SLS 26RS-615 **ORIGINAL**

2026 Regular Session

SENATE BILL NO. 251

BY SENATOR PRESSLY

HOMELAND SECURITY. Provides for critical infrastructure protection. (8/1/26)

AN ACT

To enact Part B of Chapter 51 of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:3081 through 3090, and to designate R.S. 51:3071 through 3080 as Part A of Chapter 51 of Title 51 of the Louisiana Revised Statutes of 1950, relative to critical infrastructure protection; to provide for critical infrastructure that needs protection from foreign adversaries accessing state critical infrastructure; to provide for assessing the state's vulnerability to sanctioned communications equipment; to prohibit use of adversary cameras and laser sensor technologies in Louisiana transportation systems; to provide enforcement of protected activities; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. Part B of Chapter 51 of Title 51 of the Louisiana Revised Statutes of 1950, comprised of R.S. 51:3081 through 3090, is hereby enacted to read as follows:

PART B. CRITICAL INFRASTRUCTURE PROTECTION

§3081.Title

This Part shall be known and may be cited as the "Louisiana Critical Infrastructure Protection Act of 2026".

§3082. Purpose

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

§3083. Definitions

The following definitions shall apply unless the context indicates otherwise:

(1) "Company" shall mean 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 or majority-owned subsidiary of those entities or business associations that exists to make a profit; or a nonprofit organization.

(2) "Critical infrastructure" shall mean systems and assets, whether physical or virtual, so vital to Louisiana or the United States of America 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 the following:

(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.

(g) Personal data or otherwise classified information storage systems, including cybersecurity.

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

(4) "Domicile" shall mean 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.

(5) "Foreign adversary" shall mean those countries listed in 15 CFR 791.4.

(6) "Foreign Principal" shall mean the following entities:

(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, 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 a foreign adversary and is not a citizen or lawful permanent resident of the United States.

(e) Any person, entity, or collection of persons or entities, described in Subparagraphs (a) through (d) of this Paragraph 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) "Office" means the Governor's Office of Homeland Security and Emergency Preparedness.

(8) "Software" shall mean any program or routine, or any set of one or more programs or routines, which are 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.

§3084. Prohibited access to critical infrastructure

A. A company or other entity constructing, repairing, operating, or otherwise having significant access to critical infrastructure may 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 the foreign principal from a foreign adversary country to directly or remotely access or control critical infrastructure in this state.

B. A governmental entity may 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.

C. Notwithstanding the provisions in Subsections A and B 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 all of the following apply:

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

(2) The contract is pre-approved by Governor's Office of Homeland Security and Emergency Preparedness.

(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.

§3085. Requirements for access to critical infrastructure

A. In order to access critical infrastructure, a company shall file a certification form with the Governor's Office of Homeland Security and Emergency Preparedness. The office shall prescribe the registration form to be

filed pursuant to this Section.

B. In order to maintain satisfactory registration as a company with access to critical infrastructure, a company shall do the following:

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

(2) Prior to hiring a person described in Subsection A of this Section or allowing a person to continue to have access to critical infrastructure, obtain from the office or a private vendor criminal history record information relating to the prospective employee and any other background information considered necessary by the company or required by the office to protect critical infrastructure from foreign adversary infiltration or interference.

(3) Prohibit foreign nationals from an 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 servers outside of foreign adversaries.

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

(7) Immediately report any cyberattack, security breach, or suspicious activity to the Governor's Office of Homeland Security and Emergency Preparedness.

(8) Be in compliance with the provisions of R.S. 51:3084.

C. The Governor's Office of Homeland Security and Emergency Preparedness shall provide that a company is compliant with all requirements of this Section or revoke certification.

§3086. Powers of Governor's Office of Homeland Security and Emergency Preparedness

A. The office 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.

B. The office shall have no more than thirty days following the notice to investigate a proposed sale, transfer, or investment in an entity as provided in this Section. If the office finds, within a reasonable suspicion, that such proposed sale, transfer, or investment shall threaten state critical infrastructure security, state economic security, state public health, or any combination of those matters, the attorney general, on behalf of the office, shall file a request for injunction opposing the proposed sale, transfer, or investment with the Louisiana Supreme Court.

C. 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 court shall issue a denial of approval.

D. The office shall notify critical infrastructure entities of known or suspected cyber threats, vulnerabilities, and adversarial activities in a manner consistent with the following:

(1) Identifying and closing similar exploits in like critical infrastructure installations or processes, especially after being notified of the activity.

(2) Maintaining operational security and normal functioning of critical infrastructure.

(3) Any notification given pursuant to this Subsection shall 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 Governor's Office of Homeland Security and Emergency Preparedness to effectively communicate the threat of a known or suspected exploit or adversarial activity.

