FIRST REGULAR SESSION

HOUSE BILL NO. 1231

103RD GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVE SIMMONS.

2618H.01I JOSEPH ENGLER, Chief Clerk

AN ACT

To amend chapter 1, RSMo, by adding thereto two new sections relating to the infrastructure security, with penalty provisions.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Chapter 1, RSMo, is amended by adding thereto two new sections, to be known as sections 1.1400 and 1.1410, to read as follows:

1.1400. 1. This section shall be known and may be cited as the "Missouri Critical Infrastructure Protection Act".

2. As used in this section, the following terms mean:

(1) "Company", a for-profit sole proprietorship, organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including a wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate of those entities or business associations that exists to make a profit; or a non-profit organization;

(2) "Critical infrastructure", systems and assets, whether physical or virtual, so vital to the state of Missouri or the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on state or national security, state or national economic security, or state or national public health. A critical infrastructure may be publicly or privately owned, and includes but is not limited to:

(a) Gas and oil production, storage, or delivery systems;

(b) Water supply, refinement, storage, or delivery systems;

(c) Telecommunications networks;

(d) Electrical power delivery systems;

EXPLANATION — Matter enclosed in bold-faced brackets **[**~~thus~~**]** in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

(e) Emergency services;

(f) Transportation systems and services; and

(g) Personal data or other classified information storage systems, including cybersecurity;

(3) "Cybersecurity", the measures taken to protect a computer, computer network, computer system, or other technology infrastructure against unauthorized use or access;

(4) "Domicile", either the country in which a company is registered, where the company's affairs are primarily completed, or where the majority of ownership share is held;

(5) "Foreign adversary", an individual or government identified as a foreign adversary in 15 CFR 7.4;

(6) "Foreign principal", any of the following:

(a) The government or any official of the government of a foreign adversary;

(b) A political party or member of a political party or any subdivision of a political party of a foreign adversary;

(c) A partnership, association, corporation, organization, or other combination of persons organized under the laws of or having its principal place of business in the country of a foreign adversary, or a subsidiary of such entity, or owned or controlled wholly or in part by any person, entity, or collection of persons or entities of a foreign adversary;

(d) Any person who is domiciled in the country of a foreign adversary and is not a citizen or lawful permanent resident of the United States; or

(e) Any person, entity, or collection of persons or entities, described in paragraphs (a) to (d) having a controlling interest in a partnership, association, corporation, organization, trust, or any other legal entity or subsidiary formed for the purpose of owning real property;

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

3. A company or other entity constructing, repairing, operating, or otherwise having significant access to critical infrastructure shall not enter into an agreement relating to critical infrastructure in this state with a foreign principal from the country of a foreign adversary if the agreement would allow the foreign principal from a foreign adversary country to directly or remotely access or control critical infrastructure in this state.

4. A governmental entity shall not enter into a contract or other agreement relating to critical infrastructure in this state with a company that is a foreign principal from a foreign adversary country if the agreement would allow the foreign principal from a foreign adversary country to directly or remotely access or control critical infrastructure in this state.

5. Notwithstanding subsections 3 and 4 of this section, an entity or governmental entity may enter into a contract or agreement relating to critical infrastructure with a foreign principal from a foreign adversary country or use products or services produced by a foreign principal from a foreign adversary country if:

(1) There is no other reasonable option for addressing the need relevant to state critical infrastructure;

(2) The contract is pre-approved by the department of public safety; and

(3) Not entering into such a contract or agreement would pose a greater threat to the state than the threat associated with entering into the contract.

6. Before accessing critical infrastructure, a company shall file a certification form with and pay a certification fee to the department of public safety. The department of public safety shall develop a form to fulfill the requirements of this subsection.

7. To maintain registration as a company with access to critical infrastructure, a company shall:

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

(2) Obtain from the department of public safety or private vendor, for each employee that will have access to critical infrastructure, a criminal background check and any other background information considered necessary by the company or required by the department of public safety to protect critical infrastructure from foreign adversary infiltration or interference;

(3) Prohibit foreign nationals from a foreign adversary nation from access to critical infrastructure;

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

(5) Store and process all data generated by such critical infrastructure on domestic servers;

(6) Not use cloud service providers or data centers that are foreign entities;

(7) Immediately report any cyber attack, security breach, or suspicious activity to the department of public safety; and

(8) Be compliant with subsections 3 to 5 of this section.

8. The department of public safety 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 an entity with any foreign adversary ownership.

9. The department of public safety shall have no more than thirty days following the notice to investigate the proposed sale, transfer, or investment. If the department of public safety reasonably believes that such proposed sale, transfer, or investment will threaten state critical infrastructure security, state economic security, state public health, or any combination of those matters, the attorney general, on behalf of the department of public safety, shall file a request for injunction opposing the proposed sale, transfer, or investment with the supreme court of Missouri.

10. If the supreme court finds that such sale, transfer, or investment poses a reasonable threat to state critical infrastructure security, state economic security, state or national public health, or any combination of those matters, the supreme court shall issue a denial of approval.

11. The department of public safety shall act to notify critical infrastructure entities of known or suspected cyber threats, vulnerabilities, and adversarial activities in order to:

(1) Identify and close similar exploits in similar critical infrastructure installation or processes, especially after being notified of activity under subdivision (7) of subsection 7 of this section;

(2) Maintain operation security and normal functioning of critical infrastructure; and

(3) Protect the rights of private critical infrastructure entities, including by reducing the extent to which trade secrets or other proprietary information is shared between entities, to the extent that such precaution does not inhibit the ability of the department of public safety to effectively communicate the threat of a known or suspected exploit or adversarial activity.

