

Substitute for HOUSE BILL NO. 2560

By Committee on Government, Technology and Security

Proposed Substitute to HB2560 - Amendment 1 February 9, 2018 Prepared by Jenna Moyer, Office of Revisor of Statutes

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

retirement system, regents' institutions, or the board of regents.

~~(h) "Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency or other instrumentality of the executive branch that acquires, maintains, stores or uses data in electronic form containing personal information, but does not include the Kansas public employees retirement system.~~

(and striking term 'governmental entity' or 'governmental entities' throughout remainder of bill)

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

(i) "Municipality" shall have the meaning ascribed to it in K.S.A. 75-6102, and amendments thereto.

(j) (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 health care 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

(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. (a) The CISO may adopt rules and regulations providing for the administration of this act, including:

(1) 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 governmental entities, 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;

~~(2) a fee structure for non-executive branch governmental entities connecting to the state network based on how many employees in each entity are connected to state network resources;~~

(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