Session of 2018

Substitute for HOUSE BILL No. 2560

By Committee on Government, Technology and Security

2-14

AN ACT concerning information systems and communications; creating the Kansas cybersecurity act; establishing the Kansas information security office; establishing the cybersecurity state fund.

Be it enacted by the Legislature of the State of Kansas:

Section 1. Sections 1 through 15, and amendments thereto, shall be known and may be cited as the Kansas cybersecurity act.

Sec. 2. As used in sections 1 through 15, and amendments thereto:

(a) "Act" means the Kansas cybersecurity act.

(b) "Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the agency's business and is not subject to further unauthorized use.

(c) "CISO" means the executive branch chief information security officer.

(d) "Cybersecurity" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

(e) "Cybersecurity positions" do not include information technology positions within executive branch agencies.

(f) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(g) "Executive branch agency" means any agency in the executive branch of the state of Kansas, but does not include elected office agencies, the Kansas public employees retirement system, regents' institutions, or the board of regents.

(h) "KISO" means the Kansas information security office.

(i) (1) "Personal information" means:

(A) An individual's first name or first initial and last name, in combination with at least one of the following data elements for that individual:

(i) Social security number;

(ii) driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity;

(iii) financial account number or credit or debit card number, in combination with any security code, access code or password that is necessary to permit access to an individual's financial account;

(iv) any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional; or

(v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or

(B) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(2) "Personal information" does not include information:

(A) About an individual that has been made publicly available by a federal agency, state agency or municipality; or

(B) that is encrypted, secured or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(k) "State network resources" means any transmission, emission or reception of data of any kind containing communications of any nature, by wire, radio, optical or other electromagnetic means, including all facilities, equipment, supplies and services for such transmission, emission or reception that is owned, operated or managed by the state of Kansas.

Sec. 3. (a) There is hereby established the position of executive branch chief information security officer. The CISO shall be in the unclassified service under the Kansas civil service act, shall be appointed by the governor and shall receive compensation in an amount fixed by the governor.

(b) The CISO shall:

(1) Report to the executive branch chief information technology officer;

(2) serve as the state's CISO;

(3) serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance and technologies impacting executive branch cybersecurity programs;

(4) ensure cybersecurity training programs are provided for the executive branch;

(5) ensure technology resources assigned or provided to executive branch agencies are in compliance with applicable laws and rules and regulations and the national institute of standards technology cybersecurity framework or equivalent industry standard;

(6) ensure personnel resources assigned or provided to executive branch agencies report to the agency's appropriate executive leadership;

(7) coordinate cybersecurity efforts among executive branch agencies at the state and municipality level and private vendors;

(8) provide an annual report on the economic impact of cybersecurity insurance as a mitigation measure for data breach or unauthorized disclosure of personal information to the house government, technology and security committee, or its successor committee;

(9) have authority to:

(A) Oversee and approve executive branch cybersecurity plans for information technology projects;

(B) halt executive branch information technology projects or information systems that are not compliant with approved cybersecurity plans;

(C) conduct ad hoc security assessments of executive branch information systems and internal information technology operating environments;

(D) suspend public access to executive branch information resources when compromise of personal information or computer resources has occurred or is likely to occur as the result of an identified high-risk vulnerability or threat; and

(E) hire, promote, suspend, demote, discipline and dismiss executive branch cybersecurity positions; and

(10) perform such other functions and duties as provided by law and as directed by the executive chief information technology officer.

Sec. 4. (a) There is hereby established the Kansas information security office. The Kansas information security office shall be administered by the CISO and be staffed appropriately to effect the provisions of the Kansas cybersecurity act.

(b) For the purpose of preparing the governor's budget report and related legislative measures submitted to the legislature, the Kansas information security office, established in this section, shall be considered a separate state agency and shall be titled for such purpose as the "Kansas information security office." The budget estimates and requests of such office shall be presented as from a state agency separate from the department of administration, and such separation shall be maintained in the budget documents and reports prepared by the director of the budget and the governor, or either of them, including all related legislative reports and measures submitted to the legislature.

(c) Under direction of the CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) assist the executive branch in developing, implementing and monitoring strategic and comprehensive information security risk-

management programs;

(3) provide the executive branch strategic risk guidance for information technology projects, including the evaluation and recommendation of technical controls;

(4) facilitate the executive branch information security governance, including the formation of an information security steering committee or advisory board, which shall include representation from cabinet and non-cabinet agencies of the executive branch;

(5) create and manage a unified and flexible control framework to integrate and normalize requirements resulting from global laws, standards and regulations;

(6) ensure that security programs and technology solutions offered by vendors to the state are in compliance with relevant laws, rules and regulations and policies;

(7) provide the executive branch contract provisions with information security language for compliance requirements to expedite review of contracts for security programs and technology solutions;

(8) facilitate a metrics, logging and reporting framework to measure the efficiency and effectiveness of state information security programs;

(9) coordinate the use of external resources involved in information security programs, including, but not limited to, interviewing and negotiating contracts and fees;

(10) liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

(11) assist in the development of effective disaster recovery policies and standards;

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

(13) coordinate information technology security interests among governmental entities at the municipality and state levels; and

(14) perform such other functions and duties as provided by law and as directed by the CISO.

