SESSION OF 2017

SUPPLEMENTAL NOTE ON SUBSTITUTE FOR HOUSE BILL NO. 2331

As Amended by House Committee of the Whole

Brief*

Sub. for HB 2331 would enact the Representative Jim Morrison Cybersecurity Act (Act). The bill would create the Kansas Information Security Office (KISO) and establish the position of Chief Information Security Officer (CISO) in statute. The bill also would establish the Kansas Information Technology Enterprise (KITE), which would consolidate the functions of the Office of Technology Services (OITS) and transfer current OITS employees and officers to KITE.

KITE

Transfer of Powers, Moneys, and Employees

On July 1, 2017, OITS would be re-designated as KITE and all properties, moneys, appropriations, rights, and authorities once vested in OITS would become vested in KITE.

The bill would require all officers and employees of cabinet agencies whose duties and functions concern IT report directly to the Chief Information Technology Officer (CITO) on July 1, 2017, but would allow all other executive branch agencies to maintain their independent information technology (IT) functions until July 1, 2019. On and after this date, officers and employees of such agencies whose duties and functions concern IT would report directly to the CITO.

---

*Supplemental notes are prepared by the Legislative Research Department and do not express legislative intent. The supplemental note and fiscal note for this bill may be accessed on the Internet at http://www.kslegislature.org

After July 1, 2018, officers and employees engaged in the performance of powers, duties, or functions for cabinet agencies (as defined by the bill) concerning IT immediately prior to such date would retain their employment with KITE if the CITO determines the officers and employees are necessary to perform the powers, duties, and functions of KITE. After July 1, 2020, officers and employees engaged in functions concerning IT in all other executive branch agencies would retain their employment with KITE if the CITO determines such officers and employees are necessary to perform the powers, duties, and functions of KITE. Any such officer or employee would retain all retirement benefits and rights of civil service that have accrued to or vested in such officer or employee at the time of the transfer. Service of transferred officers or employees would be deemed continuous and any transfer or abolition of classified positions would be made pursuant to the Kansas Civil Service Act and applicable rules and regulations. Any employment conflict arising due to the creation of KITE and subsequent transfer of employees and officers would be resolved by the Governor, whose decision would be final.

Approval of Expenditures

All cabinet agencies would be required to receive approval from the CITO for all IT expenditures within the agency on and after July 1, 2017. All other executive branch agencies would be required to receive such approval on and after July 1, 2019.

The bill would authorize the CITO to adopt rules and regulations to establish a system of prioritization for IT expenditure requests before July 1, 2018. The system would allow agencies to request planning meetings with KITE to discuss pertinent details of projects prior to submission of expenditure requests.

KITE Fund

A fund for KITE would be created in the state treasury and administered by the CITO. Moneys could be used to meet statewide IT requirements, including:

- Project management;
- Security;
- Electronic mail;
- KITE expenses; and
- Any other IT operations.

The CITO would be required to calculate the reasonably anticipated itemized costs of providing IT services to executive branch agencies, and each agency receiving services would reimburse KITE for services provided. All moneys received as reimbursement would be credited to the KITE fund. The CITO would report agencies' reasonably anticipated itemized costs to the Joint Committee on Information Technology on or before August 1 every year.

Additionally, the bill would specify that nothing in the Act would be construed to impair any contract, lease, or agreement in existence before July 1, 2017.

Fund Management

KITE would coordinate with the Division of the Budget to develop an implementation plan to manage all executive branch IT funding, and agency heads would work with KITE and the Division of the Budget to identify IT expenses, contracts, projects, resources, and payment sources.

Information Technology Advisory Board (ITAB)

The bill also would establish in statute the ITAB, attached to KITE for administrative purposes. The membership of ITAB would be composed of various state

entities representing their IT interests and the CITO, who would act as chairperson. The duties of ITAB would include:

- Providing direction and coordination for the application of the state's IT resources for all state agencies;
- Receiving reports from state agencies regarding the state of IT projects and soliciting feedback for improving such services;
- Organizing and directing technical advisory committees to address technology issues and resource management issues as necessary;
- Reviewing and proposing programs and projects referred by CITOs and making recommendations regarding the appropriateness of planning, technologies used, compliance with policy and standards, and resource estimates; and
- Addressing and making recommendations on other IT resource management issues at the request of the CITO of the Information Technology Executive Council.

