

House Substitute for SENATE BILL No. 56

By Committee on Government, Technology and Security

3-22

1 AN ACT concerning information systems and communications; creating
2 the Kansas cybersecurity act; establishing the Kansas information
3 security office; relating to executive branch agencies; membership of
4 the information technology executive council; amending K.S.A. 2017
5 Supp. 75-7202 and repealing the existing section.

6
7 *Be it enacted by the Legislature of the State of Kansas:*

8 New Section 1. Sections 1 through 8, and amendments thereto, shall
9 be known and may be cited as the Kansas cybersecurity act.

10 New Sec. 2. As used in sections 1 through 8, and amendments
11 thereto:

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

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

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

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

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

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

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

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

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

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

1 individual:

2 (i) Social security number;

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

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

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

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

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

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

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

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

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

29 (b) The CISO shall:

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

32 (2) serve as the state's CISO;

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

36 (4) ensure Kansas information security office resources assigned or
37 provided to executive branch agencies are in compliance with applicable
38 laws and rules and regulations;

39 (5) coordinate cybersecurity efforts between executive branch
40 agencies;

41 (6) provide guidance to executive branch agencies when compromise
42 of personal information or computer resources has occurred or is likely to
43 occur as the result of an identified high-risk vulnerability or threat; and

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

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

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

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

18 (1) Administer the Kansas cybersecurity act;

19 (2) assist the executive branch in developing, implementing and
20 monitoring strategic and comprehensive information security risk-
21 management programs;

22 (3) facilitate executive branch information security governance,
23 including the consistent application of information security programs,
24 plans and procedures;

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

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

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

34 (7) assist in the development of executive branch agency
35 cybersecurity programs that are in compliance with applicable state and
36 federal laws and rules and regulations and standards adopted by the
37 information technology executive council;

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

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

43 (10) assist in the development of plans and procedures to manage and

- 1 recover business-critical services in the event of a cyberattack or other
2 disaster;
- 3 (11) assist executive branch agencies to create a framework for roles
4 and responsibilities relating to information ownership, classification,
5 accountability and protection;
- 6 (12) ensure a cybersecurity training program is provided to executive
7 branch agencies;
- 8 (13) provide cybersecurity threat briefings to the information
9 technology executive council;
- 10 (14) provide an annual status report of executive branch cybersecurity
11 programs of executive branch agencies to the joint committee on
12 information technology and the house committee on government,
13 technology and security; and
- 14 (15) perform such other functions and duties as provided by law and
15 as directed by the CISO.
- 16 New Sec. 5. The executive branch agency heads shall:
- 17 (a) Be solely responsible for security of all data and information
18 technology resources under such agency's purview, irrespective of the
19 location of the data or resources. Locations of data may include: (1)
20 Agency sites; (2) agency real property; (3) infrastructure in state data
21 centers; (4) third-party locations; and (5) in transit between locations;
- 22 (b) ensure that an agency-wide information security program is in
23 place;
- 24 (c) designate an information security officer to administer the
25 agency's information security program that reports directly to executive
26 leadership;
- 27 (d) participate in CISO-sponsored statewide cybersecurity program
28 initiatives and services;
- 29 (e) implement policies and standards to ensure that all the agency's
30 data and information technology resources are maintained in compliance
31 with applicable state and federal laws and rules and regulations;
- 32 (f) implement appropriate cost-effective safeguards to reduce,
33 eliminate or recover from identified threats to data and information
34 technology resources;
- 35 (g) include all appropriate cybersecurity requirements in the agency's
36 request for proposal specifications for procuring data and information
37 technology systems and services;
- 38 (h) (1) submit a cybersecurity assessment report to the CISO by
39 October 16 of each even-numbered year, including an executive summary
40 of the findings, that assesses the extent to which a computer, a computer
41 program, a computer network, a computer system, a printer, an interface to
42 a computer system, including mobile and peripheral devices, computer
43 software, or the data processing of the agency or of a contractor of the

1 agency is vulnerable to unauthorized access or harm, including the extent
2 to which the agency's or contractor's electronically stored information is
3 vulnerable to alteration, damage, erasure or inappropriate use;

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

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

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

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

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

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

39 New Sec. 6. (a) An executive branch agency head, with input from
40 the CISO, may require employees or contractors of executive branch
41 agencies, whose duties include collection, maintenance or access to
42 personal information, to be fingerprinted and to submit to a state and
43 national criminal history record check at least every five years.

