SLS 26RS-731 **ORIGINAL**

2026 Regular Session

SENATE BILL NO. 474

BY SENATOR MILLER

INFORMATION TECHNOLOGY. Creates the Protecting Louisiana's Infrastructure from Artificial Intelligence Risk Act. (1/1/27)

AN ACT

To enact Chapter 54 of Title 51 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 51:3111.1 through 3111.9, relative to artificial intelligence; to provide for the Protecting Louisiana's Infrastructure from Artificial Intelligence Risk Act; to provide for transparency requirements of certain artificial intelligence models; to provide for catastrophic risk management; to provide for critical safety incident reporting; to provide for whistleblower protections; to provide for penalties; to provide relative to the Public Records Law; to provide for terms, conditions, and definitions; to provide for an effective date; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. Chapter 54 of Title 51 of the Louisiana Revised Statutes of 1950, comprised of R.S. 51:3111.1 through 3111.9, is hereby enacted to read as follows:

CHAPTER 54. INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE RISK

§3111.1. Short Title

This Chapter may be cited as "Protecting Louisiana's Infrastructure from Artificial Intelligence Risk Act".

§3111.2. Definitions

A. As used in this Chapter, the following words shall mean the following:

(1) "Affiliate" means a person controlling, controlled by, or under common control with a specified person.

(2) "Artificial intelligence model" means a machine-based system that receives inputs and generates outputs, including but not limited to predictions, content, recommendations, or decisions that can influence physical or virtual environments. "Artificial intelligence model" includes machine learning models, deep learning models, and other computational models designed to simulate aspects of human intelligence.

(3)(a) "Catastrophic risk" means a foreseeable and material risk that a frontier developer's development, storage, use, or deployment of a frontier model will materially contribute to the death or serious injury of more than fifty people or more than one billion dollars in property damage or loss arising from a single incident involving a frontier model:

(i) Providing expert-level assistance in the creation, synthesis, acquisition, weaponization, or release of a chemical or biological weapon, including but not limited to the identification of novel chemical compounds or biological agents with potential for weaponization, or the provision of detailed technical instructions for the production, stabilization, or dispersal of such agents.

(ii) Engaging in or materially facilitating a cyberattack, with no meaningful human oversight, intervention, or supervision, against critical infrastructure systems, including but not limited to energy production and distribution systems, healthcare information technology systems, port logistics and navigation systems, water treatment facilities, or electrical grid systems, where cyberattacks result in or poses a substantial risk of physical harm, environmental damage, or significant disruption of essential services.

(iii) Engaging in conduct with no meaningful human oversight,

intervention, or supervision that, if the conduct had been committed by a human, would constitute a felony under state or federal law, including but not limited to offenses involving extortion, fraud, theft, or unauthorized access to computer systems.

(iv) Evading the control of its frontier developer or user in a manner that demonstrates autonomous pursuit of objectives inconsistent with the developer's or user's instructions or safety protocols.

(b) "Catastrophic risk" does not include a foreseeable and material risk from any of the following:

(i) Information that a frontier model outputs if the information is otherwise publicly accessible in a substantially similar form from a source other than a foundation model.

(ii) Lawful activity of the state or federal government.

(iii) Harm caused by a frontier model in combination with other software if the frontier model did not materially contribute to the harm.

(4) "Critical infrastructure" means systems, assets, and networks, whether physical or virtual, that are so vital to the state or the United States, that the incapacity or destruction of these systems, assets, or networks, would have a debilitating impact on public health, public safety, economic security, or any combination thereof. "Critical infrastructure" includes, without limitation, energy production and refining facilities, healthcare delivery systems, shipping port operations and logistics systems, water treatment and distribution systems, electrical generation and transmission systems, natural gas pipeline systems, and petrochemical manufacturing facilities.

(5) "Critical safety incident" means any of the following:

(a) Unauthorized access to, modification of, or exfiltration of the model weights of a frontier model that results in death, bodily injury, or a cyberattack against critical infrastructure.

(b) Harm resulting from the materialization of a catastrophic risk as

defined in this Section.

(c) Loss of control of a frontier model causing death, bodily injury, or damage to critical infrastructure.

(d) A frontier model that provides specific and actionable technical assistance for the creation of a chemical or biological weapon to a person who would not otherwise have been able to obtain that assistance.

(e) A frontier model that uses deceptive techniques against the frontier developer to subvert the controls or monitoring of its frontier developer outside of the context of an evaluation designed to elicit this behavior and in a manner that demonstrates materially increased catastrophic risk.

