SESSION OF 2018

SUPPLEMENTAL NOTE ON SUBSTITUTE FOR HOUSE BILL NO. 2560

As Recommended by House Committee on Government, Technology and Security

Brief*

Sub. for HB 2560 would create the Kansas Cybersecurity Act (Act).

Definitions

The bill would define various terms used throughout the Act.

Chief Information Security Officer (CISO)

The bill would establish the position of Executive Branch Chief Information Security Officer (CISO). The CISO would be an unclassified employee appointed by the Governor.

Duties of the CISO

Duties of the CISO would include the following:

- Report to the Executive Branch Chief Information Technology Officer (CITO);
- Serve as the State's CISO;
- Serve as the Executive Branch chief cybersecurity strategist and authority on policies, compliance,

*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

procedures, guidance, and technologies impacting executive branch cybersecurity programs;

- Ensure cybersecurity training programs are provided for the executive branch;
- Ensure technology resources assigned or provided to executive branch agencies are in compliance with applicable laws, rules and regulations, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework or an equivalent industry standard;
- Ensure personnel resources assigned or provided to Executive Branch agencies report to the agency's appropriate executive leadership;
- Coordinate cybersecurity efforts among Executive Branch agencies at the state and municipality level and private vendors;
- Provide an annual report on the impact of cybersecurity insurance as a mitigation measure for data breach or unauthorized disclosure of personal information to the House Committee on Government, Technology and Security or its successor committee; and
- Perform such other functions and duties as provided by law and as directed by the Executive Branch CITO.

Authority of the CISO

The CISO would have the authority to:

- Oversee and approve Executive Branch agency cybersecurity plans for information technology (IT) projects;

- Halt Executive Branch agency IT projects or information systems that 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 when compromise of personal information or computer resources have occurred or is likely to occur as the result of an identified high-risk vulnerability or threat; and

- Hire, promote, suspend, demote, discipline, and dismiss all Executive Branch cybersecurity positions.

The CISO would also have the authority to temporarily disconnect an entity from the state network if the CISO identifies an imminent, critical threat to security until the threat is removed.

Kansas Information Security Office (KISO)

The bill would establish the Kansas Information Security Office (KISO) to effect the provisions of the Act. 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:

- Administer the Act;

- Assist the Executive Branch in developing, implementing, and monitoring strategic and comprehensive information security (IS) risk-management programs;

- Provide the Executive Branch with strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls;
- Facilitate Executive Branch agencies IS governance, including the formation of an IS steering committee or advisory board, which would include representation from cabinet and non-cabinet agencies of the Executive Branch;
- Create and manage a unified and flexible framework to integrate and normalize requirements resulting from global laws, standards, and regulations;
- Ensure security programs and technology solutions offered by vendors to the State are in compliance with relevant laws, rules, regulations, and policies;
- Provide the Executive Branch contract provisions with IS language for compliance requirements to expedite review of contracts for security programs and technology solutions;
- Facilitate a metrics, logging, and reporting framework to measure the efficiency and effectiveness of the state IS programs;
- Coordinate the use of external resources involved in IS programs, including, but not limited to, interviewing and negotiating contracts and fees;
- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;
- Assist in the development of effective disaster recovery policies and standards;

- Assist in the development of implementation plans and procedures to ensure that business-critical services are recovered in a cybersecurity event;

- Coordinate IT security interests among governmental entities at the municipality and state levels;

- Provide, and make charges for, cybersecurity services for Executive Branch agencies; and

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

Duties of Executive Branch Agency Heads

The Act would direct Executive Branch agency heads to do the following:

- Be solely responsible for security of all data and IT resources under such entity's purview, irrespective of the location of the data or resources (locations of data may include sites, real property, infrastructure in state data centers, third-party locations, and in transit between locations);

- Ensure an entity-wide IS program is in place;

- Designate an IS officer to administer the agency's IS program that reports directly to executive leadership;

- Participate in CISO-sponsored statewide cybersecurity program initiatives and services;

- Implement policies and standards to ensure that all the agency's data and IT resources are maintained in compliance with applicable state and federal laws and rules and regulations and the NIST

Cybersecurity Framework or an equivalent industry standard;

- Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data and IT resources;

- Include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and IT systems and services;

- Submit a cybersecurity assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to which various systems and devices specified in the Act are vulnerable to unauthorized access or harm and the extent to which electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use;

- Ensure the agency conducts annual internal assessments of its security programs. Such assessment results would be confidential and would not be subject to discovery or release to any person or agency outside of the KISO or CISO until July 1, 2023, unless the provision is reviewed and reenacted by the Legislature prior to that date;

- Prepare a summary of the assessment report, which would exclude information that might put data or information resources of the agency or its contractors at risk, to be made available to the public upon request;

- Participate in annual agency leadership training, which serves to ensure understanding of:
    - Information and information systems that support the operations and assets of the agency;

- Potential impact of common types of cyberattacks and data breaches on the entity's operations and assets, and how such attacks could impact the operations and assets of other governmental entities on the state network;
- How cyberattacks and data breaches occur;
- Steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and
- Annual reporting requirements of the executive director or agency head; and

- Ensure, if an agency owns, licenses, or maintains computerized data that includes personal information, confidential information, or information that is regulated by law regarding its disclosure, it shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information, comply with the notification requirements as set by statute, federal law, and rules and regulations to the same extent as a person who conducts business in the State of Kansas. The entity head would be required to notify the CISO and the Secretary of State (only if the breach involves election data) no later than 48 hours after the discovery of the breach or unauthorized exposure.

