HOUSE BILL 549
By Cochran

SENATE BILL 378

By Rose

AN ACT to amend Tennessee Code Annotated, Title 4, relative to critical infrastructure.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Title 4, is amended by adding the following as a new chapter:

4-59-101.

(a) This chapter is known and may be cited as the "Tennessee Critical Infrastructure Protection Act."

(b) The purpose of this chapter is to protect critical infrastructure in this state by prohibiting foreign adversaries from accessing state critical infrastructure, assessing the state's vulnerability to sanctioned communications equipment, and prohibiting the use of adversary cameras and laser sensor technologies in this state's transportation systems.

4-59-102. As used in this chapter:

(1) "Company" means:

(A) 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

(B) A nonprofit organization;

(2) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to this state 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, state or national public health, or any combination of those matters. 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;

(E) Emergency services;

(F) Transportation systems and services; or

(G) Personal data or otherwise classified information storage systems, including cybersecurity;

(3) "Cybersecurity" means an information system or nonpublic information stored on an information system;

(4) "Department" means the department of commerce and insurance;

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

(6) "Foreign adversary" means those countries listed in 15 CFR 791.4, as amended;

(7) "Foreign principal" means:

(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 a foreign adversary, or a subsidiary of such entity, or owned or controlled wholly or in part by a person, entity, or collection of persons or entities of a foreign adversary;

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

(E) A person, entity, or collection of persons or entities, described in subdivisions (7)(A)-(D) having a controlling interest in a partnership, association, corporation, organization, trust, or other legal entity or subsidiary formed for the purpose of owning real property; and

(8) "Software" means a program or routine, or a set of one (1) or more programs or routines that are used or intended for use to cause one (1) 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 operational software.

4-59-103.

(a) A company or other entity that constructs, repairs, operates, or otherwise has significant access to critical infrastructure shall not enter into an agreement relating to critical infrastructure in this state with a foreign principal from a foreign adversary country if the agreement would allow such foreign principal to directly or remotely access or control critical infrastructure in this state.

(b) 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 such foreign principal to directly or remotely access or control critical infrastructure in this state.

(c) Notwithstanding subsections (a) and (b), a governmental or non-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 such foreign principal 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 finance and administration; 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.

4-59-104.

(a) In order to access critical infrastructure, a company must file a certification form with and pay a certification fee to the department on a registration form created by the department.

(b) To maintain registration as a company with access to critical infrastructure, a company must:

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

(2) Before hiring a person described in subsection (a) or allowing such person to continue to have access to critical infrastructure, obtain from the department of safety or a private vendor the:

(A) Criminal history of the prospective employee; and

(B) Any other background information considered necessary by the company or required by the department to protect critical infrastructure from foreign adversary infiltration or interference;

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

(4) Disclose any ownership of, partnership with, or control from an 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 cyberattack, security breach, or suspicious activity to the department; and

(8) Be in compliance with § 4-59-103.

(c) The department shall set the fee in an amount sufficient to cover the costs of administering the certification process, however such fee may not exceed one hundred fifty dollars ($150).

(d) The department shall revoke the certification of a company that is not in compliance with this section.

4-59-105.

(a) An owner of a critical infrastructure installation shall notify the department of a proposed sale or transfer of such critical infrastructure to, or investment in such critical infrastructure by, an entity domiciled outside of the United States or an entity with any foreign adversary ownership.

(b) The department has thirty (30) days from the receipt of the notice required in subsection (a) to investigate the proposed sale, transfer, or investment therein. If the department reasonably determines that the proposed sale or transfer of, or investment in, critical infrastructure is a threat to state critical infrastructure security, state economic

security, state public health, or any combination of those matters, then the attorney general and reporter shall file a request for an injunction opposing the proposed sale, transfer, or investment on behalf of the department. Upon a finding by a court 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, then the court shall permanently enjoin the proposed sale, transfer, or investment.

(c)

(1) The department shall notify critical infrastructure entities of known or suspected cyber threats, vulnerabilities, and adversarial activities to:

(A) Identify and close similar threats, vulnerabilities, and activities in like critical infrastructure installations or processes, in accordance with § 4-59-104(b)(7); and

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

(2) The notification given pursuant to this subsection (c) is intended to protect the rights of private critical infrastructure entities 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 to effectively communicate the threat of a known or suspected exploit or adversarial activity.