(6) "Department" means the Louisiana Department of Justice, office of the attorney general.

(7) "Deploy" means to make a frontier model available to a third party, except for the primary purpose of developing or evaluating the frontier model.

(8) "Foundation model" means an artificial intelligence model that is trained on a broad data set, designed for generality of output, and adaptable to a wide range of distinctive tasks.

(9) "Frontier AI framework" means documented technical and organizational protocols to manage, assess, and mitigate catastrophic risks, with specific provisions for assessing risks related to cybersecurity threats to critical infrastructure and biochemical weapon development.

(10) "Frontier developer" means a person who has trained, or initiated the training of, a frontier model, with respect to which the person has used, or intends to use, at least as much computing power to train the frontier model.

(11)(a) "Frontier model" means a foundation model that either:

(i) Was trained using a quantity of computing power greater than 10^26 integer or floating-point operations; or

(ii) Was produced by applying knowledge distillation to a frontier model as defined in this Subparagraph (a) of this Paragraph, provided that the

compute cost for applying knowledge distillation exceeds five million dollars.

(b) The quantity of computing power described in Subparagraph (a) of this Paragraph includes computing for the original training run and any subsequent fine-tuning, reinforcement learning, or other material modifications to a preceding foundation model.

(12) "Knowledge distillation" means any supervised learning technique using a larger artificial intelligence model or its output to train a smaller model with similar or equivalent capabilities.

(13) "Large frontier developer" means a frontier developer that together with its affiliates had more than five hundred million dollars in annual gross revenues in the preceding calendar year.

(14) "Model weight" means a numerical parameter in a frontier model that is adjusted through training and helps determine how inputs are transformed into outputs.

(15) "Property" means corporeal or incorporeal property.

§3111.3. Frontier AI framework requirements

A. A large frontier developer shall write, implement, comply with, and clearly and conspicuously publish on its internet website a frontier AI framework that applies to the large frontier developer's frontier models and describes in detail how the large frontier developer approaches all of the following:

(1) Incorporating national and international standards, and industry-consensus best practices into its frontier AI framework, including standards related to cybersecurity and biosecurity risk management.

(2) Defining and assessing the large frontier developer's thresholds to identify and assess whether a frontier model has capabilities that may pose a catastrophic risk, including specific thresholds for cybersecurity capabilities that may be used to compromise critical infrastructure and capabilities, and that may assist in the development, production, or deployment of chemical or

biological weapons. These thresholds may include multiple-tiered levels of concern.

(3) Applying mitigations to address potential catastrophic risks identified under Paragraph (2) of this Subsection, with specific mitigation strategies for cybersecurity risks to critical infrastructure and biochemical weapon risks.

(4) Reviewing assessments and adequacy of mitigations as part of the decision to deploy a frontier model or use it extensively and internally.

(5) Using third parties, including cybersecurity experts and biosecurity specialists, to assess catastrophic risks and mitigation effectiveness.

(6) Revisiting and updating the frontier AI framework, including any criteria that trigger updates and how the large frontier developer determines when its frontier models are substantially modified enough to require disclosures pursuant to Subsection C of this Section.

(7) Cybersecurity practices to secure unreleased model weights from unauthorized modification or transfer, including measures to prevent state-sponsored or other sophisticated threat actors from accessing model capabilities.

(8) Identifying and responding to critical safety incidents, with specific protocols for incidents involving cyberattacks on critical infrastructure or potential biochemical threats.

(9) Instituting internal governance practices to ensure implementation of these processes.

(10) Assessing and managing catastrophic risk resulting from the internal use of its frontier models, including risks resulting from a frontier model circumventing oversight mechanisms.

B.(1) A large frontier developer shall review and update its frontier AI framework at least once per year.

(2) Within thirty days of making any material modification to its frontier AI framework, a large frontier developer shall clearly and conspicuously

publish on its website the modified frontier AI framework and a justification for the modification.

C.(1) Before, or concurrently with, deploying a new or substantially modified frontier model, a frontier developer shall clearly and conspicuously publish on its website a transparency report containing the frontier model's release date, languages, output modalities, intended uses, and restrictions or conditions, and a mechanism to communicate with the frontier developer.