Sec. 5. The executive branch agency heads shall:

(a) Be solely responsible for security of all data and information technology resources under such agency's purview, irrespective of the location of the data or resources. Locations of data may include: (1) Agency sites; (2) agency real property; (3) infrastructure in state data centers; (4) third-party locations; and (5) in transit between locations;

(b) ensure that an agency-wide information security program is in place;

(c) designate an information security officer to administer the agency's information security program that reports directly to executive leadership;

(d) participate in CISO-sponsored statewide cybersecurity program initiatives and services;

(e) implement policies and standards to ensure that all the agency's data and information technology resources are maintained in compliance with applicable state and federal laws and rules and regulations and the national institute of standards technology cybersecurity framework or equivalent industry standard;

(f) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;

(g) include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;

(h) (1) 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 a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or the data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure or inappropriate use;

(2) ensure that the agency conducts annual internal assessments of its security program. Internal assessment results shall be considered confidential and shall not be subject to discovery by or release to any person or agency outside of the KISO or CISO. This provision regarding confidentiality shall expire on July 1, 2023, unless the legislature reviews and reenacts such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023; and

(3) prepare or have prepared a summary of the cybersecurity assessment report required in paragraph (1), excluding information that might put the data or information resources of the agency or its contractors at risk. Such report shall be made available to the public upon request;

(i) participate in annual agency leadership training to ensure understanding of: (1) The information and information systems that support the operations and assets of the agency; (2) the potential impact of common types of cyberattacks and data breaches on the agency's operations and assets; (3) how cyberattacks and data breaches on the agency's operations and assets could impact the operations and assets of other governmental entities on the state enterprise network; (4) how cyberattacks and data breaches occur; (5) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and (6) the annual reporting requirements required of the executive director or agency head; and

(j) ensure that if an agency owns, licenses or maintains computerized data that includes personal information, confidential information or information, the disclosure of which is regulated by law, such agency shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) Comply with the notification requirements set out in K.S.A. 2017 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal laws and rules and regulations, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: (A) The CISO; and (B) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

Sec. 6. (a) All executive branch agencies connecting to state network resources shall demonstrate cybersecurity effectiveness by validating both technical and non-technical cybersecurity controls that constitute information security programs. Validation reports of these controls shall be provided to the CISO biennially. Reports provided to the CISO shall:

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

(2) include an itemized list of all cybersecurity expenditures through accounts payable reports;

(3) include the positions, qualifications and duties of all cybersecurity staff through personnel records or equivalent information when third parties are used; and

(4) demonstrate the agency's ability to secure the information of Kansas citizens and businesses.

(b) (1) Cybersecurity plans shall be reviewed and approved by agency heads annually.

(2) The CISO shall review an agency's validation reports and cybersecurity plans to make recommendations to respective executive directors or agency heads and the governor.

(c) An agency shall not be disconnected from state network resources unless the CISO determines the existence of an imminent, critical threat. If such a threat is identified, the CISO may temporarily disconnect such agency from the state network until the identified threat is removed.

(d) The CISO shall establish and distribute the validation requirements to applicable executive branch agencies and private entities no later than October 1, 2018. The first validation requirement shall be completed by such entities prior to July 1, 2020.

Sec. 7. (a) Executive branch agencies shall adopt and implement a policy to protect the privacy of individuals or businesses by preserving the confidentiality of information processed by their websites or applications. Each agency shall submit such policy to the CISO for review and recommendation.

(b) Before deploying an internet website or mobile application that processes confidential or personal information:

(1) The developer of the website or application shall submit to the executive branch agency's security officer the information required under policies adopted by the agency. The agency's policies shall require the developer to submit for approval a detailed security plan that addresses at a minimum: (A) The architecture of the website or application; (B) the authentication mechanism for the website or application; (C) logging strategy that addresses specific data elements to be recorded; (D) security of data in transit; (E) security of data at rest; and (F) the administrator level access to data included in the website or application; and

(2) the executive branch agencies shall subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

Sec. 8. (a) An executive director or agency head, with input from the CISO, may require employees or contractors of executive branch agencies, 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.

(b) The fingerprints shall be used to identify the employee and to determine whether the employee or other such person has a record of criminal history in this state or another jurisdiction. The executive director or agency head shall submit the fingerprints to the Kansas bureau of investigation and the federal bureau of investigation for a state and national criminal history record check. The executive director or agency head may use the information obtained from fingerprinting and the criminal history record check for purposes of verifying the identity of the employee or other such person and in the official determination of the qualifications and fitness of the employee or other such person to work in the position with access to personal information.

