SESSION OF 2016

SUPPLEMENTAL NOTE ON HOUSE BILL NO. 2509

As Amended by House Committee on Vision 2020

Brief*

HB 2509, as amended, would require all executive branch agencies to receive approval from the Executive Chief Information Technology Officer (E-CITO) for all expenditures for information technology by the agency, but would provide a basis for an agency to be exempted from this approval requirement. The bill would establish the duties of the E-CITO with regard to the approval of such expenditures, and set out the information to be reviewed by the Executive Chief Information Security Officer (E-CISO) at the direction of the E-CITO and amend the existing duties of the E-CITO. The provisions regarding the review, coordination, and approval of all appropriate information technology expenditures for all executive branch agencies would not apply to the Information Technology Office of the Kansas Lottery. The bill also would establish the Kansas Information Security Office, address the appointment of the E-CISO, and establish the duties of the E-CISO. An "executive branch agency" also would be defined.

Duties of E-CITO in Expenditure Approval

Executive branch agencies would be required to receive approval from the E-CITO for all expenditures for information technology by the agency. Executive branch agencies would be defined as those agencies under the authority of the Governor. The Information Technology Office of the Kansas Lottery would be exempt from the requirements established by the bill to carry out this purpose. The E-CITO would be

---

*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

authorized to exempt an agency from this requirement based on proven competency and exigent circumstances. An annual review of the competency and special circumstances would be required.

The E-CITO would be responsible for the review, coordination, and approval of information technology expenses for executive branch agencies. The head of each agency would be required to provide information to and cooperate with the E-CITO to facilitate the implementation and administration of the new process.

The E-CITO would be responsible for the following:

- Annually presenting the integrated proposed information technology budget for executive branch agencies to the Senate Committee on Ways and Means, the House Committee on Appropriations, and the Joint Committee on Information Technology;
- Developing and adopting policies and procedures for reviewing and approving the information technology expenses of executive branch agencies;
- Delegating, at the E-CITO's discretion, the authority to any executive branch agency to approve any information technology expenses under conditions and procedures prescribed by the E-CITO; and
- Directing the E-CISO to review the:
    - Appropriate information technology structure for ensuring information technology security within executive branch agencies;
    - Security between executive branch agencies and local governmental entities and private vendors;

- Training programs for executive branch employees regarding cyber security;
- Existing assistance programs for local governmental entities that interact with executive branch agencies;
- Compliance monitoring for executive branch agencies regarding cyber security;
- Current information technology security responsibilities for executive branch agencies, and to restructure, as necessary;
- Information technology interests between institutions governed by the regents and executive branch agencies and coordinate such interests; and
- Any other relevant information technology security issues as determined by the E-CITO.

The bill would require the E-CITO be invited to speak before every standing legislative committee at the beginning of the 2017 Legislative Session.

The E-CITO would be prohibited from sweeping the information technology funds and personnel that are deemed by the agency as essential to the agency's meeting of its statutory requirements to serve its constituency and public well being but are not directly associated with information technology security.

General Duties of the E-CITO

The bill would remove the existing requirement that the E-CITO report all deviations from the state information architecture reported to the executive information technology officer by executive branch agencies.

The E-CITO would be tasked with additional responsibilities as follows:

- Monitor executive branch agencies' compliance with the standards for information security adopted by the Information Technology Executive Council; and

- Review, coordinate, and approve all appropriate information technology expenditures for all executive branch agencies pursuant to Section 1 of the bill.

Kansas Information Security Office

The bill would establish the Kansas Information Security Office, administered under the direction and supervision of the E-CISO appointed by the Governor. The initial scope of responsibility of the Kansas Information Security Office would be executive branch agencies, and the scope of this responsibility would be required to be evaluated in fiscal year 2020. The provisions of the Kansas Governmental Operations Accountability Law would apply to the Kansas Information Security Office, and the office would be subject to audit, review, and evaluation under such law.