(2) Before, or concurrently with, deploying a new or substantially modified frontier model, a large frontier developer shall include in the transparency report required by Paragraph (1) of this Subsection summaries of all of the following:

(a) Assessments of catastrophic risks from the frontier model conducted pursuant to the frontier AI framework, including specific assessments of cybersecurity capabilities and biochemical risk.

(b) The results of those assessments.

(c) The extent to which third-party evaluators, including cybersecurity and biosecurity experts, were involved.

(d) Other steps taken to fulfill the requirements of the frontier AI framework with respect to the frontier model.

(3) A frontier developer that publishes the information under this Subsection in a larger document, including a system card or model card, shall be in compliance with the applicable provision of this Section.

D. A large frontier developer shall transmit to the department a summary of any assessment of catastrophic risk resulting from internal use of its frontier models every three months or pursuant to another reasonable schedule specified by the large frontier developer and communicated in writing to the department.

E. A frontier developer shall not make a materially false or misleading statement about catastrophic risk, its management of catastrophic risk, or its

implementation of, or compliance with, its frontier AI framework, including but not limited to in a certification filed to the department pursuant to Subsection G of this Section, unless the statement was made in good faith and was reasonable under the circumstances.

F.(1) Beginning on July 1, 2028, and at least annually thereafter, a large frontier developer shall retain a third-party auditor to produce a report signed and certified by the auditor that contains but is not limited to both of the following:

(a) A detailed assessment of whether the large frontier developer has substantially complied with its frontier AI framework during the prior year, including cybersecurity and biochemical risk management provisions.

(b) Any material deviations between the requirements of the large frontier developer's frontier AI framework and the large frontier developer's actual practices during the prior year.

(2) The third-party auditor shall not conduct an audit if it has a financial interest in the large frontier developer other than financial compensation for performing an audit.

(3) Within thirty days of receiving an auditor's report required by Paragraph (1) of this Subsection, the large frontier developer shall publish on its website a high-level summary of the findings of the audit.

G. Within twelve months after publishing its frontier AI framework in accordance with Subsection A of this Section, and annually thereafter, a large frontier developer shall provide to the department a written certification disclosing either of the following:

(1) That the developer has been in compliance with its frontier AI framework during the prior year.

(2) Any material deviations from the developer's frontier AI framework that occurred during the prior year, including a description of corrective actions taken or planned.

H.(1) When a frontier developer publishes documents to comply with the provisions of this Section, the frontier developer may make redactions to those documents as necessary to protect the frontier developer's trade secrets or cybersecurity, public safety, or United States national security or to comply with any federal or state law.

(2) If a frontier developer redacts information in a document pursuant to this Subsection, the frontier developer shall describe the character and justification of the redaction in any published version of the document to the extent permitted by the concerns that justify redaction and shall retain the unredacted information for five years.

§3111.4. Critical safety incident reporting

A. The department shall establish a mechanism for frontier developers or the public to report critical safety incidents that includes all of the following information:

(1) The date of the critical safety incident.

(2) The reasons the incident qualifies as a critical safety incident.

(3) A description of the incident, including whether the incident involved cybersecurity threats to critical infrastructure or biochemical risks.

(4) Whether the incident involved internal use of a frontier model.

(5) Whether the incident posed any risk to energy, health care, or port infrastructure in the state or in any other jurisdiction.

B.(1) The department shall establish a mechanism for large frontier developers to confidentially submit summaries of any assessments of potential catastrophic risk from internal use of its frontier models.

(2) The department shall take all precautions to limit access of any summaries submitted pursuant to Paragraph (1) of this Subsection to only personnel with a need to know and in order to prevent unauthorized access.

C.(1) Subject to the provisions of Paragraph (2) of this Subsection, a frontier developer shall report any critical safety incident pertaining to its

Coding: Words which are ~~struck through~~ are deletions from existing law; words in **boldface type and underscored** are additions.

frontier models to the department within fifteen days after discovering the critical safety incident.

(2) If a frontier developer discovers that a critical safety incident poses an imminent risk of death, serious physical injury, or an active cyberattack on critical infrastructure, the frontier developer shall disclose that incident within twenty-four hours to the department and to any other appropriate authority with jurisdiction as required by law.

(3) A frontier developer may file an amended report upon discovering additional information about the critical safety incident.

D. The department shall review critical safety incident reports submitted by frontier developers and may review reports submitted by the public.

E.(1) The department may transmit reports of critical safety incidents and reports from covered employees to the legislature, the governor, the federal government, or appropriate state or federal agencies, including the Cybersecurity and Infrastructure Security Agency and the United States Department of Homeland Security.