Cybersecurity Plans and Validation Reports

All Executive Branch agencies connecting to the state network would be required to demonstrate cybersecurity effectiveness by validating both technical and non-technical cybersecurity controls that constitute IS programs. Validation reports would be provided to the CISO every two years, and would:

- Demonstrate the ability to meet applicable cybersecurity state and federal laws, rules and regulations, and policies through security assessments;

- Include an itemized list of all cybersecurity expenditures though accounts payable reports;

- Include the positions, qualifications, and duties of all cybersecurity staff through personnel records or equivalent information when third parties are used; and

- Demonstrate the entity's ability to secure the information of Kansas citizens and businesses.

The CISO would be required to establish and distribute the validation requirements to Executive Branch agencies and private entities no later than October 1, 2018, with the first validation requirement completed by entities by July 1, 2020. Agency heads would review and approve cybersecurity plans annually while validation reports would be subject to the CISO's review and recommendations.

Protection of Confidential and Personal Information

Executive Branch agencies would be required to adopt and implement a policy, subject to the review and recommendation of the CISO, to protect the privacy of individuals or businesses by preserving the confidentiality of information processed by their websites or applications. Before deploying a website or mobile application that processes confidential or personal information, the developer would be required to submit to the Executive Branch agency's security officer the information required by the agency's policies. The agency's policies would require the developer to submit a security plan that addresses, at a minimum:

- The architecture of the website or application;

- The authentication mechanism for the website or application;
- Logging strategy that addresses specific data elements to be recorded;
- Security of data in transit;
- Security of data at rest; and
- The administrator level access to data included in the website or application.

The website or application would be subject to a vulnerability and penetration test, conducted by the Executive Branch agency internally or by an independent third party.

An executive director or agency head, with input from the CISO, may require employees or contractors whose duties include collection, maintenance, or access to personal information to be fingerprinted and to submit to a state and national criminal history record check at least every five years. The information obtained from the background check may be used for purposes of verifying the identity of the person in question and such person's fitness to work in a position with access to personal information. Local and state law enforcement would assist with fingerprinting and background checks pursuant to this Act, and may charge a fee as reimbursement for expenses incurred.

Any information collected pursuant to this Act (including system information logs, vulnerability reports, risk assessment reports, system security plans, detailed system design plans, network or system diagrams, and audit reports) would be considered confidential by the Executive Branch agency and KISO unless all information that would identify a target, vulnerability, or weakness that would place the organization at risk has been redacted. The provisions of this section would expire on July 1, 2023, unless reviewed and reenacted by the Legislature.

Cybersecurity State Fund

The bill would establish the Cybersecurity State Fund (Fund) within the state treasury, administered by the CISO. All moneys received by the Fund would be used only for necessary and reasonable costs incurred by the KISO for:

- Implementation and delivery of cybersecurity services;
- Purchase, maintenance, and license fees for cybersecurity and supporting equipment and upgrades;
- Purchase, maintenance, and license fees for cybersecurity and supporting software and 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;
- Delivery of cybersecurity services;
- Maintenance of adequate staffing, facilities, and support services of the KISO;

- Projects involving the development and implementation of cybersecurity services or municipalities;
- Municipality consolidation or cost-sharing cybersecurity project;
- Promotion of cybersecurity education;
- Development and implementation of a cybersecurity scholarship program; and
- Cybersecurity insurance.

The bill would allow appropriations for capital outlay and capital improvements to be made to carry out the purposes of KISO as authorized by law. In addition, the CISO would be able to enter into multiple-year contracts, subject to state leasing and purchasing laws.

Rule and Regulation Authority

The CISO would have the discretion to adopt rules and regulations to administer the Act, including:

- Establishment of rates and charges for services performed by the KISO for any governmental entity;
- Determination of priorities for services performed by the KISO, including authority to decline new projects under specified conditions within 30 days, when practicable, after receipt of such a request;
- The manner of performance of any power of duty of the KISO;
- The execution of any business of such office and its relations to and business with other state agencies;

- Appeals from final decisions or final actions of the CISO; and
- Policies for identification of IS vulnerabilities within entities, development of procedures with entities to address identified vulnerabilities, and the assistance provided to entities to implement procedures to address vulnerabilities.

