SLS 19RS-68 **REENGROSSED**

2019 Regular Session

SENATE BILL NO. 46

BY SENATOR PEACOCK

Prefiled pursuant to Article III, Section 2(A)(4)(b)(i) of the Constitution of Louisiana.

INTERNET. Enacts the Louisiana Cybersecurity Information Sharing Act. (8/1/19)

AN ACT

To enact Chapter 31 of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:2101 through 2110, relative to cybersecurity; to authorize private entities to monitor, share, and receive certain information relative to cyber threats; to authorize certain defensive measures; to provide relative to certain security and information controls; to provide for definitions; to provide for immunity; to provide for public records exemptions; and for confidentiality of certain information; to provide for annual reporting of certain information by state entities; to provide for certain terms, conditions, and procedures; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. Chapter 31 of Title 51 of the Louisiana Revised Statutes of 1950, comprised of R.S. 51:2101 through 2110, is hereby enacted to read as follows:

CHAPTER 31. LOUISIANA CYBERSECURITY INFORMATION SHARING ACT

§2101. Short title

This Chapter shall be known and may be cited as the "Louisiana Cybersecurity Information Sharing Act".

§2101.1. Legislative intent; federal law

The purpose of this Act is to provide a framework for sharing cybersecurity information under Louisiana law that is consistent with the federal law for sharing of cybersecurity information. To the extent that any provision of this Act is inconsistent with or conflicts with the requirements of the Federal Cybersecurity Information Sharing Act of 2015, 6 U.S.C.A. §1501 et seq., such provision of this Act shall not apply and the applicable federal law shall control.

§2102. Definitions

As used in this Chapter, the following words shall have the meaning ascribed to them in this Section, unless the text clearly indicates otherwise:

(1) "Appropriate entity" means any of the following:

(a) Department of Justice, investigation division.

(b) The Louisiana State Analytical and Fusion Exchange, office of state police, Department of Public Safety and Corrections.

(c) The Governor's Office of Homeland Security and Emergency Preparedness.

(d) An appropriate federal entity as defined in 6 U.S.C.A. §1501(3).

(2) "Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or passed through an information system from a cybersecurity threat or security vulnerability.

(3) "Cybersecurity threat" means an action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or passed through an information system. A "cybersecurity threat" does not include an action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(4) "Cyber threat indicator" means information that is necessary to describe or identify any of the following:

(a) A malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability.

(b) A method of defeating a security control or exploitation of a security vulnerability.

(c) A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability.

(d) A method of causing a user with legitimate access to an information system, or to information that is stored on, processed by, or passed through an information system, to unwittingly enable the defeat of a security control or exploitation of a security vulnerability.

(e) A malicious cyber command and control.

(f) An actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat.

(g) Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

(5) "Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system, or to information that is stored on, processed by, or passed through an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. A defensive measure shall not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or passed through such information system not owned by the entity operating the measure or the entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(6) "Information system" includes but is not limited to a computer, computer server, computer program, computer service, computer software, internet-connected device, or computer system. An information system shall also include industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers that store, process, or transmit information.

(7) "Federal entity" means a department or agency of the United States or any component of such department or agency.

(8) "Malicious cyber command and control" means a method for unauthorized, remote identification of, access to, or use of an information system or information that is stored on, processed by, or passed through an information system.

(9) "Malicious reconnaissance" means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(10) "Monitor" means to acquire, identify, or scan, or to possess information that is stored on, processed by, or passed through an information system.

(11) "Private entity" means any citizen of the United States or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity domiciled in the United States of America, including an officer, employee, or agent thereof. "Private entity" does not include any foreign entities, such as governments, nations, or political organizations.

(12) "Security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(13) "Security vulnerability" means any attribute of hardware, software, process, or procedure that may enable or facilitate the defeat of a security control.

(14) "State entity" means the state, a political subdivision of the state, and any officer, agency, board, commission, department or similar body of the state or any political subdivision of the state.

§2103. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats; private entities

A. Notwithstanding any provision of law to the contrary, a private entity may, for a cybersecurity purpose, monitor the following:

(1) An information system of the private entity.