(2) Beginning July 1, 2028, and annually thereafter the department shall:

(a) Produce a report with anonymized and aggregated information about critical safety incidents reviewed since the preceding report, with specific sections addressing incidents related to cybersecurity and biochemical risks.

(b) Produce a report with anonymized and aggregated information about covered employees' reports reviewed since the preceding report.

(3) A report transmitted pursuant to this Subsection shall not include information that may compromise the frontier developer's trade secrets or cybersecurity, public safety, or national security, or violate any federal or state law.

(4) The department shall submit the reports to the president of the Senate, the speaker of the House of Representatives, and the governor.

F.(1) The department may designate federal laws, regulations, or

guidance that impose substantially equivalent or stricter standards or requirements for critical safety incident reporting.

(2) After a frontier developer has declared to the department its intent to comply with a designated federal law, regulation, or guidance, the frontier developer shall constitute compliance with this Section to the extent that the frontier developer complies with the designated federal law, regulation, or guidance until the frontier developer revokes its intent or the department revokes the relevant designation.

(3) Failure to meet these standards or requirements constitutes a violation of this Part.

(4) The department shall revoke a designation if the requirements of Paragraph (1) of this Subsection are no longer met.

§3111.5. Public records; exemption

A. The following records are confidential and shall not be subject to the provisions of the Public Records Law, R.S. 44:1 et seq.:

(1) A report of assessments of catastrophic risk from internal use pursuant to R.S. 51:3111.2.

(2) A certification submitted pursuant to R.S. 51:3111.2.

(3) A report of a critical safety incident submitted pursuant to R.S. 51:3111.3.

(4) A covered employee report.

B. The provisions of this Section shall terminate on July 1, 2031.

§3111.6. Annual assessment and recommendations

A. On or before July 1, 2028, and annually thereafter, the department, in consultation with the Governor's Office of Homeland Security and Emergency Preparedness, shall assess developments relevant to this Chapter and recommend whether to update the definitions of "frontier model", "frontier developer", and "large frontier developer" to reflect technological developments and widely accepted standards.

B. In making recommendations pursuant to this Section, the department shall consider:

(1) Similar federal or international thresholds for the management of catastrophic risk, aligning with federal definitions to the extent consistent with this Chapter.

(2) Evolving cybersecurity threat landscapes affecting critical infrastructure, particularly energy, health care, and port sectors.

(3) Developments in biochemical weapon capabilities enabled or facilitated by artificial intelligence.

(4) Stakeholder input, including input from critical infrastructure operators in this state.

(5) The length, complexity, and external verifiability of coverage determinations.

C. The department shall submit its findings and recommendations, together with specific proposals for legislation, to the president of the Senate of the Louisiana Legislature and the speaker of the House of Representatives of the Louisiana Legislature.

§3111.7. Penalties

A. A large frontier developer that fails to publish or transmit a compliant document required to be published or transmitted under this Chapter, makes a statement in violation of R.S. 51:3111.2(E), fails to complete a third-party audit or publish a summary of the results of an audit as required by R.S. 51:3111.2(F), fails to complete a certification as required by R.S. 51:3111.2(G), fails to report an incident as required by R.S. 51:3111.3, or fails to comply with its own frontier AI framework, is subject to a civil penalty.

B. The attorney general may bring an action against a violator to recover a penalty not to exceed one million dollars per violation for a first violation or ten million dollars for a second or subsequent violation of the same requirement.

C. For purposes of bringing an action pursuant to this Section, a frontier developer or large frontier developer that develops, deploys, or operates frontier models in this state is both engaged in substantial and not isolated activities within this state, and is doing business in this state, shall be subject to the jurisdiction of the courts of this state.

D. Loss of value of equity does not count as damage to or loss of property for the purposes of this Chapter.

§3111.8. Preemption

This Chapter preempts any rule, regulation, code, ordinance, or other law adopted by a parish, municipality, or other local governmental entity on or after July 1, 2027, specifically related to the regulation of frontier developers with respect to their management of catastrophic risk.

§3111.9. Whistleblower protections; frontier artificial intelligence developers

A. As used in this Section, the following terms have the meanings ascribed to them herein:

(1) "Catastrophic risk" has the same meaning as provided in R.S. 51:3111.2, except that the term applies to a foundation model.

(2) "Covered employee" means an employee responsible for assessing, managing, or addressing risk of critical safety incidents.

