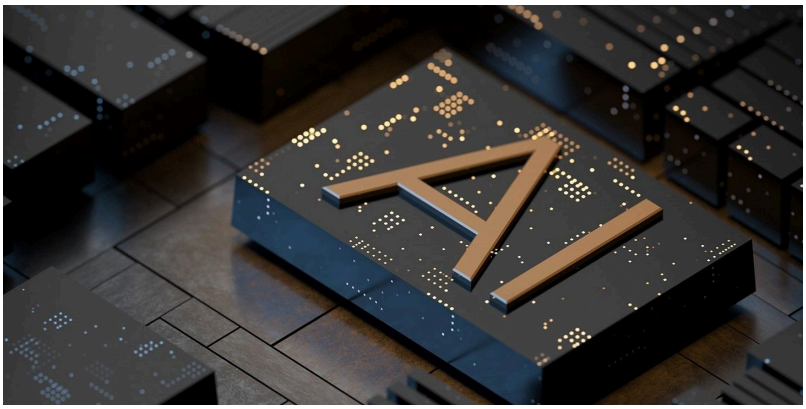

Illinois Enacts AI Safety and Transparency Law for Frontier AI Developers

ALERTS
July 17, 2026

On July 6, 2026, Illinois Governor JB Pritzker signed into law Senate Bill 315, the Artificial Intelligence Safety Measures Act (AISMA), which will require large AI developers to publicly disclose how they plan to mitigate potentially "catastrophic risks" posed by advanced frontier AI models. In a first for a U.S. state AI law, AISMA also requires covered entities to retain independent auditors to assess their compliance. The Illinois legislature otherwise largely modeled AISMA after California's Transparency in Frontier Artificial Intelligence Act (TFAIA) (discussed in a prior alert) and New York's Responsible AI Safety and Education Act (RAISE Act). AISMA's provisions will become effective in two waves, with most provisions effective January 1, 2027, and AI framework and independent audit provisions effective January 1, 2028.

What Is Similar to California's TFAIA and New York's RAISE Act?

AISMA's core substantive obligations closely track California's TFAIA and New York's RAISE Act:

- *Covered developers.* Most requirements apply to "large frontier developers," meaning those that train frontier models using computing power exceeding 10^{26} integer or floating-point operations and had, together with their affiliates, $500 million in annual gross revenue in the preceding calendar year.
- *AI safety framework.* As under both other laws, large frontier developers must adopt, comply with, and publicly publish a framework describing how they identify, assess, and mitigate "catastrophic risks" from their frontier models and must review or update it at least annually.
- *Transparency reports.* Frontier developers must publish model-level transparency reports before or upon deploying a new or substantially modified frontier model.
- *Incident reporting.* As under New York's RAISE Act, critical safety incidents must be reported to the Illinois Emergency Management Agency and Office of Homeland Security (IEMA-OHS) and the Illinois Attorney General (AG) within 72 hours. Separately, if an incident poses an imminent risk of death or serious physical injury, the developer must disclose it within 24 hours to an appropriate authority with jurisdiction.
- *Internal-use reporting.* All three laws require quarterly (or otherwise agreed) transmission of any assessments of "catastrophic risk" resulting from internal use of frontier models to the designated agency.
- *Prohibited statements.* Similar to California's and New York's laws, AISMA prohibits materially false or misleading statements about catastrophic risks or framework compliance, subject to a good-faith exemption.
- *Penalties.* AISMA imposes civil penalties of up to $1 million for a first violation and up to $3 million for subsequent violations depending on severity, plus $1,000-per-day fines for failing to file or correct disclosure statements. This structure mimics New York's RAISE Act.

CONTRIBUTORS


Maneesha Mithal


Eddie Holman


Malcolm Yeary

- *Whistleblower protections.* AISMA bars retaliation against covered employees who report catastrophic risks or violations and requires developers to notify employees of their rights. Large frontier developers must also maintain anonymous internal reporting channels and give monthly status updates. These provisions closely track California's TFAIA. (Note that Connecticut's recently enacted SB 5, the Connecticut Artificial Intelligence Responsibility and Transparency Act, also adopts comparable protections on the same California template, using identical 10^{26}-operation and $500 million thresholds, with anti-retaliation effective October 1, 2026, and anonymous reporting channels required by January 1, 2027.)
- *No private right of action.* AISMA is enforceable only by the AG and expressly disclaims any private right of action. New York's RAISE Act contains the same express bar. California's TFAIA likewise reserves civil-penalty enforcement to the state's AG but includes no comparable express disclaimer, and its whistleblower provisions separately authorize covered employees to bring private retaliation actions, including injunctive relief and recovery of attorney's fees.

What's New in Illinois' AISMA?

Third-party audits. For the first time in the U.S., large frontier developers will be required to annually retain a third party to perform an independent audit of compliance with AISMA's AI framework requirements, beginning January 1, 2028, or 90 days after a developer first qualifies as a large frontier developer, whichever is later. The developer must provide the auditor access to all materials reasonably necessary to complete the audit, including unredacted versions of materials published under the law, though the developer may impose other protective security and confidentiality protocols. The resulting audit report must address whether the developer substantially complied with the law, identify any material deviations and recommended improvements, assess the developer's internal controls, and describe the auditor's methodology and conflicts procedures. Large frontier developers must retain the unredacted report for as long as the relevant frontier model is deployed plus five years and, within 30 days of receiving the report, publish a high-level summary and an appropriately redacted copy of the report on their website and transmit the redacted report to the IEMA-OHS and the AG.

Machine-readable report summaries. AISMA requires the "catastrophic risk" assessment summaries in large frontier developers' transparency reports to be provided in a machine-readable format, a formatting mandate not imposed by California's TFAIA or New York's RAISE Act.

Federal safe harbor and interoperability. AISMA includes a federal interoperability and safe-harbor mechanism that is broader than its analogues. Whereas New York's and California's safe harbors cover only incident reporting, Illinois requires a qualifying federal standard to also match its "catastrophic risk" assessment and independent third-party audit obligations. Once a developer declares its intent to rely on a designated federal standard, it is deemed compliant only to the extent it complies with that standard. Conversely, its failure to meet the designated standard is itself a violation of AISMA.

How Does This Law Interact with Federal Policy on AI Safety?

Illinois' AISMA remains broader and more burdensome than what the Trump administration appears to want from the states, particularly given its first-in-the-nation independent audit mandate. Whether that tension will draw a federal challenge, however, is far from clear given the White House's recent and evolving posture toward AI.

Last month, on June 2, 2026, President Trump issued the Executive Order (EO), Promoting Advanced Artificial Intelligence Innovation and Security. It directs the Departments of the Treasury, War, and Homeland Security, as well as the National Security Agency, Cybersecurity and Infrastructure Security Agency, and the Office of the Attorney General, to take a more active role with respect to the risks posed by AI (discussed in a prior alert). The EO is consistent with the administration's preference for voluntary engagement with the private sector and its policy of promoting AI innovation and managing the related risks without imposing "overly burdensome regulation." Although there has been no federal challenge of California's TFAIA and New York's RAISE Act, Illinois' AISMA may be more exposed than other AI safety laws because of the annual third-party audit requirement.

Wilson Sonsini routinely helps companies navigate complex issues pertaining to AI and Machine Learning. For more information or advice concerning AI development or practices, please contact Maneesha Mithal, Eddie Holman, Malcolm Yeary, or any member of the firm's Data, Privacy, and Cybersecurity practice.