*Session of 2026*

# SENATE BILL No. 453

By Senator Bowser

2-3

AN ACT concerning infrastructure; enacting the Kansas critical infrastructure protection act; prohibiting access to state critical infrastructure by countries of concern; prohibiting the acquisition of critical software and other technology used in state infrastructure from countries of concern.

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

Section 1. (a) Sections 1 through 9, and amendments thereto, shall be known and may be cited as the Kansas critical infrastructure protection act.

(b) The purpose of this act is to protect state critical infrastructure, including software and other technology, by prohibiting countries of concern from accessing state critical infrastructure and prohibiting the acquisition of critical components of such critical infrastructure, including software, routers, cameras and laser sensor technology, from countries of concern or any foreign principal of a country of concern.

Sec. 2. As used in sections 1 through 9, and amendments thereto:

(a) "Adjutant general" means the adjutant general of the state of Kansas.

(b) "Company" means any:

(1) For-profit corporation, partnership, limited partnership, limited liability partnership, limited liability company, joint venture, trust, association, sole proprietorship or other organization, including any:

(A) Subsidiary of such company, a majority ownership interest of which is held by such company;

(B) parent company that holds a majority ownership interest of such company; and

(C) other affiliate or business association of such company whose primary purpose is to make a profit; or

(2) nonprofit organization.

(c) (1) "Country of concern" means the following:

(A) People's republic of China, including the Hong Kong special administrative region;

(B) republic of Cuba;

(C) islamic republic of Iran;

(D) democratic people's republic of Korea;

(E) Russian federation; and

(F) Bolivarian republic of Venezuela.

(2) "Country of concern" does not include the republic of China (Taiwan).

(d) "Critical infrastructure" means any privately or publicly owned systems or assets, whether physical or virtual, that are vital to the state of Kansas or the United States, such that the incapacity or destruction of such systems or assets would have a debilitating impact on state or national security, economic security, public health or any combination thereof. "Critical infrastructure" includes, but is not limited to:

(1) Any facility described in K.S.A. 21-5818, and amendments thereto; and

(2) personal data or otherwise classified information storage systems, including cybersecurity of such storage systems.

(e) "Critical component" means those components or subcomponents that are:

(1) Distinct and serviceable articles; and

(2) the primary component or subcomponent of an identifiable process or subprocess necessary to the proper functioning of the infrastructure or equipment.

(f) "Cybersecurity" means any measures taken to protect a computer, computer network, computer system or other technology infrastructure against unauthorized use or access.

(g) "Domicile" means the country where:

(1) A company is organized;

(2) a company completes a substantial portion of its business; or

(3) a majority of a company's ownership interest is held.

(h) "Foreign entity" means any company whose domicile is any country other than the United States.

(i) "Foreign principal" means:

(1) The government or any official of the government of a country of concern;

(2) any political party, subdivision thereof or any member of a political party of a country of concern;

(3) any corporation, partnership, association, organization or other combination of persons organized under the laws of or having its principal place of business in a country of concern. "Foreign principal" includes any subsidiary owned or wholly controlled by any such entity;

(4) any agent of or any entity otherwise under the control of a country of concern; or

(5) any individual whose residence is in a country of concern and who is not a citizen or lawful permanent resident of the United States; or

(6) any individual, entity or combination thereof described in

paragraphs (1) through (5) that has a controlling interest in any company formed for the purpose of manufacturing, distributing, transporting or selling software, critical components for critical infrastructure or drones and related services and equipment.

(j) "Governmental agency" means the state or any political or taxing subdivision of the state or any office, agency or instrumentality thereof.

(k) "Software" means any program, routine or set of one or more programs or routines that are used or intended for use to cause one or more computers, computer-related pieces of equipment or any combination thereof to perform a task or set of tasks as it relates to state infrastructure.

Sec. 3. (a) Except as provided in subsection (c), in addition to the provisions of K.S.A. 75-3739, and amendments thereto, and any other applicable statutes concerning purchases, no governmental agency or company constructing, repairing, operating or otherwise having significant access to critical infrastructure in this state shall enter into any agreement with a foreign principal for the acquisition of services or critical components for such infrastructure if such agreement would allow such foreign principal to directly or remotely access or control such infrastructure.

(b) Any critical components for critical infrastructure that were acquired prior to July 1, 2026, may continue to be used by the governmental agency or company that acquired such critical component. Except as provided in subsection (c), when such governmental agency or company determines that such critical component must be replaced, the replacement component shall be acquired from a company that is domiciled in the United States and that certifies that such critical component was manufactured in the United States.

