their jobs. Steps in the election process such as vote tabulation and equipment testing open to view by the public were described.

Emergency Telecommunications Systems

The Statewide Interoperability Coordinator (Coordinator), Adjutant General's Department, reviewed the status and services of the Government Emergency Telecommunications Service (GETS) and FirstNet.

The Coordinator described the GETS as a DHS Cybersecurity and Infrastructure Security Agency service that prioritizes emergency response calls on congested wireline networks during a crisis or disaster. The service issues cards with access numbers and dialing instructions to those authorized for this priority; 1,874 cards have been issued to local agencies or individuals in Kansas. He listed participation numbers for other types of users within the state, such as 549 cards with state agencies or employees. The Coordinator said the State and the Cybersecurity and Infrastructure Security Agency are coordinating to increase the number of cards authorized in Kansas.

The Coordinator provided a brief history of FirstNet, an interoperable wireless communications platform specifically for first responders developed in a public-private partnership using a reserved portion the 700 MHz frequency (Band 14). Congress created the First Responder Network Authority in response to recommendations from the 9/11 Commission. The Coordinator stated AT&T received a 25-year contract to operate FirstNet.

The Coordinator provided lists of new Kansas FirstNet sites, which were identified by state and public safety stakeholders as priority locations; counties in which Band 14 was added to existing sites; and tribal nations with new tower sites. He stated coverage was expanded in the period of 2018-2020 but that the high Verizon market share for public safety broadband had slowed FirstNet adoption.

Information Security Audit Reports

Staff members of the Legislative Division of Post Audit (Post Audit) presented information on several information technology (IT) security audits recently completed by that agency:

- "School Districts' Self-Reported IT Security Practices and Resources," in open session; and

- IT security audits of Wichita State University, the Kansas Department of Revenue, and the Kansas Department for Aging and Disability Services, in closed sessions.

Information presented about the limited-scope audit "School Districts' Self-Reported IT Security Practices and Resources" included that approximately half of all Kansas school districts responded to the Post Audit survey. Of those, nearly 60 percent reported they do not require IT security awareness training or require confidential data to be encrypted when sending it outside of the district's network, 65 percent do not scan their computer systems for vulnerabilities as often as standards suggest, 69 percent did not have an incident response plan, and smaller districts lag behind large districts in implementing some security controls.

Several Post Audit staff were present during the closed sessions. Representatives of each agency for which an IT security audit was reviewed were present only when the audit on their agency was presented. The state CISO was present for presentations on the audits of the Kansas Department of Revenue and the Kansas Department for Aging and Disability Services.

Kansas Department of Labor Fraud Prevention Tools

The Chief of Staff for the Kansas Department of Labor presented information on online security and fraud prevention tools in a closed session. Also present in the closed session were the Secretary of Labor, the Deputy Secretary of Labor, and several other agency representatives.

In open session following the closed session, the Deputy Secretary discussed the differences between traditional fraud, such as wage fraud, and imposter fraud, which he described as primary during the COVID-19 pandemic.

Kansas Crime Statistics and Kansas Bureau of Investigation Activities

After the KBI Director presented introductory remarks, the agency's Executive Officer provided information on various topics.

Violent crime. The Executive Officer stated the FBI had determined overall crime in the United States decreased from 2019 to 2020, but the number of violent crime incidents rose 5 percent, and the number of murders rose 29 percent. KBI data show violent crime in Kansas rose 24.4 percent and homicides rose 48.5 percent (from 130 to 193) from 2019 to 2020. The Executive Officer stated aggravated assaults and battery offenses, 11,201 of them, comprised 81 percent of total violent crime in Kansas in 2020.

He noted the numbers of rapes and robberies fell by 8.2 percent and 7.7 percent, respectively, from 2019 to 2020. He reviewed provisions of 2021 HB 2228, which would create and amend law related to sexual assault evidence kits and collection of evidence related to abuse or sexual assault, to incorporate current best practices into law. He also reviewed the activities of the two-month federal, state, and local law enforcement Operation Triple Beam in south central Kansas, stating the operation resulted in 1,072 arrests and the seizure of firearms, rounds of ammunition, various illegal substances, currency, and six vehicles.

Crimes against children. Information on crimes against children provided by the Executive Officer included that the State Child Death Review Board, in its 2021 report, recommended the Department for Children and Families (DCF) and law enforcement review and adopt a best-practices approach for investigations of allegations of child abuse and neglect. He stated the KBI had requested additional funding to expand the capacity of its investigations division to support a proposed collaborative effort between the KBI and DCF to help identify and investigate incidents that involve physical or sexual abuse of children.

The Executive Officer described the work of the agency's Northeast Child Victims Task Force, whose members were trained in FY 2019 and began working cases in FY 2020; in FY 2021, the Northeast Child Victims Task Force worked 38

investigations and 4 limited assistance requests from local law enforcement agencies. The Executive Officer stated agents in the KBI Child Victims Unit are specifically trained and work crimes against children in the southeast and west regions of the state, but the capacity of the Child Victims Unit means it accepts only those cases that allege crimes under KSA 2020 Supp. 21-6627, sex-related crimes against children with mandatory minimum sentences of 25 or 40 years; the unit was involved in 21 investigations and 3 limited assistance requests in FY 2021.