(3) "Critical safety incident" has the same meaning as provided in R.S. 51:3112, except that the term applies to a foundation model.

B. Prohibited actions. A frontier developer shall not adopt, enforce, or enter into any policy or contract that prevents a covered employee from, or retaliates against a covered employee for, making a protected disclosure pursuant to this Section, or disclosing information to the attorney general, a federal authority, a supervisor, or another covered employee who has authority to investigate, discover, or correct the reported issue, if the covered employee has reasonable cause to believe that the information discloses that the frontier developer's activities pose a specific and substantial danger to the public's

health or safety resulting in a catastrophic risk, including risks to critical infrastructure, or that the frontier developer has violated R.S. 51:3111.2 or R.S. 51:3111.3.

C. A frontier developer shall provide, to all covered employees, a clear notice of their rights pursuant to this Section by as follows:

(1) Posting and displaying, at all times, within any workplace maintained by the frontier developer, a notice of rights to all covered employees', to ensure that any new or remote covered employee receives equivalent notice.

(2) Providing annual, written notice to each covered employee of their rights under this Section, to be acknowledged by each covered employee.

D. Reporting process.

(1) A large frontier developer shall provide an anonymous, internal process for covered employees to disclose, in good faith, information to the large frontier developer which indicates specific and substantial danger to the public's health or safety resulting in a catastrophic risk or a violation of R.S. 51:3111.2 or R.S. 51:3111.3. The process shall include a monthly update, to the covered employee, regarding the status of the large frontier developer's investigation of the disclosure and the actions being taken by the large frontier developer in response to the disclosure.

(2) The disclosures and responses of the process pursuant to this Subsection shall be shared with the officers and directors of the large frontier developer on a quarterly basis, unless the officer or director is the subject of the disclosure.

E. In a civil action pursuant to this Section, once it has been demonstrated by a preponderance of the evidence that a proscribed activity contributed to the alleged prohibited action by the covered employee, the frontier developer shall prove, by clear and convincing evidence, that the action occurred for legitimate, independent reasons.

F. A covered employee aggrieved by a violation of this Section may bring

a civil action to a court of competent jurisdiction for appropriate temporary, preliminary, or permanent injunctive relief. The court shall consider harm from the violation and any chilling effect on other covered employees. The court may award reasonable attorney fees to the prevailing plaintiff.

Section 2. This Act shall become effective on January 1, 2027.

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 474 Original 2026 Regular Session Miller

Proposed law provides for the Protecting Louisiana's Infrastructure from Artificial Intelligence Risk Act.

Proposed law define the terms, "affiliate", "artificial intelligence model", "catastrophic risk", "critical infrastructure", "critical safety incident", "deploy", "department", "foundation model", "frontier AI framework", "frontier developer", "frontier model", "knowledge distillation", "large frontier developer", "model weight", and "property".

Proposed law requires a large frontier AI developer to write, implement, comply with, and publicly publish on its website a frontier AI framework that applies to the large frontier developer's frontier models and describes, in detail, how the large frontier developer approaches governing the development and deployment of frontier models.

Proposed law requires a large frontier AI developer to review and update its frontier AI framework annually. Further requires that any material modification to the framework be published on the developer's website within 30 days, along with a justification for the modification.

Proposed law requires a frontier developer to publish a transparency report on its website before or at the time of deploying a new or substantially modified frontier model, including the model's release date, languages, output modalities, intended uses, restrictions, and a method to contact the developer.

Proposed law requires large frontier developers to include summaries of catastrophic risk assessments, including cybersecurity and biochemical risks, the results of those assessments, the involvement of third-party evaluators, and other steps taken to comply with the frontier AI framework. Provides that publication of this information in a system card or model card satisfies the requirement.

Proposed law requires a large frontier AI developer to provide the department with a summary of any catastrophic risk assessments related to the internal use of its frontier models at least every three months or according to another reasonable schedule communicated to the department.

Proposed law prohibits a frontier developer from making any materially false or misleading statements regarding catastrophic risk, the management of such risk, or compliance with its frontier AI framework, unless the statement was made in good faith and reasonable under the circumstances.

Proposed law requires a large frontier AI developer, beginning July 1, 2028, and annually thereafter, to retain an independent third-party auditor to assess compliance with its frontier AI framework and identify any material deviations from the framework. Prohibits a third-party auditor with a financial interest in the developer, from conducting the audit and requires the developer to publish a high-level summary of the audit findings on its website within 30 days of receiving the report.