(c) Local and state law enforcement officers and agencies shall assist the executive director or agency head in the taking and processing of fingerprints of employees or other such persons. Local law enforcement officers and agencies may charge a fee as reimbursement for expenses incurred in taking and processing fingerprints under this section, to be paid by the governmental agency employing or contracting the individual required to submit to fingerprinting and a criminal history record check.

Sec. 9. Information collected to effectuate this act shall be considered confidential by the executive branch agency and KISO unless all data elements or information that specifically identifies a target, vulnerability or weakness that would place the organization at risk have been redacted, including: (a) System information logs; (b) vulnerability reports; (c) risk assessment reports; (d) system security plans; (e) detailed system design plans; (f) network or system diagrams; and (g) audit reports. The provisions of this section shall expire on July 1, 2023, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023.

Sec. 10. (a) There is hereby established in the state treasury the cybersecurity state fund, which shall be administered by the CISO. All expenditures from the cybersecurity state fund shall be made in accordance with appropriation acts upon warrants of the director of accounts and reports issued pursuant to vouchers approved by the CISO or the designee of the CISO. All moneys received pursuant to the provisions of the Kansas cybersecurity act shall be deposited in the state treasury in accordance with the provisions of K.S.A. 75-4215, and amendments thereto, and shall be credited to the cybersecurity state fund.

(b) All moneys received by the cybersecurity state fund shall be used only for necessary and reasonable costs incurred or to be incurred by the KISO for: (1) Implementation and delivery of cybersecurity services; (2) purchase, maintenance and license fees for cybersecurity and supporting equipment and upgrades; (3) purchase, maintenance and license fees for cybersecurity and supporting software and upgrades; (4) training of personnel; (5) installation, service establishment, start-up charges and monthly recurring charges billed by service suppliers; (6) capital improvements and equipment or other physical enhancements to the cybersecurity program; (7) projects involving the development and implementation of cybersecurity services; (8) cybersecurity consolidation or cost-sharing projects; (9) delivery of cybersecurity services; (10) maintenance of adequate staffing, facilities and support services of the KISO; (11) projects involving the development and implementation of cybersecurity services for municipalities; (12) municipality consolidation or cost-sharing cybersecurity projects; (13) promotion of cybersecurity education; (14) development and implementation of a cybersecurity scholarship program; and (15) cybersecurity insurance.

Sec. 11. Appropriations may be made for capital outlay and other expenses to carry out the purposes of the KISO for the same period as is authorized by K.S.A. 46-155, and amendments thereto, for capital improvements. The CISO may enter into multiple-year lease or acquisition contracts, subject to state leasing and purchasing laws not in conflict with the foregoing authorization and so long as such contracts do not extend beyond the appropriation periods, limitations and restrictions therefor.

Sec. 12. The CISO may adopt rules and regulations providing for the administration of this act, including:

(a) Establishment of rates and charges for services performed by the KISO for any governmental entity. Such rates and charges shall be maintained by a cost system in accordance with generally accepted accounting principles. In determining cost rates for billing executive branch agencies, overhead expenses shall include, but not be limited to, light, heat, power, insurance, labor and depreciation. Billings shall include direct and indirect costs and shall be based on the foregoing cost accounting practices;

(b) determination of priorities for services performed by the KISO, including authority to decline new projects under specified conditions, with project determinations made within 30 days after receipt of a completed request for approval or review, when practicable;

(c) the manner of performance of any power or duty of the KISO;

(d) the execution of any business of such office and its relations to and business with other state agencies;

(e) appeals from the final decisions or final actions of the CISO; and

(f) policies for identification of information security vulnerabilities within entities, development of procedures with entities to address identified vulnerabilities and the assistance provided to entities to implement procedures to address vulnerabilities.

Sec. 13. (a) Under the supervision of the CISO, the KISO shall provide cybersecurity services for executive branch agencies, and shall make charges for such services pursuant to section 12, and amendments thereto. The furnishing of cybersecurity services by the KISO shall be a transaction to be settled in accordance with the provisions of K.S.A. 75-5516, and amendments thereto. All receipts for sales of services shall be deposited in the cybersecurity state fund.

(b) Except as otherwise provided by law and subject to the provisions of appropriation acts relating thereto, all fees and charges imposed by this act, provided or contracted for by the CISO, shall be deposited in the state treasury and credited to the cybersecurity state fund.

Sec. 14. Executive branch agencies may pay for cybersecurity services from existing budgets, from grants or other revenues, or through a special assessment to offset costs. Any executive branch agency's increase in fees or charges related to this act shall be used only for cybersecurity and no other purpose. Service or transactions with an applied cybersecurity cost recovery fee may indicate the portion of the fee dedicated to cybersecurity on all receipts and transaction records.

Sec. 15. Any entity or agency of the legislative or the judicial branch that is connecting to state network resources shall annually certify to the CISO that the entity or agency, in the opinion of such entity or agency, is maintaining substantial compliance with the national institute or standards technology cybersecurity framework or equivalent industry standard.

Sec. 16. This act shall take effect and be in force from and after its publication in the statute book.