12. All software used in state infrastructure located within or serving this state shall not include any software produced by a company headquartered in and subject to the laws of a foreign adversary or a company under the direction or control of a foreign adversary. Any state infrastructure provider that removes, discontinues, or replaces any prohibited software shall not be required to obtain any additional permits from any state agency or political subdivision for the removal, discontinuance, or replacement of such software as long as the state agency or political subdivision is properly notified of the necessary replacements and the replacement software is similar to the existing software.

13. After August 28, 2025, a governmental entity or critical infrastructure provider shall not knowingly enter into or renew a contract with a vendor if:

(1) The contracting vendor is owned by the government of a foreign adversary;

(2) The government of a foreign adversary has a controlling interest in the contracting vendor; or

(3) The contracting vendor is selling a product produced by a government of a foreign adversary, a company primarily domiciled in the country of a foreign adversary, or a company owned or controlled by a company primarily domiciled in the country of a foreign adversary.

14. After August 28, 2025, a governmental entity or critical infrastructure provider shall not knowingly enter into or renew a contract with a vendor that is owned by the government of a foreign adversary, primarily domiciled within the country of a foreign adversary, owned or controlled by a company primarily domiciled in the country of a foreign adversary, or in which the government of a foreign adversary has a controlling interest for any of the following products or services:

(1) School bus infraction detection systems;

(2) Speed detection systems or traffic infraction detectors;

(3) Any camera system used for enforcing traffic laws;

(4) Video surveillance equipment or software technology;

(5) Light detection and ranging technology (LiDAR); and

(6) Wi-Fi routers or modem systems.

15. The department of public safety shall create a public listing of products and companies prohibited under subsection 14 of this section for governmental entities and critical infrastructure providers.

16. After August 28, 2025, each critical infrastructure provider in Missouri shall certify to the department of public safety that they are in compliance with section 14 of this section.

1.1410. 1. This section shall be known and may be cited as the "Missouri Secure Communications Act."

2. As used in this section, the following terms mean:

(1) "Communications provider" any corporation, public or private, that operates any system supporting the transmission of information of a user's choosing, regardless of the transmission medium or technology employed, that connections to a network permitting the end user to engage in communications including, but not limited to, service provided directly to the public or to such classes of users as to be effectively available directly to the public;

(2) "Critical communications infrastructure", all physical broadband infrastructure and equipment that supports the transmission of information of a user's choosing, regardless of the transmission medium or technology employed, that connects to a network that permits the end user to engage in communications including, but not limited to, service provided directly to the public or to such classes of users as to be effectively available to the public;

(3) "Federally banned corporation", any company or designated equipment banned by the Federal Communications Commission including, but not limited to, any equipment or service deemed to pose a threat to national security and identified on the covered list developed as required in 47 CFR Section 1.50002 and published by the Public Safety and Homeland Security Bureau of the Federal Communications Commission as required in 47 U.S.C. 1601 et seq.

3. All critical communications infrastructure located within or serving this state shall not include any equipment manufactured by a federally banned corporation.

4. All critical communications infrastructure in operation within or serving this state, including any critical communications infrastructure that is not permanently disabled, shall have all equipment prohibited by this section removed and replaced with equipment not prohibited by this section. Any communications provider that removes, discontinues, or replaces any prohibited communications equipment or service shall not be required to obtain any additional permits from any state agency or political subdivision for the removal, discontinuance, or replacement of such communications equipment or service as long as the state agency or political subdivision is properly notified of the necessary replacements and the replacement communications equipment is similar to the existing communications equipment.

5. Any communications provider providing service in this state that utilizes equipment from a federally banned corporation shall file a registration form with and pay a registration fee to the public service commission before September 1, 2025, and on January first of each subsequent year until such equipment is removed. The public service commission shall create the form, which shall contain, at a minimum:

(1) The name, address, telephone number, and email address of each person with managerial responsibility for operations in this state; and

(2) A certification of all instances of prohibited critical communications equipment or services prohibited under subsection 3 to 5 of section 1.1400; if the communications provider is a participant in the Federal Secure and Trusted Communications Networks Reimbursement Program, established under 47 U.S.C. Section 1601, et seq.; and the geographic coordinates of the areas served by such prohibited equipment.

6. A communications provider shall notify the commission of changes to any information submitted under subsection 5 of this section within sixty days.

7. If, under subdivision (2) of subsection 5 of this section, a communications provider certifies to the public service commission that it is a participant in the Federal Secure and Trusted Communications Networks Reimbursement Program, established under 47 U.S.C. Section 1601, et seq., the communications provider shall submit a status report to the public service commission every quarter that details the communications provider's compliance with the reimbursement program.

8. Any communications provider that violates this section shall be subject to a fine of no less than five thousand dollars per day and no more than twenty-five thousand dollars per day of noncompliance. Any communications provider that submits a false registration form described in this section shall be subject to a fine of no less than ten thousand dollars per day and no more than twenty thousand dollars per day of noncompliance.

9. Any communications provider that fails to comply with this section is prohibited from receiving any state or local funds for the development or support of new or existing critical communications infrastructure, including the Missouri communications universal service fund, and is prohibited from receiving any federal funds subject to distribution by state or local governments for the development or support of new or existing critical communications infrastructure.

10. The public service commission shall develop and publish, on a quarterly basis, a map of known prohibited communications equipment within all communications providers within or serving this state. The map shall:

(1) Clearly show the location of the prohibited equipment and the communications area serviced by the prohibited equipment;

(2) Identify the communications provider responsible for the prohibited equipment;

(3) Make clearly legible the areas serviced by the prohibited equipment; and

(4) Describe the nature of the prohibited equipment by stating, at minimum, the prohibited equipment manufacturer and equipment type or purpose.

✓