KISO

KISO would be created within KITE, and KISO would be administered by the executive branch CISO, a position created by the bill. For budgeting purposes, KISO would be a separate agency from the Department of Administration. Under the direction of the CISO, the KISO would perform the following functions for executive branch agencies, unless otherwise specified:

- Assist in developing, implementing, and monitoring strategic and comprehensive information security risk-management programs;

- Facilitate information security governance, including the formation of an information security steering committee or advisory board;
- Create and manage a unified and flexible control framework to integrate and normalize requirements of global laws, standards, and regulations;
- Facilitate a metrics, logging, and reporting framework to measure the efficiency and efficacy of the state information security programs;
- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls;
- Ensure security programs, and technology services offered by vendors, are in compliance with relevant laws, rules, regulations, and policies;
- Coordinate the use of external resources and agencies involved in information security programs;
- Interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects and services;
- Assist in the development of effective disaster recovery policies and standards;
- Assist in the development of implementation plans and procedures to ensure critical services are recovered in a cybersecurity event;
- Review and restructure, as necessary, current IT security responsibilities within the executive branch;
- Coordinate IT security interests among Regents institutions, the legislative branch, the judicial

branch, executive elected office state agencies, and local government entities; and

- Perform other such functions and duties as provided by law and directed by the CISO.

CISO

Duties of the CISO

The CISO would be appointed by the Governor and would have the following duties:

- Report to the CITO;
- Serve as the State's CISO;
- Serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance, and technologies impacting executive branch agency cybersecurity programs;
- Ensure compliance with local policy and applicable regulatory authority for background investigations of executive branch agency personnel;
- Ensure compliance with cybersecurity policies established by the Kansas Information Technology Executive Council;
- Ensure KISO personnel assigned to executive branch agencies are protected from retribution for reporting violations; and
- Coordinate cybersecurity efforts among executive branch agencies, state information resources, and local government.

Authority of the CISO

The CISO would have the authority to carry out the following functions:

- Oversee executive branch agency cybersecurity plans for IT projects, and to stop such projects if they are not compliant with approved cybersecurity plans;
- Conduct *ad hoc* security assessments of executive branch agency information systems and internal IT operating environments;
- Suspend public access to executive branch agency information resources where such resources have been compromised or are likely to be compromised as the result of an identified high-risk vulnerability or threat;
- Hire, promote, suspend, demote, discipline, and dismiss all executive branch cybersecurity positions; and
- Perform such other functions and duties as provided by law and as directed by the CITO or the Governor.

The CISO also would have authority to adopt rules and regulations related to the development of a standard cybersecurity rating for agencies and the process by which agencies could appeal security decisions made by the CISO.

CISO Annual Report

The CISO would be required to submit an annual report to relevant standing and joint legislative committees, to include:

- Projected budget for the next three fiscal years;

- Description of cybersecurity expenditures made in the most recent fiscal year;
- Status of ongoing cybersecurity plans and projects;
- Strategic planning goals met in the most recent fiscal year;
- Results of agency security assessments; and
- Training provided to state employees.

Information related to strategic planning goals, results of security assessments, and state employee training would not be required to be included in the report after July 1, 2020, unless the provision is reviewed and reenacted by the Legislature prior to July 1, 2020.

Cybersecurity State Grant Fund (Grant Fund) and Cybersecurity State Grant Fund Coordinating Council (CSGFCC)

The bill would establish the Grant Fund, which would be administered by the CISO and the CSGFCC for the purpose of responding to a cybersecurity breach. The Grant Fund would contain any unencumbered balance in the Fund not required for expenditures in the upcoming fiscal year on June 30 each year. The balance of the Grant Fund could not fall below $10.0 million during any fiscal year unless the CISO determines expenditure of such funds is necessary to respond to a cybersecurity breach. The CSGFCC would monitor and approve the delivery of cybersecurity services, develop strategies for cybersecurity initiatives, and award available grant funds pursuant to the Act. The CSGFCC would be composed of the CISO, serving as a permanent voting member, and five representatives of executive branch agencies appointed by the Governor to terms of three years, as follows:

- Two members representing IT personnel;

- Two members representing legal counsel; and
- One member representing financial personnel.

The CISO, serving as chair of the CSGFCC, would have authority to administer any Grant Fund service as adopted by CSGFCC, as well as carry out the following duties:

- Serve as the coordinator of Grant Fund services and initiatives;
- Implement statewide Grant Fund service planning;
- Serve subject to the direction of the CSGFCC;
- Ensure that policies adopted by the CSGFCC are carried out;
- Preside over all CSGFCC meetings; and
- Assist the CSGFCC in effectuating the provisions of the Act.

