

RÉSUMÉ DIGEST

ACT 750 (SB 251)

2026 Regular Session

Pressly

New law enacts the "Louisiana Critical Infrastructure Protection Act of 2026" to be construed and applied in a manner consistent with federal law and not be interpreted or enforced to prohibit, restrict, condition, or delay any transaction, agreement, activity, technology, software, service, or access that has been authorized, approved, licensed, exempted, or otherwise permitted by the United States government.

New law prohibits a company or other entity constructing, repairing, operating, or otherwise having significant access to critical infrastructure from entering into an agreement relating to critical infrastructure in this state with a foreign principal from a foreign adversary if the agreement would allow the foreign principal from a foreign adversary to directly or remotely exercise operational authority over critical infrastructure in this state.

New law defines "company", "critical infrastructure", "cybersecurity", "domicile", "foreign adversary", "foreign principal", "office", "operational command authority", "significant access", and "software".

New law defines "critical infrastructure" to mean systems and assets, whether physical or virtual, so vital to the state or the nation that the incapacity or destruction of these 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. Provides that a critical infrastructure may be publicly or privately owned, and includes but is not limited to the following:

- (1) Gas and oil production, storage, or delivery systems.
- (2) Water supply, refinement, storage, or delivery systems.
- (3) Telecommunications network.
- (4) Electrical power delivery systems.
- (5) Emergency services.
- (6) Transportation systems and services.
- (7) Personal data or otherwise classified information storage system, including cybersecurity.

New law provides that "cybersecurity" means measures taken to protect a computer, computer network, computer system, or other technology infrastructure against unauthorized use or access.

New law provides that "operational command authority" means the authority to direct, control, or make real-time operational decisions affecting the physical functioning, safety, or emergency response of critical infrastructure.

New law prohibits a company or other entity constructing, repairing, or otherwise having significant access to critical infrastructure from knowingly entering into a contract or other agreement relating to critical infrastructure in this state with a company that is a foreign principal of a foreign adversary if the agreement would allow the foreign principal of a foreign adversary to directly or remotely exercise operational control over critical infrastructure in this state.

New law prohibits a governmental entity from knowingly entering 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 if the agreement would allow the foreign principal from a foreign adversary to directly or remotely exercise operational control over critical infrastructure in this state.

New law provides for authority of an entity or governmental entity to enter into an agreement relating to critical infrastructure with a foreign principal from a foreign adversary country.

New law provides for exemptions for certain transactions, agreements, activities, technology, software, services, or access conducted pursuant to and in compliance with a specific license or authorization issued by the United States government.

New law prohibits the use of certain software providing operational command authority over critical infrastructure produced by companies subject to or controlled by a foreign adversary, and procedures regarding the replacement of any such software.

New law provides exemptions for certain telecommunications providers and certain electric utilities.

New law authorizes the attorney general to institute civil enforcement proceedings beginning November 29, 2026 including but not limited to actions against a foreign adversary company or any other vendor, provider, distributor, or relabeler or white-labeler of a foreign adversary technology for violations of the Unfair Trade Practices and Consumer Protection Law.

Effective August 1, 2026.

(Adds R.S. 51:3081-3089)