(2) An information system of another private entity, upon the authorization and written consent of such other entity.

(3) An information system of a federal or state entity, upon the authorization and written consent of an authorized representative of the federal or state entity.

(4) Information that is stored on, processed by, or passed through an information system monitored by the private entity.

B. Notwithstanding any provision of law to the contrary, a private entity may, for a cybersecurity purpose, operate a defensive measure that is applied to the following:

(1) An information system of the private entity in order to protect the rights or property of the private entity.

(2) An information system of another private entity, upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity.

(3) An information system of a federal or state entity, upon written consent of an authorized representative of such federal or state entity for operation of such defensive measure to protect the rights or property of the

federal or state government.

C.(1) Except as provided in Paragraph (2) of this Subsection and notwithstanding any other provision of law to the contrary, a private entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, another private entity or a federal or state entity a cyber threat indicator or defensive measure.

(2) A private entity receiving a cyber threat indicator or defensive measure from another private entity or a federal or state entity shall comply with any lawful restriction placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity.

D.(1) A private entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure pursuant to this Section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) Prior to sharing a cyber threat indicator or defensive measure, a private entity shall either:

(a) Review the cyber threat indicator to assess whether such indicator contains any information not directly related to a cybersecurity threat that the private entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such personal information. For the purposes of this Chapter, "personal information" shall refer to "personal information" as defined in La. R.S. 51:3073(4)(a).

(b) Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the private entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

(3)(a) A cyber threat indicator or defensive measure shared or received

pursuant to the provisions of this Section may, for a cybersecurity purpose, be used by a private entity to monitor or operate a defensive measure that is applied to an information system of the private entity or an information system of another private entity or a federal or state entity, provided such other private entity or a such federal or state entity has given its written consent.

(b) A cyber threat indicator or defensive measure shared or received pursuant to the provisions of this Section may, for a cybersecurity purpose, be used, retained, and further shared by a private entity subject to a lawful restriction placed by the sharing private entity or federal or state entity on such cyber threat indicator or defensive measure or an otherwise applicable provision of law.

(4)(a) A state entity that receives a cyber threat indicator or defensive measure pursuant to the provisions of this Section may use such cyber threat indicator or defensive measure in accordance with the provisions of R.S. 51:2104.

(b) A cyber threat indicator or defensive measure shared by a state entity with an appropriate entity shall be deemed voluntarily shared information and exempt from disclosure under the Public Records Law, R.S. 44:1 et seq.

E. The sharing of a cyber threat indicator or defensive measure with a private entity shall not create a right or benefit to similar information from that private entity.

§2104. Sharing of a cyber threat indicator and defensive measure with an appropriate entity

A.(1) A private entity may, for a cybersecurity purpose and consistent with the protection of classified information, share a cyber threat indicator or defensive measure with an appropriate entity through the transmission of an email to such entity.

(2) In sharing a cyber threat indicator or defensive measure with an appropriate entity, the private entity shall:

(a) 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 a cyber threat indicator.

(b) 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.

(c) Protect to the greatest extent practicable, the confidentiality of a cyber threat indicator containing personal information of specific individuals or information that identifies specific individuals and requires recipients to be informed that such indicator may be used only for purposes authorized by this Chapter.

(d) Expressly state in the subject line of the email to the appropriate entity that the private entity is conveying a "Cyber Threat Indicator" or "Cyber Defensive Measure".

(3)(a) 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.

(b) 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.

(c) A cyber threat indicator or defensive measure shared with an appropriate entity shall be deemed voluntarily shared information and exempt from disclosure under the Public Records Law, R.S. 44:1 et seq.

(d) A cyber threat indicator and defensive measure provided to an appropriate entity may be disclosed to, retained by, and used by, consistent with

applicable provisions of law, any federal or state entity solely for the following purposes:

(i) A cybersecurity purpose.

(ii) Identifying a cybersecurity threat, including the source of such threat or a security vulnerability.

(iii) Responding to, or otherwise mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction.

(iv) Responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety.

(v) Preventing, investigating, disrupting, or prosecuting an offense arising out of a threat as provided in Item (iii) of this Subparagraph.