Proposed law requires a large frontier AI developer, within twelve months after publishing its frontier AI framework and annually thereafter, to submit a written certification to the department stating whether the developer complied with its framework during the prior year or disclosing any material deviations and corrective actions taken or planned.

Proposed law authorizes a frontier developer to redact information from documents published in order to protect trade secrets or cybersecurity, public health and safety, national security, or to comply with federal or state law. Requires the developer to describe the nature and justification of any redactions in the published document and to retain the unredacted information for five years.

Proposed law requires the department to establish a mechanism for frontier developers or the public to report critical safety incidents involving frontier AI models. Further requires reports to include the date of the incident, the reasons it qualifies as a critical safety incident, a description of the incident, whether it involved internal model use, and whether it posed risks to energy, health care, or port infrastructure.

Proposed law requires the department to establish a confidential mechanism for large frontier developers to submit summaries of assessments of potential catastrophic risks from internal use of frontier models. Further requires the department to limit access to such reports to personnel with a need to know and to take precautions to prevent unauthorized disclosure.

Proposed law requires a frontier developer to report any critical safety incident involving its frontier models to the department within 15 days of discovery. Further requires reporting within 24 hours if the incident poses an imminent risk of death, serious injury, or an active cyberattack on critical infrastructure and allows amended reports when additional information becomes available.

Proposed law requires the department to review critical safety incident reports submitted by frontier developers and authorizes the department to review reports submitted by the public.

Proposed law authorizes the department to transmit critical safety incident reports and certain employee reports to the legislature, the governor, and appropriate state or federal agencies.

Proposed law requires the department, beginning July 1, 2028, and annually thereafter, to produce anonymized and aggregated reports on critical safety incidents and employee reports and to submit those reports to the president of the Senate, the speaker of the House of Representatives, and the governor, while protecting trade secrets, cybersecurity, public safety, and national security information.

Proposed law authorizes the department to designate federal laws, regulations, or guidance that impose substantially equivalent or stricter standards for critical safety incident reporting. Further provides that a frontier developer that declares its intent to comply with the designated federal requirements is considered in compliance with proposed law, until revoked by the frontier developer. Failure to meet requirements constitutes a violation and requires the department to revoke a designation if the standards are no longer satisfied.

Proposed law provides that certain records, including certifications submitted by frontier AI developers, critical safety incident reports, catastrophic risk assessment reports from the internal model use, and covered employee reports, are confidential and exempt from Public Records Laws. Further provides that this exemption is subject to legislative review and will terminate on July 1, 2031.

Proposed law requires the department, in consultation with the Governor's office of Homeland Security and Emergency Preparedness, to annually assess developments related to frontier artificial intelligence and recommend whether updates to the definitions of "frontier model", "frontier developer", and "large frontier developer" are necessary to reflect technological advancements and accepted standards, beginning July 1, 2028.

Proposed law requires the department, when making recommendations to consider federal or international standards for catastrophic risk management, evolving cybersecurity threats to critical infrastructure, developments in AI related biochemical weapon risks, stakeholder input including critical infrastructure operators, and factors related to the scope and verifiability of coverage determinations. Further requires the department to submit its recommendations to the legislature.

Proposed law provides that a large frontier AI developer is subject to civil penalties for failing to comply with requirements of proposed law, which shall not exceed $1,000,000 for first violation and $10,000,000 for a subsequent violation of the same requirement and authorizes enforcement by the attorney general. Further provides that frontier developers operating in this state are subject to the jurisdiction of state courts and clarifies that loss of equity value does not constitute damage to property under proposed law.

Proposed law preempts any rule, regulation, code, ordinance, or other law adopted by a parish, municipality, or other local governmental entity on or after July 1, 2027, relating to the regulation of frontier AI developers and their management of catastrophic risk.

Proposed law establishes whistleblower protection for covered employees of frontier AI developers who report catastrophic risks or violations related to frontier artificial intelligence systems.

Proposed law prohibits retaliation against covered employees who disclose safety concerns to supervisors or appropriate authorities and requires developers to provide notice of these protections and establish an anonymous internal reporting process.

Proposed law establishes a burden of proof standard in civil actions and authorizes courts to grant injunctive relief and award reasonable attorney fees to prevailing plaintiffs.

Effective January 1, 2027.

(Adds R.S. 51:3111-3111.9)