

HOUSE BILL No. 2560

By Committee on Government, Technology and Security

1-26

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

4
5 *Be it enacted by the Legislature of the State of Kansas:*

6 Section 1. Sections 1 through 14, and amendments thereto, shall be
7 known and may be cited as the Kansas cybersecurity act.

8 Sec. 2. As used in sections 1 through 14, and amendments thereto:

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

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

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

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

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

24 (f) "Executive branch agency" means any agency in the executive
25 branch of the state of Kansas, but does not include elected office agencies,
26 regents' institutions, or the board of regents.

27 (g) "Governmental entity" means any department, division, bureau,
28 commission, regional planning agency, board, district, authority, agency or
29 other instrumentality of this state that acquires, maintains, stores or uses
30 data in electronic form containing personal information.

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

32 (i) "Municipality" shall have the meaning ascribed to it in K.S.A. 75-
33 6102, and amendments thereto.

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

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

34 (b) The CISO shall:

35 (1) Report to the governor;

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

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

40 (4) ensure cybersecurity training programs are provided for executive
41 branch agencies;

42 (5) ensure technology resources assigned or provided to
43 governmental entities are in compliance with applicable laws and rules and

1 regulations;

2 (6) ensure personnel resources assigned or provided to governmental
3 entities report to the entity's appropriate executive leadership;

4 (7) coordinate cybersecurity efforts among governmental entities at
5 the state and municipality level and private vendors;

6 (8) have authority to:

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

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

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

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

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

21 (9) perform such other functions and duties as provided by law and as
22 directed by the executive chief information technology officer or the
23 governor.

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

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

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

39 (1) Administer the Kansas cybersecurity act;

40 (2) assist executive branch agencies in developing, implementing and
41 monitoring strategic and comprehensive information security risk-
42 management programs;

43 (3) provide executive branch agencies strategic risk guidance for

1 information technology projects, including the evaluation and
2 recommendation of technical controls;

3 (4) facilitate executive branch agencies information security
4 governance, including the formation of an information security steering
5 committee or advisory board;

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

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

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

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

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

19 (10) assist in the development of effective disaster recovery policies
20 and standards;

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

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

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

28 Sec. 5. (a) The executive director or agency head of any
29 governmental entity connecting to state network resources shall:

30 (1) Be solely responsible for security of all data and information
31 technology resources under such entity's purview, irrespective of the
32 location of the data or resources. Locations of data may include: (A) Entity
33 sites; (B) entity real property; (C) infrastructure in state data centers; (D)
34 third-party locations; and (E) in transit between locations;

35 (2) ensure that an entity-wide information security program is in
36 place;

37 (3) designate an information security officer to administer the entity's
38 information security program that reports directly to executive leadership;

39 (4) participate in CISO-sponsored statewide cybersecurity program
40 initiatives and services;

41 (5) implement policies and standards to ensure that all the entity's
42 data and information technology resources are maintained in compliance
43 with applicable state and federal laws and rules and regulations;

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

4 (7) include all appropriate cybersecurity requirements in the entity's
5 request for proposal specifications for procuring data and information
6 technology systems and services;

7 (8) (A) submit a cybersecurity assessment report to the CISO by
8 October 16 of each even-numbered year, including an executive summary
9 of the findings, that assesses the extent to which a computer, a computer
10 program, a computer network, a computer system, a printer, an interface to
11 a computer system, including mobile and peripheral devices, computer
12 software, or the data processing of the entity or of a contractor of the entity
13 is vulnerable to unauthorized access or harm, including the extent to which
14 the entity's or contractor's electronically stored information is vulnerable to
15 alteration, damage, erasure or inappropriate use;

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

23 (C) prepare or have prepared a summary of the cybersecurity
24 assessment report required in subparagraph (A), excluding information
25 that might put the data or information resources of the entity or its
26 contractors at risk. Such report shall be made available to the public upon
27 request;

28 (9) participate in annual executive director or agency head
29 cybersecurity training to ensure understanding of: (A) The information and
30 information systems that support the operations and assets of the entity;
31 (B) the potential impact of common types of cyberattacks and data
32 breaches on the entity's operations and assets; (C) how cyberattacks and
33 data breaches on the entity's operations and assets could impact the
34 operations and assets of other governmental entities on the state enterprise
35 network; (D) how cyberattacks and data breaches occur; (E) steps to be
36 undertaken by the executive director or agency head and entity employees
37 to protect their information and information systems; and (F) the annual
38 reporting requirements required of the executive director or agency head;
39 and

