

Illinois enacts frontier AI law requiring annual independent audits from 2028

Source copy kept by wheresthe.ai for the story "Illinois enacts frontier AI law requiring annual independent audits from 2028" (<https://wheresthe.ai/d/us-il-sb315-ai-safety-measures-act-2026-07/>).

Source: <https://www.hunton.com/privacy-and-cybersecurity-law-blog/illinois-governor-signs-frontier-ai-model-law>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: 0d2d43f310b5d0b068e030306b02685b41c9e4d930dfb90fbeb198722f5063a

Illinois Governor Signs Frontier AI Model Law

5 Minute Read July 17, 2026

Categories: U.S. State Law , Information Security On July 6, 2026, Illinois Governor JB Pritzker signed Senate Bill 315 , the Artificial Intelligence Safety Measures Act (the "Act"), into law, making Illinois the third state, after California and New York, to enact comprehensive safety and transparency requirements for developers of the largest AI systems. The Act positions Illinois as an aggressive player in the fast-growing patchwork of state-level AI regulation, and notably goes further than similar statutes in one key respect: it is the first in the nation to mandate annual independent third-party audits of covered developers' safety practices.

The Act, certain provisions of which start to become effective on January 1, 2027, passed the General Assembly with bipartisan support and drew backing from both AI safety advocates and industry players.

Who Is Covered

The Act applies to "frontier developers," defined as companies that train AI models using more than 10^{26} integer or floating-point operations of computing power, with the most substantial obligations reserved for "large frontier developers," defined as frontier developers (together with affiliates) with more than \$500 million in annual gross revenue in the preceding calendar year.

Key Obligations

Frontier AI Framework : Beginning January 1, 2028, large frontier developers must publish and maintain a "frontier AI framework" describing how:

The large frontier developer incorporates relevant national and international best standards and industry practices into its frontier AI framework;

It defines and evaluates thresholds, including any tiered thresholds, for determining whether a frontier model could pose catastrophic risk;

It applies mitigations based on those assessments;

It reviews both the assessments and the adequacy of mitigations when deciding whether to deploy a model or use it extensively internally;

It uses independent third parties to evaluate catastrophic risks and the effectiveness of mitigations;

It revisits and updates the framework over time, including what triggers updates and how it determines when a frontier model has been substantially modified enough to require renewed review;

It implements cybersecurity practices to protect unreleased model weights from unauthorized modification or transfer by internal or external parties;

It identifies and responds to critical safety incidents;

It institutes internal governance practices to ensure implementation of these processes;

It assesses and manages catastrophic risk arising from internal use of its frontier models, including risks that a model could circumvent oversight mechanisms.

Frameworks must be reviewed at least annually, with material updates published within 30 days.

Transparency Reports: Before, or concurrently with, deploying a new or substantially modified frontier model, developers must publish a transparency report covering, among other requirements, intended uses, supported languages and modalities, and points of contact. Large frontier developers must also summarize their catastrophic-risk assessments and the extent of third-party involvement in those assessments.

Independent Audits: Starting in 2028, large frontier developers must retain independent third parties to annually audit compliance. Audit reports, summarized and appropriately redacted, must be published and shared with the Illinois Emergency Management Agency and Office of Homeland Security (the “Agency”) and the Illinois Attorney General.

Critical Safety Incident Reporting: Developers must report “critical safety incidents,” including harm resulting from the materialization of a catastrophic risk or if, outside a controlled test, the frontier model uses deception against its developer to evade oversight or controls in a way that shows a materially higher risk of catastrophic harm. Reports must be made to the Agency and Attorney General within 72 hours of learning facts sufficient to establish a reasonable belief that such an incident occurred, or within 24 hours if the incident poses an imminent risk of death or serious injury.

Whistleblower and Internal Reporting Protections: The Act bars developers from contractually or otherwise preventing, or retaliating against, “covered employees” that report safety concerns or violations of the Act to regulators, and requires large frontier developers to maintain an anonymous internal reporting channel with monthly status updates to the reporting employee.

Disclosure and Registration: Beginning January 1, 2027, large frontier developers must file an annual disclosure statement with the Agency. Disclosures must cover corporate identity, ownership, and points of contact, and developers must pay associated fees before developing, deploying or operating a frontier model in Illinois.

Internal Use Risk Reporting : A large frontier developer must provide the Agency with a summary of any assessment of catastrophic risk arising from internal use of its frontier models every three months (or on another reasonable schedule the developer submits in writing to the Agency and the Attorney General and the Agency accepts), with written updates as appropriate.

False or Misleading Statements : A frontier developer shall not make a materially false or misleading statement about catastrophic risk from its frontier models or about its management of catastrophic risk. A large frontier developer also may not make a materially false or misleading statement about its implementation of, or compliance with, its frontier AI framework.

Enforcement : The Attorney General has exclusive authority to bring civil enforcement actions. Violations, including false or misleading statements about catastrophic risk, failure to conduct required audits or failure to report critical safety incidents carry civil penalties of up to \$1 million for a first violation and up to \$3 million for subsequent violations. The Act does not create a private right of action.

Implications for AI Developers : Companies developing frontier-scale models should begin evaluating whether they meet the Act’s revenue and compute thresholds in advance of the Act’s effective date. Given the law’s alignment with, and expansion upon, similar frameworks in California and New York, multistate developers may find it efficient to build compliance programs designed around the strictest common denominator across all three regimes, particularly the audit and incident-reporting timelines.

Tags: Artificial Intelligence (AI) , California , Illinois , New York