

Report of the Joint Committee on Information Technology to the 2018 Kansas Legislature

CHAIRPERSON: Representative Blake Carpenter

VICE-CHAIRPERSON: Senator Mike Petersen

OTHER MEMBERS: Senators Marci Francisco, Tom Holland, Dinah Sykes, and Caryn Tyson; and Representatives Pam Curtis, Keith Esau, Kyle Hoffman, and Brandon Whipple

CHARGE

The Committee is directed to:

- Review, monitor, and report on technology plans and expenditures;
- Review and monitor state agency and institution technology plans and expenditures;
- Make recommendations to the Senate Committee on Ways and Means and House Committee on Appropriations on implementation plans, budget estimates, and three-year strategic information technology plans of state agencies and institutions;
- Evaluate the status of the Kansas Eligibility Enforcement System project;
- Evaluate the status of cybersecurity preparedness within the State;
- Follow up with the Kansas Department of Commerce on activity related to the data breach that occurred in March 2017;
- Allow members of the private sector to present relevant information to the Committee; and
- Review information technology security reports and information technology project reports, in executive session, from the Legislative Division of Post Audit.

Joint Committee on Information Technology

REPORT

Conclusions and Recommendations

The Committee agreed on the following recommendations to the 2018 Legislature:

- Request the Office of Information Technology Services (OITS) present a clear roadmap for the process of mandating actions to improve cybersecurity for state agencies. OITS should ensure the roadmap treats all agencies fairly;
- Request OITS include in its plans the expectation that, if agencies are given the option to take control of their own cybersecurity efforts, agencies be required to consent to a cybersecurity responsibility statement, which would specify actions necessary to improve cybersecurity within each agency and identify individuals within each agency responsible for oversight of cybersecurity activities;
- Elevate the relevance of the cybersecurity discussion, the importance of preventative action, and the responsibility of the State to protect the data entrusted to the State by its citizens;
- Determine how agencies may implement any changes necessary to improve cybersecurity;
- Continue investigation into what needs to be accomplished to allow archiving of the livestream of committee hearings held in the Old Supreme Court Room;
- Enable OITS to provide oversight beyond the initial stages of a project;
- Encourage OITS to develop more tools that will provide better project portfolio management, such as automated reporting tools and software, and work toward better collaboration and integration of systems to avoid duplicative projects; and
- Schedule a meeting of the Joint Committee on Information Technology early in the 2018 Session to consider OITS' proposed roadmap for information technology security and make recommendations for legislative action in the 2018 Session, including discussion on 2017 HB 2331 and 2017 SB 204.

Proposed Legislation: None.

BACKGROUND

The Joint Committee on Information Technology (Committee) has statutory duties assigned by its authorizing legislation in KSA 46-

2101 *et. seq.* The Committee may set its own agenda, meet on call of its Chairperson at any time and any place within the state, and introduce legislation. The Committee consists of ten members: five senators and five representatives.

The duties assigned to the Committee by KSA 46-2102 and by KSA 2017 Supp. 75-7201 *et seq.* are as follows:

- Study computers, telecommunications, and other information technologies used by state agencies and institutions. The state governmental entities defined by KSA 2017 Supp. 75-7201 include executive, judicial, and legislative agencies and Board of Regents institutions;
- Review proposed new acquisitions, including implementation plans, project budget estimates, and three-year strategic information technology (IT) plans of state agencies and institutions. All state governmental entities are required to comply with provisions of KSA 2017 Supp. 75-7209 *et. seq.* in submitting such information for review by the Committee;
- Monitor newly implemented technologies of state agencies and institutions;
- Make recommendations to the Senate Committee on Ways and Means and the House Committee on Appropriations on implementation plans, budget estimates, and three-year plans of state agencies and institutions; and
- Report annually to the Legislative Coordinating Council (LCC) and make special reports to other legislative committees as deemed appropriate.

In addition to the Committee's statutory duties, the Legislature or its committees, including the LCC, may direct the Committee to undertake special studies and to perform other specific duties.

KSA 2017 Supp. 75-7210 requires the legislative, executive, and judicial chief information technology officers (CITOs) to submit annually to the Committee all IT project budget estimates and revisions, all three-year plans, and all deviations from the state IT architecture. The Legislative CITO is directed to review the

estimates and revisions and the three-year plans and the deviations, and then to make recommendations to the Committee regarding the merits of and appropriations for the projects. In addition, the Executive and Judicial CITOs are required to report to the Legislative CITO the progress regarding implementation of projects and proposed expenditures, including revisions to such proposed expenditures.

COMMITTEE ACTIVITIES

The Committee met during the 2017 Interim, as authorized by the LCC, on September 8 and 22, 2017. In addition to these interim meetings, the Committee met during the 2017 Session on March 23, May 3, and May 10, 2017. In addition, the Committee toured the Kansas Intelligence Fusion Center jointly with the House Committee on Government, Technology, and Security on May 23, 2017.

March 23

The Executive CITO presented the most recent Kansas Information Technology Office (KITO) quarterly report of IT projects and explained why four projects were in "alert" status. Members posed questions to the Chief Information Officer (CIO) of the Kansas Department of Health and Environment (KDHE) regarding the Medicaid Management Information System modernization project. The CIO also briefly outlined the history of the Kansas Eligibility Enforcement System (KEES) and provided a status update on that project. The Committee also elected a new Chairperson and Vice-chairperson.

May 3

The CIO of KDHE provided a more thorough update on KEES. The CIO explained that the major challenge in implementing the system has been integrating the older legacy systems into KEES. The CIO then answered several questions posed by members.

In a closed (executive) session, representatives of the Kansas Department of Commerce (KDC) briefed the Committee on the breach occurring within that agency's data system, affecting many Kansas job-seekers.