The CSGFCC also would have authority to adopt rules and regulations as necessary to carry out the provisions of the Act.

Cybersecurity State Fund (Fund)

The bill would establish a Fund administered by the CISO and financed by a transfer of all unobligated funds remaining in the OITS special revenue funds designated by the CITO as cybersecurity fee moneys on July 1, 2017. In subsequent years any unencumbered balance in the Fund on June 30 not required for operating expenditures in the upcoming fiscal year could be transferred to the Grant Fund.

Restrictions on Use of Moneys of the Fund and Grant Fund

The moneys of the Fund and the Grant Fund could be used only for necessary and reasonable costs incurred by KISO for the following functions:

- Implementation and delivery of cybersecurity services;
- Purchase, maintenance, and license fees for supporting equipment and software upgrades;
- Training of personnel;
- Installation, service establishment, start-up charges, and monthly recurring charges billed by service suppliers;
- Capital improvements and equipment or other physical enhancements to the cybersecurity program;
- Projects involving the development and implementation of cybersecurity services;
- Cybersecurity consolidation or cost-sharing projects;
- Maintenance of adequate staffing, facilities, and support services of KISO;
- Projects involving the development and implementation of cybersecurity services for local government entities;
- Local government entities' consolidation or cost-sharing cybersecurity projects;
- Promotion of cybersecurity education;

- Development and implementation of a cybersecurity scholarship program; and

- Cybersecurity self-insurance.

Any local government entity using state cybersecurity fund moneys for any purpose other than those authorized by the Act would be required to pay back the funds plus 10 percent to the Grant Fund, upon written order of the CSGFCC. The local government entity could file a request for a hearing within 15 days after service of an order pursuant to the Kansas Administrative Procedure Act. If the CSGFCC finds the local government entity was working in good faith to use the funds in an authorized manner, no repayment would be required.

Amendments to Current Law

Duties of the CITO

In addition to duties outlined in current statute, the CITO would be required to:

- Review, coordinate, and approve all appropriate executive branch IT expenditures;

- Manage and order executive branch IT systems and employees in a uniform, efficient, and cost-effective manner; and

- Deliver IT services to the executive branch agencies through IT systems, to further the priorities of service, effectiveness, prevention of fraud and abuse, and adaptation to developing technologies.

CITO Annual Report

The CITO would be required to submit an annual report to the President of the Senate and the Speaker of the House of Representatives on or before the first day of the legislative session, to be distributed to relevant standing and joint committees, the Kansas Legislative Research Department, and the State Library. The report would include:

- Projected budget for the next three fiscal years;
- Fund balances and expenditures from the most recent fiscal year, broken down by agency;
- Three-year strategic plan for technology for the state;
- Performance measures for KITE;
- Cost savings to the state achieved through implementation of the Act;
- Customer satisfaction ratings; and
- All other information the CITO deems relevant and necessary.

Chief Information Technology Architect (CITA)

The bill would allow the position of CITA to be filled by the KITE Architecture and Standards Committee (Committee), which would be appointed by the CITO. If the CITA position is filled by the Committee, no compensation would be made to Committee members.

Definitions

The bill would change the definition of "executive agency" found in Chapter 75, Article 72 of the Kansas Statutes Annotated (statutes related to IT in state

departments) to “executive branch agency” to mean any agency in the executive branch of the State of Kansas and not elected office agencies, the Kansas Public Employees Retirement System (KPERS), or Regents’ institutions. The bill also would add a definition of “cabinet agency” to terms defined in Chapter 75, Article 72 of the Kansas Statutes Annotated. “Cabinet agency” would be defined as:

- Department of Administration;
- Department of Revenue;
- Department of Commerce;
- Department of Labor;
- Department of Health and Environment (KDHE);
- Kansas Department for Aging and Disability Services;
- Kansas Department for Children and Families;
- Department of Corrections (KDOC);
- Adjutant General;
- Kansas Highway Patrol;
- Kansas Department of Agriculture;
- Kansas Department of Wildlife, Parks and Tourism; and
- Department of Transportation.

Update of Statutory References; Repeal of Certain Sections

The bill would update statutory references to OITS as well as strike references to the Division of Information Systems and Communications (DISC) and repeal sections of law related to DISC.

