

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. 51:3111.1-3111.9)