B. A cyber threat indicator and defensive measure shared with an appropriate entity shall not be disclosed to, retained by, or used by any federal or state entity for any use not permitted under Subsection A of this Section.

C. A cyber threat indicator or defensive measure provided to an appropriate entity shall be retained, used, and disseminated by the federal or state government as follows:

(1) In a manner consistent with Subsection A of this Section.

(2) In a manner that protects from unauthorized use or disclosure any cyber threat indicator that may contain personal information of a specific individual or information that identifies a specific individual.

(3) In a manner that protects the confidentiality of any cyber threat indicator containing information of a specific individual or information that identifies a specific individual.

§2105. Protection from liability; private entities

If conducted in accordance with the provisions of this Chapter, there shall be no cause of action against any private entity:

(1) 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.

(2) For the monitoring of an information system or information stored on, processed by, or passed through such information system, of another private entity, a federal or state entity, or an appropriate entity.

(3) For the monitoring of a private entity's information system or information stored on, processed by, or passed through such information system, after receipt of a cyber threat indicator or defensive measure from another private entity, federal or state entity, or an appropriate entity.

§2106. State regulatory authority

A cyber threat indicator or defensive measure shared in accordance with the provisions of this Chapter with a state entity or an appropriate entity shall not be used by any state entity for the criminal prosecution of the lawful activity of any private entity or any activity taken by a private entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator. However, a shared cyber threat indicator or defensive measure may be used in the development or implementation of a regulation relating to such information systems.

§2107. Antitrust immunity; exception

A. It shall not be considered a violation of state antitrust laws for two or more private entities to exchange or provide, for a cybersecurity purpose, a cyber threat indicator or defensive measure or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat. The provisions of this Paragraph shall apply only to information that is exchanged, or assistance provided, in order to assist with either of the following:

(1) Facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or to information that is stored on, processed by, or passed through an information system.

(2) Communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or to information that is stored on, processed by, or passed through an information system.

B. Nothing in this Section shall authorize price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

§2108. Compliance with Database Security Breach Notification Law

Nothing in this Chapter shall relieve a person or entity from compliance with the Database Security Breach Notification Law, R. S. 51:3071 et seq., specifically including but not limited to, the requirements under R.S. 51:3074.

§2109. Annual report; state agencies

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.

§2110. Rulemaking authority

The Department of Corrections, office of state police, may, in accordance with the Administrative Procedure Act, adopt all rules necessary to implement the provisions of this Chapter.

The original instrument and the following digest, which constitutes no part of the legislative instrument, were prepared by Michelle Ridge.

DIGEST

SB 46 Reengrossed 2019 Regular Session Peacock

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

Proposed law provides that the purpose of this Act is to provide a framework for sharing cybersecurity information under Louisiana law that is consistent with federal law.

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.

(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 be used only for purposes authorized by proposed law.

(4) Expressly state in the subject line of the email to the appropriate entity that the

private entity is conveying a "Cyber Threat Indicator" or "Cyber Defensive Measure".

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 following, if conducted in accordance with the provisions of proposed law:

(1) 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.

(2) The monitoring of an information system or information stored on, processed by, or passed through such information system of another private entity, state or federal entity, or an appropriate entity.

(3) The monitoring of a private entity's information system or information stored on, processed by, or passed through such information system, after receipt of a cyber threat indicator or defensive measure from another private entity, federal or state entity, or an appropriate entity.

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 for the criminal prosecution of 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 does not relieve a person from compliance with the Database Security Breach Notification Law.

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. 51:2101-2110)

Summary of Amendments Adopted by Senate

Committee Amendments Proposed by Senate Committee on Commerce, Consumer Protection, and International Affairs to the original bill

1. Makes technical changes.

2. Adds a provision relative to legislative intent and federal law.

3. Adds a provision requiring the subject line of emails conveying a cyber threat indicator or defensive measure to include certain information.

4. Revises language on causes of action.

5. Removes a provision that requires the annual report submitted by state entities to the governor to be subject to public records law.

Senate Floor Amendments to engrossed bill

1. Makes Legislative Bureau amendments.