Proposed Substitute to HB2560 - Amendment 2
February 9, 2018
Prepared by Jenna Moyer, Office of Revisor of Statutes

Substitute for HOUSE BILL NO. 2560

By Committee on Government, Technology and Security

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 the executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or 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 governmental entities

(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" means any governmental entity in the executive branch of the state of Kansas, but does not include elected office agencies, the Kansas public employees

businesses.

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

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

(c) An entity 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 an entity from the state network until the identified threat is removed.

(d) The CISO shall establish and distribute the validation requirements to each applicable governmental and non-governmental entity no later than October 1, 2018. The first validation requirement shall be completed by such agencies by July 1, 2020.

Sec. 7. (a) Governmental entities 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 entity 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 governmental entity's information security officer the information required under policies adopted by the entity. The entity'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 governmental entities shall subject the website or application to a vulnerability

(3) 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;

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

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

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

(7) 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;

(b) (1) To establish a base rate for effectuating the provisions of this act, there is hereby imposed a basic cybersecurity service rate for the executive branch:

(A) For fiscal year 2019, this rate shall not exceed $350 per employee connecting to the state network per year;

(B) for fiscal year 2020, this rate shall not exceed $360 per employee connecting to the state network per year; and

(C) for fiscal year 2021, this rate shall not exceed $400 per employee connecting to the state network per year.

(2) Network connection rates paid by non-executive branch governmental entities connecting to the state network shall remain unchanged until January 1, 2020, and shall not exceed the per employee network connection rates paid by the executive branch connecting to the state network.

(3) The house government, technology and security committee shall assess the adequacy of the basic cybersecurity rate beginning in 2022, and every two years thereafter. It shall be the duty of each entity to remit such moneys to the division of the budget as provided in section 13, and amendments thereto.

Sec. 13. (a) Under the supervision of the CISO, the KISO shall provide cybersecurity services for governmental entities, 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.

~~(c) The duty to collect payment imposed pursuant to this act shall commence on July 1, 2020.~~

(d) The basic cybersecurity service rate and the amounts required to be collected shall be due on October 1 of each year.

Sec. 14. (a) Governmental entities may pay for cybersecurity services from existing budgets, from grants or other revenues, or through a special assessment to offset costs associated with meeting cybersecurity service rates as specified in section 12, and amendments thereto.

(b) Any governmental entity's increase in fees or charges related to this act shall be used only for cybersecurity and no other purpose.

(c) Service or transactions with an applied cybersecurity cost recovery fee may indicate

(c) CISO shall not charge a municipality higher service rates than currently being charged until January 1, 2020, unless approved by the legislature. The CISO shall present the legislature with a proposed cybersecurity fee schedule by first day of the regular legislative session in 2019 for municipalities to access specific network resources.