40 (10) ensure that if an entity owns, licenses or maintains computerized
41 data that includes personal information, confidential information or
42 information, the disclosure of which is regulated by law, shall, in the event
43 of a breach or suspected breach of system security or an unauthorized

1 exposure of that information:

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

6 (B) not later than 48 hours after the discovery of the breach, suspected
7 breach or unauthorized exposure, notify: (i) The CISO; and (ii) if the
8 breach, suspected breach or unauthorized exposure involves election data,
9 the secretary of state.

10 Sec. 6. (a) All governmental entities or non-governmental entities
11 connecting to state network resources, shall demonstrate cybersecurity
12 effectiveness by validating both technical and non-technical cybersecurity
13 controls that constitute information security programs. Validation reports
14 of these controls shall be provided to the CISO biennially. Reports
15 provided to the CISO shall:

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

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

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

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

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

28 (c) The CISO shall review all results and make recommendations to
29 respective executive directors or agency heads and the governor. If the
30 CISO determines that an entity is unable to meet compliance standards, the
31 entity shall be disconnected from state network resources, unless the CISO
32 determines that the entity is working in good faith to comply. Entities may
33 appeal such decision to the governor.

34 Sec. 7. (a) Governmental entities shall adopt and implement a policy
35 to protect the privacy of individuals or businesses by preserving the
36 confidentiality of information processed by their websites or applications.
37 Each entity shall submit such policy to the CISO for review and
38 recommendation.

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

41 (1) The developer of the website or application shall submit to the
42 governmental entity's information security officer the information required
43 under policies adopted by the entity. The entity's policies shall require the

1 developer to submit for approval a detailed security plan that addresses at
2 a minimum: (A) The architecture of the website or application; (B) the
3 authentication mechanism for the website or application; (C) logging
4 strategy that addresses specific data elements to be recorded; (D) security
5 of data in transit; (E) security of data at rest; and (F) the administrator
6 level access to data included in the website or application; and

7 (2) the governmental entities shall subject the website or application
8 to a vulnerability and penetration test conducted internally or by an
9 independent third party.

10 Sec. 8. (a) The CISO may require employees or contractors of
11 governmental entities whose duties include collection, maintenance or
12 access to personal information to be fingerprinted and to submit to a state
13 and national criminal history record check at least every five years.

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

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

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

42 Sec. 10. (a) There is hereby established in the state treasury the
43 cybersecurity state fund, which shall be administered by the CISO. All

1 expenditures from the cybersecurity state fund shall be made in
2 accordance with appropriation acts upon warrants of the director of
3 accounts and reports issued pursuant to vouchers approved by the CISO or
4 the designee of the CISO. All moneys received pursuant to the provisions
5 of the Kansas cybersecurity act shall be deposited in the state treasury in
6 accordance with the provisions of K.S.A. 75-4215, and amendments
7 thereto, and shall be credited to the cybersecurity state fund.

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

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

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

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

43 (2) determination of priorities for services performed by the KISO,

1 including authority to decline new projects under specified conditions;

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

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

5 (5) appeals from the final decisions or final actions of the CISO.

6 (b) To establish a base rate for effectuating the provisions of this act,
7 there is hereby imposed a basic cybersecurity service rate per year per
8 employee for all governmental and non-governmental entities connecting
9 to state network resources. This rate shall not exceed \$700 per employee
10 per year. The house government, technology and security committee shall
11 assess the adequacy of the basic cybersecurity rate beginning in 2022, and
12 every two years thereafter. It shall be the duty of each entity to remit such
13 moneys to the division of the budget as provided in section 13, and
14 amendments thereto.

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

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

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

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

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

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

36 (c) Service or transactions with an applied cybersecurity cost
37 recovery fee may indicate the portion of the fee dedicated to cybersecurity
38 on all receipts and transaction records.

39 Sec. 15. This act shall take effect and be in force from and after its
40 publication in the statute book.