Duties of the E-CISO

The E-CISO would be appointed by the Governor and would be an unclassified position under the Kansas Civil Service Act. The E-CISO would receive an annual salary fixed by the Governor. The E-CISO would be required to report to the E-CITO.

The E-CISO would perform the duties outlined in detail in the bill under the supervision of the E-CITO, which would include:

- Managing the Kansas Information Security Office organization;

- Developing, implementing, and monitoring a strategic, comprehensive information security and information technology risk-management plan;

- Facilitating information security governance, including the formation of an information security steering committee or advisory board;

- Facilitating a metrics and reporting framework to measure the efficiency and effectiveness of the state information security program;

- Coordinating the use of external resources involved in the information security program, including interviewing, negotiating contracts and fees, and managing external resources;

- Acting as a liaison with external agencies, such as law enforcement and other advisory bodies, to ensure a strong security posture;

- Assisting in the development of effective disaster recovery policies and standards and the development of implementation plans and procedures to ensure business-critical services are recovered, in the event of an information security incident; and

- Reviewing and restructuring, as necessary, current information technology security responsibilities for executive branch agencies.

Background

The bill was introduced by the House Committee on Vision 2020. At the House Committee on Vision 2020 hearing, a representative of Legislative Division of Post Audit testified providing the Committee with an overview of the 2014 State Agency Information Systems Audit and explaining the information technology security concerns. Proponent

testimony was provided by the E-CITO. The E-CITO stated there are real and present risks requiring increased diligence and rigor, and centralizing information security presents a clear benefit to the State. Neutral testimony was provided by the Chief Information Officer of the Kansas Bureau of Investigation explaining, while the bill would provide stronger security, there are concerns about the potential impact to the Kansas Bureau of Investigation mission and to other criminal justice entities. The Interim Secretary of Corrections provided written neutral testimony explaining increased security is important; however, there are concerns about the E-CITO's ability to review funding allocations.

The House Committee amended the bill to:

- Specify the bill applies to the executive branch state agencies, and to define executive branch agencies;
- Establish and clarify additional duties to the E-CITO;
- Establish the Kansas Information Security Office and clarify the responsibilities of the E-CISO;
- Exempt certain agencies from the provisions of the bill;
- Prohibit the E-CITO from sweeping funds or personnel the agency has deem essential; and
- Remove the annual requirement that the executive branch state agencies submit a three-year information technology management and budget plan that includes planned expenses for information technology.

According to the revised fiscal note prepared by the Division of the Budget on the original bill, the Office of Information Technology Services (OITS) indicates the bill

would allow information technology activities to be centralized and improved in the executive branch. Based on a 2013 Wisegate Research Security Benchmark Report, the 2015 Information Security Strategy, and recommendations in the Kansas Statewide Efficiency Review by Alvarez and Marsal, OITS estimates improving executive branch information security would require additional State General Fund expenditures of $2.8 million in FY 2017, $5.5 million in FY 2018 and $8.3 million in FY 2019. These expenditures would be in addition to current information security spending by executive branch agencies. The original fiscal note indicated the costs would be absorbed within the aggregate executive branch information security budget in FY 2017 and FY 2018 and an additional $2.0 million from the State General Fund would be added in FY 2019. OITS also indicates additional information security staff of 5.00 FTE positions in FY 2017, 12.00 FTE positions in FY 2018 and 12.00 FTE positions in FY 2019 would be needed.

The incremental approach for increasing spending proposed by OITS would help bring executive branch security information spending to the recommended benchmark of $8.3 million. OITS indicates the 2015 Information Security Strategy recommends ongoing executive branch information security spending of $8.3 million annually, which includes $3.3 million for staff, $2.2 million for security software, $1.6 million for security hardware, and $1.2 million for outsourcing and third-party services. Any fiscal effect associated with enactment of the bill is not reflected in *The FY 2017 Governor's Budget Report.*