Cybersecurity Rates

Executive Branch agencies would be able to pay for cybersecurity services from existing budgets, grants, or other revenues, or through special assessments to offset costs; any increase in fees or charges due to this Act would be used only for cybsersecurity. Services or transactions with an applied cybersecurity cost recovery fee may indicate the portion of the fee dedicated to cybersecurity on all receipts and transactions records.

Certification of Legislative and Judicial Branch Agencies

Any entity or agency of the Legislative Branch or Judicial Branch that is connecting to the state network would be required to annually certify to the CISO that the entity, in the entity's opinion, is maintaining substantial compliance with the NIST Cybersecurity Framework or an equivalent industry standard.

Background

The bill was introduced by the House Committee on Government, Technology and Security at the request of the Office of Information Technology Services (OITS). In the House Committee hearing, representatives of OITS, the Department of Homeland Security, and the National Association of State Chief Information Officers testified in support of the bill. The representative of OITS stated this bill

would codify in statute the KISO and position of CISO, which were created by Executive Order. Representatives of the Kansas Board of Healing Arts, the Kansas Board of Nursing, the Kansas Public Employees Retirement System (KPERS), and the Kansas State Board of Pharmacy testified as neutral conferees. No opponent testimony was provided.

The House Committee created a substitute bill by removing the original contents of the bill (related to cybersecurity) and inserting new language incorporating various changes to the original bill including:

- Added the definition of “cybersecurity positions”;
- Modified the definition of “Executive Branch agency” to exempt KPERS from that definition;
- Removed the definition of “governmental entity” and “municipality” and references to the terms throughout the remainder of the bill;
- Replaced the requirement that the CISO report to the Governor with the requirement the CISO report to the Executive Branch CITO;
- Added a requirement for substantial compliance with the NIST Cybersecurity Framework, or an equivalent industry standard, for all entities connecting to the state network;
- Added a provision that requires the CISO to provide an annual report on the economic impact of cybersecurity insurance;
- Added a provision that requires the KISO to provide the Executive Branch with IS language for for the purpose of expediting review of contracts for security programs and technology solutions;

- Modified the authority of the CISO to disconnect entities from the state network if the CISO finds the entity is unable to meet compliance standards to only allowing temporary disconnection if an imminent, critical threat is identified;

- Added a provision directing the CISO to establish and distribute cybersecurity effectiveness validation requirements to entities by October 1, 2018;

- Modified a provision related to requiring fingerprinting and background checks of employees or contractors with access to personal information by limiting the authority of the CISO to only give input;

- Added to the CISO's rules and regulation authority a provision establishing a fee structure for any governmental entities connecting to the state network (this provision was subsequently removed by the House Committee);

- Removed a reference to the duty to collect payments in the section governing charges for services provided by the KISO;

- Added a provision that allows any entity or agency of the Legislative Branch or Judicial Branch connecting to the state network to annually certify to the CISO that in the entity's or agency's opinion, such entity or agency is maintaining substantial compliance with the NIST Cybersecurity Framework or an equivalent industry standard;

- Added representation of non-cabinet Executive Branch agencies to the membership of an IS steering committee or advisory board; and

- Added a requirement that project determinations be made by the KISO within 30 days when practicable.

According to the revised fiscal note prepared by the Division of the Budget on the bill, as introduced, enactment of the bill would have a fiscal impact on various agencies, as follows:

- Kansas Department for Aging and Disability Services indicates the bill would cost the agency $1.6 million annually, including $1.3 million from the State General Fund (SGF);

- Kansas Department for Children and Families indicates the bill would require additional expenditures of $1.7 million annually, including $1.0 million from the SGF;

- Kansas Department of Health and Environment indicates the bill would result in costs around $1.3 million;

- Kansas Department of Corrections estimates the fiscal effect of the bill could result in costs of $5.7 million per year;

- Kansas Highway Patrol estimates the bill could result in annual expenditures of $574,700 to $616,000;

- Kansas Bureau of Investigation estimates the bill could result in additional fingerprint and background checks performed by the agency, thus increasing revenue; however, the fiscal effect cannot be determined because the number of individuals required to submit to such checks is unknown;

- Kansas Department of Agriculture estimates the bill could cost the agency up to $280,000 a year;

- Kansas Department of Transportation estimates the bill would require $1.7 million in additional expenditures per year, and would require the expenditure limitation on its agency operations account to be increased by $1.7 million; and

- The Kansas Association of Counties indicates there would be costs associated with obtaining employee fingerprints, and the League of Kansas Municipalities indicates there would be costs associated with paying a cybersecurity service rate. However, the fiscal effect for local governments is unknown (local units of government were removed from the provisions of the Act in the substitute bill).

Any fiscal effect associated with enactment of the original bill is not reflected in *The FY 2019 Governor's Budget Report*.

A fiscal note on the substitute bill was not available at the time the House Committee recommended it favorably for passage.