4-59-106.

(a) No software used in state infrastructure located within or serving this state shall include 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.

(b) All software used in state infrastructure in operation within or serving this state, including state infrastructure that is not permanently disabled, must comply with § 4-59-105.

(c) Any state infrastructure provider that removes, discontinues, or replaces any prohibited software shall not be required to obtain additional permits from a 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 such agency or subdivision can reasonably determine that the replacement software is similar to the existing software.

4-59-107.

(a) On or after July 1, 2025, a governmental entity or critical infrastructure provider shall not knowingly enter into or renew a contract with a contracting vendor of a school bus infraction detection system, speed detection system, traffic infraction detector, or other camera system used for enforcing traffic 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 a foreign adversary, or a company owned or controlled by a company primarily domiciled in a foreign adversary.

(b) On or after July 1, 2025, a governmental entity shall not knowingly enter into or renew a contract with a Light Detection and Ranging (LiDAR) technology provider 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 a foreign adversary, or a company owned or controlled by a company primarily domiciled in a foreign adversary.

(c) On or after July 1, 2025, the department of safety shall create a public listing of prohibited traffic camera and Light Detection and Ranging (LiDAR) technologies for governmental entities and critical infrastructure providers.

4-59-108.

(a) On or after July 1, 2025, a governmental entity shall not knowingly enter into or renew a contract with a contracting vendor of a Wi-Fi router or modem system 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 a foreign adversary, or a company owned or controlled by a company primarily domiciled in a foreign adversary.

(b) On or after July 1, 2025, every critical infrastructure provider in this state shall certify to the department that it does not use a Wi-Fi router or modem system:

(1) Produced by a company that is owned by the government of a foreign adversary;

(2) Produced by a company in which a foreign adversary has a controlling interest; or

(3) Produced by a company primarily domiciled in a foreign adversary, or a company owned or controlled by a company primarily domiciled in a foreign adversary.

(c) On or after July 1, 2025, the department shall create, maintain, and update a public listing of prohibited Wi-Fi router and modem system technologies for government entities and critical infrastructure providers.

4-59-109.

(a) A communications provider providing service in this state and that still utilizes equipment from a federally banned corporation in providing service to this state shall file a registration form with and pay a registration fee to the department by September 1, 2025, and on January 1 on each year thereafter. The communications provider shall register with the department prior to providing service. The department shall prescribe the registration form to be filed pursuant to this section.

(b) A communications provider shall provide the department with the name, address, telephone number, and email address of a person with managerial responsibility for the operations.

(c) A communications provider shall:

(1) Submit a registration fee at the time of submission of the registration form. The department shall set the fee in an amount sufficient to cover the costs of administering the registration process but not to exceed fifty dollars ($50.00);

(2) Keep the information required by this section current and notify the commission of any changes to such information within sixty (60) days after the change; and

(3) Certify to the department by January 1 each year all instances of prohibited critical communications equipment or services covered under Section 3 of this act if the communications provider is a participant in the Federal Secure and Trusted Communications Networks Reimbursement Program, established by the federal Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601 et seq., along with the geographic coordinates of the areas served by such prohibited equipment.

(d) If a communications provider certifies to the department that the provider is a participant in the federal Secure and Trusted Communications Networks Reimbursement Program pursuant to subdivision (c)(3), then the provider shall submit a status report to the department every quarter to prove the provider's compliance with the reimbursement program.

(e) The department shall issue an administrative fine to a communications provider who:

(1) Violates this section, with the fine to be not less than five thousand dollars ($5,000) and not greater than twenty-five thousand dollars ($25,000) for each day of noncompliance; and

(2) Knowingly submits a false registration form described in this section, with the fine to be not less than ten thousand dollars ($10,000) and not greater than twenty thousand dollars ($20,000) for each day of noncompliance.

(f) A communications provider who 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 Tennessee 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.

(g) The department shall develop and publish, on a quarterly basis, a map of known prohibited communications equipment as covered in this chapter within all communications within or serving this state. The map must:

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

(2) Identify the communications provider who owns or is otherwise 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 a minimum, the prohibited equipment manufacturer and equipment type or purpose.

SECTION 2. If any provision of this act or its application to any person or circumstance is held invalid, then the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to that end, the provisions of this act are severable.

SECTION 3. This act takes effect July 1, 2025, the public welfare requiring it.