May 10

The Committee continued discussion with representatives of KDC, in executive session, regarding the data breach. The Committee returned to an executive session to hear an overview of the Kansas Intelligence Fusion Center.

September 8

A representative of the Legislative Division of Post Audit (LPA) presented the most recent IT audits of the Office of the Attorney General, the Kansas Department of Education, and Larned State Hospital. A portion of the LPA representative's presentation was conducted in executive session. LPA staff also presented an update on the KanDrive project undertaken by the Kansas Department of Revenue as a function of LPA's IT project monitoring authority. LPA noted the project was in "caution" status due to concerns regarding the scope, schedule, and quality of the project. LPA also noted enhancements to the project have raised the cost of the project to \$8.6 million from the original \$6.4 million.

The Judicial CITO presented a status update on projects within the Judicial Branch, including a centralized case management system for both district courts and appellate courts, judicial tools software, and an upgrade of the Judicial Branch website. The CITO explained the proposed case management system will increase efficiency, improve data quality and performance measurements, and enable work-sharing among district courts. He further explained, due to the proposed case management system upgrade, it is necessary to also upgrade the Judicial Branch website.

The Acting Legislative CITO told the Committee the LCC was in the process of recruiting and hiring a new Legislative CITO. The Director of Application Services for the Kansas Legislative Office of Information Services (KLOIS) presented on new and continuing projects within the Legislature, including a new Senate chamber voting system, improvements to the Kansas Legislative Information Systems and Services Law Making system used by the Office of Revisor of Statutes, House and Senate chamber automation, improvements to the committee

system, and testing for deployment of Windows 10. The Director for Technical Services for KLOIS also presented an overview of new services offered within the Legislature, including audio streaming from committee rooms, new computers for staff and legislators issued prior to the 2018 Session, and a pilot program to explore the benefits of data encryption.

The Executive CITO presented the most recent quarterly report, highlighting projects in "caution" and "alert" status. He also referenced projects recently approved.

The Executive Deputy Chief Information Security Officer (CISO) presented an overview of how cybersecurity funds allocated to the Office of Information Technology Services (OITS) in the 2017 Session will be used in the coming year: tools and services such as data logging, central user analysis, agency-wide incident response, and denial-of-service protection. He also cited the need for a long-term fiscal solution to enable OITS to provide centralized authority in order to coordinate resources across agencies to improve state cybersecurity.

September 22

The Committee again heard from the CIO of KDHE for an update on KEES. He noted the system went live statewide on August 28, 2017; ongoing support and maintenance will regularly update the system and a new operations manager will work with the vendor (Accenture) to enhance the system. The CIO then answered questions from members, including on three lessons learned from managing the project: 1) dividing such a large project into three phases enabled the team to maintain control of the project; 2) unwavering executive support kept the project stable; and 3) maintaining a good relationship with the vendor while holding the vendor accountable for the specific terms of the contract was a challenging balancing act.

The Deputy Attorney of KDC updated the Committee on the extensive data breach that occurred in March 2017. The Deputy Attorney said KDC clients whose data had been compromised were notified *via* e-mail; clients without valid email addresses were not notified by any other manner. The Committee then heard the

remainder of KDC's presentation in executive session.

The Executive CISO responded to questions presented by members at the September 8 meeting. The CISO stated a number of obstacles must be overcome in making state agencies secure from cyberattacks; among them are a lack of centralized authority, a dearth of cybersecurity professionals in state government, and a lack of funding for cybersecurity measures. The CISO recommended the Committee use 2017 SB 204, a cybersecurity bill then in the Senate Committee on Ways and Means, as a template for legislation introduced in the 2018 Session.

The Executive CITO presented a summary of portfolio project management (PPM). He stated it is an approach that provides better project execution and fewer project failures, and adds value through better outcomes. The CITO then made several recommendations to the Committee based on the principles of PPM, including revising the KITO project threshold of \$250,000 to recognize both cost and risk and transforming KITO into an Enterprise Project Management Office.

The Secretary of Revenue provided an update on the KanLicense project. He noted earlier attempts to modernize the system were unsuccessful so those projects were stopped and the project managers took a new approach in December 2016. He noted the first approach would have cost \$40 million, whereas the revamped project costs are estimated to be less than \$10 million.

CONCLUSIONS AND RECOMMENDATIONS

No legislation was recommended for introduction. The Committee agreed on the following recommendations:

- Request OITS present a clear roadmap for the process of mandating actions to improve cybersecurity for state agencies. OITS should ensure the roadmap treats all agencies fairly;

- Request OITS include in its plans the expectation that, if agencies are given the option to take control of their own cybersecurity efforts, agencies be required to consent to a cybersecurity responsibility statement, which would specify actions necessary to improve cybersecurity within each agency and identify individuals within each agency responsible for oversight of cybersecurity activities;
- Determine ways in which the Legislature may elevate the importance of the discussions surrounding cybersecurity within the State as the Legislature has the responsibility to protect data provided to the State by citizens in the course of doing business with the State;
- Determine how agencies may implement any changes necessary to improve cybersecurity;
- Continue investigation into what needs to be accomplished to allow archiving of the livestream of committee hearings held in the Old Supreme Court Room;
- Enable OITS to provide oversight beyond the initial stages of a project. (A member, noting previous consolidation initiatives and then return to distributed authority, cautioned members not to be precipitous regarding consolidation of authority);
- Encourage OITS to develop more tools that will provide better project portfolio management, such as automated reporting tools and software, and work toward better collaboration and integration of systems to avoid duplicative projects; and
- Schedule a meeting of the Joint Committee on Information Technology early in the 2018 Session to consider OITS' proposed roadmap for IT security and make recommendations for legislative action in the 2018 Session, including discussion on 2017 HB 2331 and 2017 SB 204.