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

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

19 New Sec. 7. Information collected to effectuate this act shall be
20 considered confidential by the executive branch agency and KISO unless
21 all data elements or information that specifically identifies a target,
22 vulnerability or weakness that would place the organization at risk have
23 been redacted, including: (a) System information logs; (b) vulnerability
24 reports; (c) risk assessment reports; (d) system security plans; (e) detailed
25 system design plans; (f) network or system diagrams; and (g) audit reports.
26 The provisions of this section shall expire on July 1, 2023, unless the
27 legislature reviews and reenacts this provision pursuant to K.S.A. 45-229,
28 and amendments thereto, prior to July 1, 2023.

29 New Sec. 8. Executive branch agencies may pay for cybersecurity
30 services from existing budgets, from grants or other revenues, or through a
31 special assessment to offset costs. Any executive branch agency's increase
32 in fees or charges related to this act shall be used only for cybersecurity
33 and no other purpose. Service or transactions with an applied cybersecurity
34 cost recovery fee may indicate the portion of the fee dedicated to
35 cybersecurity on all receipts and transaction records.

36 Sec. 9. K.S.A. 2017 Supp. 75-7202 is hereby amended to read as
37 follows: 75-7202. (a) There is hereby established the information
38 technology executive council which shall be attached to the office of
39 information technology services for purposes of administrative functions.

40 (b) The council shall be composed of ~~17~~ 15 voting members as
41 follows: ~~The secretary of administration;~~ Two cabinet agency heads *or*
42 *such persons' designees;* ~~one two~~ noncabinet agency ~~head heads or such~~
43 *persons' designees;* ~~the director of the budget;~~ the executive chief

1 information technology officer; the legislative chief information
2 technology officer; the judicial chief information technology officer ~~and~~
3 ~~the judicial administrator of the Kansas supreme court; the executive~~
4 ~~director of the Kansas board of regents; the commissioner of education;~~
5 ~~two representatives~~ *the chief executive officer of the state board of regents*
6 *or such person's designee; one representative of cities; two representatives*
7 *one representative of counties; the network manager of the information*
8 *network of Kansas (INK); and one representative from the private sector*
9 ~~who is a chief executive officer or chief information technology officer~~
10 *one representative appointed by the Kansas criminal justice information*
11 *system committee; one member of the joint committee on information*
12 *technology appointed by the president of the senate; one member of the*
13 *joint committee on information technology appointed by the minority*
14 *leader of the senate; one member of the house government, technology*
15 *and security committee appointed by the speaker of the house of*
16 *representatives; and one member of the house government, technology and*
17 *security committee appointed by the minority leader of the house of*
18 *representatives. The chief information technology architect shall be a*
19 *nonvoting member of the council. The two cabinet agency heads, the*
20 *noncabinet agency head heads, the representatives representative of cities;*
21 ~~and the representatives representative of counties and the representative~~
22 ~~from the private sector shall be appointed by the governor for a term not to~~
23 ~~exceed 18 months. Upon expiration of an appointed member's term, the~~
24 ~~member shall continue to hold office until the appointment of a successor.~~
25 Nonappointed members shall serve ex officio.

26 (c) The chairperson of the council shall be drawn from the chief
27 information technology officers, with each chief information technology
28 officer serving a one-year term. The term of chairperson shall rotate
29 among the chief information technology officers on an annual basis.

30 (d) The council shall hold *quarterly* meetings and hearings in the city
31 of Topeka or at such other places as the council designates, on call of the
32 chairperson or on request of four or more members.

33 (e) *Except for members specified as a designee in subsection (b),*
34 *members of the council may not appoint an individual to represent them*
35 *on the council and only members of the council may vote.*

36 (f) Members of the council shall receive mileage, tolls and parking as
37 provided in K.S.A. 75-3223, and amendments thereto, for attendance at
38 any meeting of the council or any subcommittee meeting authorized by the
39 council.

40 Sec. 10. K.S.A. 2017 Supp. 75-7202 is hereby repealed.

41 Sec. 11. This act shall take effect and be in force from and after its
42 publication in the statute book.