§3087. Prohibitions on certain software in critical infrastructure

A. All software used in critical infrastructure located within or serving Louisiana shall henceforth 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.

B. All software used in state infrastructure in operation within or serving Louisiana, to include any state infrastructure which is not permanently disabled, shall have all software prohibited under the provisions of R.S. 51:3086(A) or (B) removed and replaced with software which is not prohibited under the provisions of R.S. 51:3086(A) or (B).

C. 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.

§3088. Prohibition on adversary network-connected devices

A. On or after September 1, 2026, a governmental entity or critical infrastructure provider shall not knowingly add any additional foreign adversary network-connected technologies to any critical infrastructure operating network or renew a contract with a contracting vendor of a school bus infraction detection system, speed detection system, traffic infraction detector, or any other camera system used for enforcing traffic.

B. On or after September 1, 2026, Governor's Office of Homeland Security and Emergency Preparedness shall create a public listing of all prohibited information and communications network-connected technologies that shall not be connected to critical infrastructure operating networks starting thirty days after the technology is listed. These technologies should include at a minimum school bus infraction detection systems, speed detection systems,

traffic infraction detectors, or any other camera system used for enforcing traffic, video surveillance technology, Light Detection and Ranging (LiDAR) technology, batteries, battery management systems, routers, modems, smart meters, solar inverters, and solar panels. The office shall include technologies where the original equipment manufacturer is controlled by a foreign adversary.

§3089. Foreign Adversary Fraud Fund

A. The Foreign Adversary Fraud Office (FAFO) is hereby created within the consumer protection division of the office of the attorney general. The director of this office shall be appointed by the attorney general.

B. The FAFO shall develop and bring legal claims against entities suspected of violating consumer fraud laws in their marketing, distribution, selling and otherwise promulgating of foreign adversary technologies. The resources for staffing and costs of litigation costs with bringing consumer fraud claims under the FAFO shall be administered by the office of the attorney general who may use funds appropriated to execute contracts with outside counsel to assist in implementing the provisions of this Section.

C. The FAFO office may pursue other litigation strategies, investigations, and other legal activities as approved by the attorney general provided these monies are used for defending Louisiana against foreign adversaries.

§3090. Foreign Adversary Technology Rip and Replace Fund

A. The Foreign Adversary Technology Rip and Replace Fund (FATRRP) is hereby created under the Governor's Office for Homeland Security and Emergency Preparedness. This fund shall provide resources for the replacement of foreign adversary technologies from state and local government systems and state critical infrastructure.

B. The Governor's Office of Homeland Security and Emergency Preparedness shall develop a prioritized list of state and local government systems and state critical infrastructure based upon the security risk to the state

of incapacitation of the assets. Upon receipt of funds, the Governor's Office of Homeland Security and Emergency Preparedness shall audit these assets for the presence of foreign adversary technologies and shall rip and replace these technologies upon the availability of funds for replacement.

Section 2. The Louisiana State Law Institute is hereby directed to designate the provisions of R.S. 51:3071 through 3080 as Part A of Chapter 51 of Title 51 of the Louisiana Revised Statutes of 1950 to be entitled, "PART A. DATABASE SECURITY BREACH NOTIFICATION".

The original instrument and the following digest, which constitutes no part of the legislative instrument, were prepared by Senate Legislative Services. The keyword, summary, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

DIGEST

SB 251 Original 2026 Regular Session Pressly

Proposed law enacts the "Louisiana Critical Infrastructure Protection Act".

Proposed law provides mechanisms to protect against foreign adversaries accessing state critical infrastructure. Provides for assessing the state's vulnerability to sanctioned communications equipment and to prohibit certain use of adversary cameras and laser sensor technologies in state transportation systems.

Proposed law creates the Foreign Adversary Fraud Office (FAFO) within the consumer protection division of the office of the attorney general to develop and bring legal claims against entities suspected of violating consumer fraud laws in their marketing, distribution, selling and otherwise promulgating of foreign adversary technologies.

Authorizes the FAFO to pursue other litigation strategies, investigations, and other legal activities.

Proposed law creates Foreign Adversary Technology Rip and Replace Fund (FATRRP) within the Governor's Office for Homeland Security and Emergency Preparedness to provide funds to assist in replacement of foreign adversary technologies from state and local government systems and state critical infrastructure.

Proposed law requires that the Governor's Office of Homeland Security and Emergency Preparedness shall develop a prioritized list of state and local government systems and state critical infrastructure based upon the security risk to the state of incapacitation of the assets. Requires the office to audit these assets for the presence of foreign adversary technologies and shall rip and replace these technologies upon the availability of funds for replacement.

Effective August 1, 2026.

(Adds R.S. 51:3081-3090)