(c) Any acquisition that is otherwise prohibited under subsection (a) or (b) may be completed by a governmental agency or company if:

(1) There is no other reasonable means to acquire such services or critical components or of addressing the needs of such critical infrastructure necessitating such acquisition;

(2) the agreement for such acquisition is approved by the adjutant general; and

(3) failure to acquire such services or critical components or otherwise address the needs of such critical infrastructure would pose a greater threat to the safety and security of this state than that posed by entering into such acquisition agreement.

Sec. 4. (a) In order to access state critical infrastructure, a company shall submit an application for certification to the adjutant general along with the required certification fee. Such application shall be submitted in such form and manner as prescribed by the adjutant general.

(b) The adjutant general shall only certify a company to access state

critical infrastructure if such company:

(1) Identifies all employee positions in the organization that have access to state critical infrastructure;

(2) completes a national criminal history background check on each employee and each prospective employee prior to hiring such person that has or will have access to state critical infrastructure;

(3) prohibits foreign principals from a country of concern from accessing state critical infrastructure;

(4) discloses any ownership of, partnership with or control from any entity that is not domiciled within the United States;

(5) stores and processes all data generated by such state critical infrastructure on domestic servers;

(6) does not use cloud service providers or data centers that are domiciled outside of the United States;

(7) agrees to immediately report any cyberattack, security breach or suspicious activity to the adjutant general; and

(8) operates in compliance with section 3, and amendments thereto.

(c) If the adjutant general determines that a company is not in compliance with the requirements of this section, such company's certification shall be revoked.

(d) The amount of the certification fee shall be fixed by the adjutant general in an amount of not to exceed $150.

Sec. 5. (a) The adjutant general shall be notified by the owner of a critical infrastructure installation of any proposed sale or transfer of, or investment in, such critical infrastructure to an entity domiciled outside of the United States or any foreign principal.

(b) Within 30 days after receipt of any such notice, the adjutant general shall investigate the proposed sale, transfer or investment. If the adjutant general finds, within a reasonable suspicion, that such proposed sale, transfer or investment threatens state critical infrastructure security, economic security, public health or any combination thereof, the adjutant general may request that the attorney general, on behalf of the adjutant general, seek an injunction to enjoin such proposed sale, transfer or investment in a court of competent jurisdiction.

(c) (1) The adjutant general shall notify the owners and operators of state critical infrastructure of any known or suspected cyber threats, vulnerabilities or adversarial activities in a manner consistent with the goals of:

(A) Identifying and preventing similar action in similar critical infrastructure installations or processes; and

(B) maintaining operational security and normal functioning of such critical infrastructure.

(2) Any such notice shall protect the rights of the owners of such

critical infrastructure, including the extent to which trade secrets or other proprietary information is shared between entities, but only to the extent that such protection does not inhibit the ability of the adjutant general to effectively communicate the threat of known or suspected threats, vulnerabilities or adversarial activities.

Sec. 6. (a) No state infrastructure shall use or incorporate within its operating systems any software that is:

(1) Produced in any country of concern;

(2) produced or owned by any company whose software is subject to a ban imposed by federal law;

(3) produced or owned by any foreign principal; or

(4) subject to a ban imposed by federal law.

(b) On or before January 1, 2027, any software that is prohibited under subsection (a) shall be uninstalled or otherwise permanently disabled.

(c) No governmental agency shall knowingly enter into or renew any contract with a company that supplies a wireless internet router or modem system if such company is a foreign principal or such router or system is produced in a country of concern.

(d) Each owner or operator of state critical infrastructure shall certify to the adjutant general that such critical infrastructure does not use any wireless internet routers or modem systems produced by a foreign principal.

(e) The adjutant general shall create, maintain and update a public listing of prohibited wireless internet routers and modem system technologies for governmental agencies and owners and operators of critical infrastructure.

Sec. 7. (a) No governmental agency or owner or operator of state critical infrastructure shall knowingly enter into or renew a contract with a company for a school bus infraction detection system, speed detection system, traffic infraction detector or any other camera system used for enforcing traffic if such company is a foreign principal or such system is produced in a country of concern.

(b) No governmental agency shall knowingly enter into or renew a contract with a company for any light detection and ranging (LiDAR) technology if such company is a foreign principal or such technology is produced in a country of concern.

(c) The adjutant general shall create, maintain and update a public listing of prohibited traffic camera and LiDAR technologies for governmental agencies and owners and operators of critical infrastructure.

Sec. 8. The adjutant general shall adopt rules and regulations necessary to implement the provisions of sections 1 through 7, and amendments thereto.

Sec. 9. Sections 1 through 8, and amendments thereto, are declared severable. Any provision of sections 1 through 8, and amendments thereto, or the application thereof to any person or circumstance that is held to be unconstitutional or invalid shall not affect the validity of any remaining provisions of sections 1 through 8, and amendments thereto, or the applicability of such provisions to any person or circumstance.

Sec. 10. This act shall take effect and be in force from and after its publication in the statute book.