A KBI Catholic Clergy Task Force, created at the request of the Attorney General in 2019, has initiated 122 investigations and examined 39,610 pages of records from the 4 Catholic dioceses in Kansas, the Executive Officer said.

Drug crimes. The Executive Officer stated illicit drugs have a direct association with both violent and property crimes; methamphetamine, synthetic opioids, and marijuana continue to be the top drug threats; and the Midwest High Intensity Drug Trafficking Area (made up of representatives of law enforcement agencies in Kansas, Illinois, Iowa, Missouri, Nebraska, North Dakota, and South Dakota) identified 770 drug trafficking organizations operating in its states in 2020.

He stated the KBI Special Operations Division opened approximately 200 narcotics investigations in FY 2021 and needs to build its investigative capacity.

Cybersecurity and cybercrimes. A KBI cybersecurity operations and response center is included in the KBI strategic plan, to complement the KBI Cyber Crime Unit added in 2020, the Executive Officer said.

He noted recent cases of cyberattacks included the compromise of a county sheriff's office email system and a ransomware attack on a county government's systems; the FBI's Internet Crimes Complaint Center received almost 800,000 complaints with reported losses exceeding $4.0 billion in 2020, a 69 percent increase from 2019; and the KBI Cyber Crime Unit worked cooperatively with federal, state, and local authorities to review 291 FBI complaints plus additional business email compromises, computer intrusions, denials of service, ransomware attacks, and phishing attempts in Kansas.

He stated the KBI is concerned about threats to state critical infrastructure such as the Kansas Criminal Justice Information System. He noted a shortage of qualified IT professionals in state government across the country, and that state agency files contain much personal data.

Use of force. The Executive Officer reported the KBI, in consultation with and with the support of the Attorney General, is leading an effort to build a functional data collection system to provide information on use-of-force incidents by and against Kansas law enforcement officers.

The data would be used to make informed decisions regarding training, policy, and best practices. He stated the KBI hopes the data will start to be collected in January 2022 and the data repository is expected to have a public-facing website.

Intelligence sharing. A gap occurs in the continuity of communication between intelligence gathering entities and local law enforcement, and the KBI will support creation of a 24/7 intelligence center, the Executive Officer said.

Property crime, specifically catalytic converter thefts. The Executive Officer stated property crimes declined 1.2 percent from 2019 to 2020, but thefts of catalytic converters from vehicles increased. He noted catalytic converters do not have serial numbers or other unique identifiers and contain the precious metals platinum, palladium, and rhodium.

Of the 104 scrap metal dealers registered as of October 6, 2021, with the state scrap metal reporting system that began operation in July 2020, 61 report transactions to the KBI; more than 2 million items were reported as sold to scrap metal dealers, including about 6,000 catalytic converters. He reported the KBI is working to improve the operation of the repository and the transmittal of information to local law enforcement in an effort to assist with criminal investigations and reduce scrap metal theft.

License plate readers. The Executive Officer stated the KBI has not deployed any ALPR cameras and does not own or maintain any ALPR data. He said the KBI believes ALPR data to be a beneficial investigative tool.

Recruitment. Law enforcement agencies across the country have issues with recruiting, including greater hesitancy because of the spotlight on law enforcement, and the KBI hopes the Legislature will support law enforcement in efforts to find a recruitment and retention solution, the Executive Officer stated.

Conclusions and Recommendations

After discussion on topics including agency funding requests, emergency response training for legislators and staff within the Capitol, prosecution of cyber-related crimes, security of public servants, and sharing of information about security threats, Committee members agreed to the following:

- The Committee recommends increased attention to cybersecurity statewide. It notes increases in crimes related to cybersecurity, the personal information held by taxpayer-supported entities, and testimony it heard regarding specific vulnerabilities in state systems and needs for additional cybersecurity personnel and other capabilities. The Joint Committee recommends the Legislature, particularly the House Committee on Appropriations and the Senate Committee on Ways and Means, consider recommendations of the Kansas Cybersecurity Task Force and other entities, such as the Kansas Information Security Office, that are reviewing cybersecurity in the state and the input of agencies including those that presented testimony to this committee in determining legislative priorities to add cybersecurity capability in State agencies.

- The Committee recommends the House Committee on Judiciary and the Senate Committee on Judiciary review the penalties for crimes related to identity theft or fraud and determine whether penalties for those types of crimes should be increased.

- The Committee recommends the KBI develop and distribute protocols for documenting cybercrime for use by state agencies and become more involved with entities in the state working to address cybersecurity concerns.

- The Committee recommends emergency response training for legislators and legislative staff, coordinated through the Capitol Police, to include but not be limited to active shooter response training. A drill also could be considered.

- The Committee recommends the Capitol Police evaluate the adequacy of security measures in the lower level of the Capitol Parking Garage.