Session of 2021

SENATE BILL No. 250

By Committee on Ways and Means

2-16

AN ACT concerning state agencies; requiring information technology security training; cybersecurity status reports; amending K.S.A. 75-7239, 75-7240 and 75-7242 and repealing the existing sections.

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

Section 1. K.S.A. 75-7239 is hereby amended to read as follows: 75-7239. (a) There is hereby established within and as a part of the office of information technology services 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~~ *office of information technology services*, 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) facilitate executive branch information security governance, including the consistent application of information security programs, plans and procedures;

(4) using standards adopted by the information technology executive council, create and manage a unified and flexible control framework to integrate and normalize requirements resulting from applicable state and federal laws, and rules and regulations;

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

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

(7) assist in the development of executive branch agency cybersecurity programs ~~that are in~~ *to ensure* compliance with applicable state and federal laws and rules and regulations and standards adopted by the information technology executive council;

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

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

(10) assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;

(11) assist executive branch agencies to create a framework for roles and responsibilities relating to information ownership, classification, accountability and protection;

(12) ensure a cybersecurity ~~training program is provided to executive branch agencies at no cost to the agencies~~ *awareness training program is made available to all branches of state government*; *and*

(13) ~~provide cybersecurity threat briefings to the information technology executive council;~~

~~(14) provide an annual status report of executive branch cybersecurity programs of executive branch agencies to the joint committee on information technology and the house committee on government, technology and security; and~~

~~(15)~~ perform such other functions and duties as provided by law and as directed by the CISO.

Sec. 2. K.S.A. 75-7240 is hereby amended to read as follows: 75-7240. *(a)* The executive branch agency heads shall:

~~(a)~~*(1)* 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)~~*(A)* Agency sites;

~~(2)~~*(B)* agency real property;

~~(3)~~*(C)* infrastructure in state data centers;

~~(4)~~*(D)* third-party locations; and

~~(5)~~*(E)* in transit between locations;

~~(b)~~*(2)* ensure that an agency-wide information security program is in place;

~~(c)~~*(3)* designate an information security officer to administer the agency's information security program that reports directly to executive

leadership;

~~(d)~~*(4)* participate in CISO-sponsored statewide cybersecurity program initiatives and services;

~~(e)~~*(5)* 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;

~~(f)~~*(6)* implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;

~~(g)~~*(7)* include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;

~~(h) (1)~~*(8) (A)* submit a cybersecurity *risk* assessment report to the ~~CISO~~ *joint committee on information technology and the joint committee on Kansas security* 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)~~*(B)* 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~~ *without authorization from the executive branch agency director or head*. 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)~~*(C)* prepare or have prepared a ~~summary~~ *financial summary identifying cybersecurity expenditures addressing the findings* of the cybersecurity ~~assessment~~ *self-assessment* report required in paragraph ~~(1)~~ *(8)(A)*, excluding information that might put the data or information resources of the agency or its contractors at risk and submit such report to the house of representatives committee on ~~government, technology and security or its successor committee~~ *appropriations* and the senate committee on ways and means;

~~(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)~~*(9)* 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)~~*(A)* Comply with the notification requirements set out in K.S.A. 2020 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)~~*(B)* not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: ~~(A)~~*(i)* The CISO; and ~~(B)~~*(ii)* if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

(b) The director or head of all state agencies shall:

(1) Participate in annual agency leadership training to ensure understanding of:

(A) The potential impact of common types of cyberattacks and data breaches on the agency's operations and assets;

(B) how cyberattacks and data breaches on the agency's operations and assets may impact the operations and assets of other governmental entities on the state enterprise network;

(C) how cyberattacks and data breaches occur; and

(D) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems;

(2) ensure that all information technology login credentials are disabled the same day that any employee ends their employment with the state; and

(3) require that all employees with access to information technology receive a minimum of one hour of information technology security training per year.

Sec. 3. K.S.A. 75-7242 is hereby amended to read as follows: 75-7242. Information collected to effectuate this act shall be considered confidential by ~~the executive branch agency and KISO~~ *all state and local government organizations* 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. 4. K.S.A. 75-7239, 75-7240 and 75-7242 are hereby repealed.

Sec. 5. This act shall take effect and be in force from and after its publication in the statute book.