Background

The House Committee on Government, Technology and Security recommended a substitute bill for HB 2331 that includes amendments to HB 2331 as well as the contents of HB 2359, as amended.

HB 2331

The bill was introduced in the House Committee on Government, Technology and Security. In the House Committee hearing, representatives from OITS, KDHE, Kansas State Board of Nursing (KSBN), and KDOC provided proponent testimony. The OITS representative provided an outline of the intended purpose of the bill. The representative for KDHE discussed the importance of information security for that agency since agency staff collect and maintain large amounts of confidential and sensitive information and the benefits that this bill would bring, such as increased protection and threat monitoring. The testimony from KSBN's representative focused on the potential efficiencies created by the bill. The KDOC representative stated the agency would benefit from the standardization of IT security practices and training programs for staff. All representatives discussed the importance of information security and how this bill would help to analyze and protect agencies from the risks involved in collection and storage of confidential and sensitive information.

In written testimony in favor of the bill, Representative Sloan and Representative Campbell stated the bill would address concerns related to increased database hacks at the national, state, and private-sector levels and the disparities in protection levels among agencies.

A representative of the National Association of State Chief Information Officers (NASCIO) provided neutral testimony on the bill. The representative provided information about the general organizational models for state information

technology functions and the role of state chief information officers.

There were two opponents to the bill. A representative from the Kansas Bureau of Investigation (KBI) stated the bill would have a significant fiscal impact on the KBI and negatively impact funding for the Kansas Criminal Justice Information System. KPERS provided written-only testimony, stating the bill raises potential legal concerns that are serious enough that the agency requests to be exempt from the bill.

The House Committee made several changes to the bill, including:

- Changing a provision granting the CISO discretionary authority to transfer funds from the Fund to the Grant Fund when the Fund has an unencumbered balance from a provision mandating such transfer;
- Striking the date by which the CSGFCC must adopt rules and regulations;
- Adding the type of information to be required in the CISO's annual report and to which committees the report should be submitted;
- Striking the provision that would finance the Fund by using a portion of the vehicle modernization surcharge;
- Adding a provision granting the CISO authority to adopt rules and regulations to develop cybersecurity ratings and an appeals process for agencies;
- Adding a provision that would include vendors who provide security services to the State as entities that KISO must ensure are in compliance with relevant laws, rules, regulations, and policies; and

- Technical amendments as requested by staff.

The House Committee voted to recommend a substitute bill for HB 2331, incorporating the Committee amendments listed above.

HB 2359

The bill was introduced in the House Committee on Government, Technology and Security. In the hearing before the House Committee, one proponent, one neutral conferee, and three opponents testified on the bill.

The CITO spoke in support of the bill. The CITO provided an outline of the purpose, impact, potential funding sources, and time line of the bill.

Neutral testimony was provided by a representative of NASCIO. The representative provided information about the general organizational models for state information technology functions and the role of state chief information officers.

The Executive Director of the Kansas Board of Healing Arts spoke in opposition to the bill and provided an amendment for the Committee's consideration that would exempt fee-funded agencies from the bill. KPERS and the Kansas Historical Society provided written-only testimony in opposition to the bill. KPERS stated the bill raises potential legal concerns that are serious enough that the agency requests to be exempt from the bill. The Kansas Historical Society supported the general direction of the bill, but wanted to maintain the ability to carry out the agency's statutory duties. They also mentioned a need for agency-specific applications and would like to see similar language added to the bill.

The House Committee made the following changes to the bill:

- Striking references to and repealing sections of law related to DISC;
- Updating statutory references to OITS;
- Adding a provision that would enable contracts, leases, and agreements to continue if in existence before July 1, 2017;
- Adding a provision delaying until July 1, 2019, the requirement to receive approval of IT expenditures for non-cabinet executive branch agencies;
- Adding a provision establishing ITAB in statute;
- Adding a provision authorizing the CITO to adopt rules and regulations establishing a system of prioritization for agency requests and a provision specifying how such a system would work; and
- Adding to the CITO's duties a requirement to submit an annual report as specified.

The House Committee inserted the contents of HB 2359, as amended, into Sub. for HB 2331.

No fiscal note was available for the substitute bill when the House Committee took action.

The House Committee of the Whole amended the bill to add KPERS to the list of agencies not defined as an "executive branch agency" in the bill, which would have the effect of exempting KPERS from the provisions of the Act.