DIGEST

SB 46 Original   2019 Regular Session   Peacock

Proposed law creates the Louisiana Cybersecurity Information Sharing Act
(Act).

Proposed law defines "appropriate entity", "cybersecurity purpose", "cybersecurity threat", "cyber
threat indicator", "defensive measure", "information system", "federal entity", "malicious cyber
command and control", "malicious reconnaissance", "monitor", "private entity", "security control",
"security vulnerability", and "state entity".

Proposed law provides that a private entity may, for a cybersecurity purpose, monitor certain
information systems and information that are stored on, processed by, or passed through certain
information systems.

Proposed law provides that a private entity may, for a cybersecurity purpose, operate a defensive
measure on certain information systems.

Proposed law authorizes a private entity, for a cybersecurity purpose and consistent with the
protection of classified information, to share or receive a cyber security threat indicator or defensive
measure with certain entities.

Proposed law requires a private entity to implement and utilize a security control to protect against
unauthorized access to or acquisition of a cyber threat or defensive measure.

Proposed law provides for the protection of personal information not directly related to a
cybersecurity threat.

Proposed law exempts from the Public Records Law a cyber threat indicator or defensive measure
shared by a state entity with an appropriate entity.

Proposed law authorizes a private entity to share a cyber threat indicator or defensive measure with
an appropriate entity.

Proposed law requires the private entity to:

(1)   Take reasonable measures to remove or limit the receipt, retention, use, and dissemination
        of a cyber threat indicator containing personal information from the information shared with
        the appropriate entity, provided that the personal information is not critical to the appropriate
        entity's response or ability to mitigate the cyber threat indicator.

(2)   Include requirements to safeguard a cyber threat indicator containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the federal or state government.

(3)   Protect the confidentiality of a cyber threat indicator containing personal information of specific individuals or information that identifies specific individuals to the greatest extent practicable and require recipients to be informed that such indicator may only be used for purposes authorized by proposed law.

Proposed law does not relieve a person from compliance with the Database Security Breach Notification Law.

Proposed law provides that a cyber threat indicator and defensive measure shared with an appropriate entity shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

Proposed law provides that a cyber threat indicator or defensive measure provided by a private entity to an appropriate entity shall be considered the commercial, financial, and proprietary information of the private entity when designated by the originating private entity or a third party acting in accordance with the written authorization of the originating private entity.

Proposed law provides that a cyber threat indicator and defensive measure provided to an appropriate entity may be disclosed to, retained by, and used by any federal or state entity for certain purposes.

Proposed law restricts the disclosure, retention, or use of a cyber threat indicator and defensive measure to actions authorized by proposed law.

Proposed law provides relative to the retention, use, and dissemination of a cyber threat indicator and defensive measure by the federal or state government to an appropriate entity.

Proposed law provides that there shall be no cause of action against any private entity for the monitoring of an information system or information stored on, processed by, or passed through such information system or for the sharing or receipt of a cyber threat indicator or defensive measure with another private entity, a federal or state entity, or an appropriate entity if such monitoring, sharing, or receipt is conducted in accordance with proposed law.

Proposed law provides that a cyber threat indicator or defensive measure shared with a state entity or an appropriate entity shall not be used by any state entity to regulate the lawful activity of any private entity or any activity taken by a private entity. Proposed law does allow such indicator or measure to be used in the development or implementation of a regulation relating to such information systems.

Proposed law provides relative to antitrust immunity under certain circumstances.

Proposed law requires that on or before March first of each year, a state entity that receives information concerning a cyber threat indicator or defensive measure during the preceding calendar year shall submit to the governor an annual report containing a statistical summary of the following:

(1)   Entities or types of industries that shared information with the state entity.

(2)   Cyber threat indicators and defensive measures shared with the state entity.

Proposed law authorizes the office of state police, in accordance with the APA, to adopt rules necessary to implement the provisions of proposed law.

Effective August 1, 2019.

(Adds R.S. 51:2101-2109)