

Illinois SB 315

Artificial Intelligence Safety Measures Act

Signed July 6, 2026 — Effective January 1, 2027

Overview

On July 6, 2026, Illinois Governor JB Pritzker signed [Senate Bill 315, the Artificial Intelligence Safety Measures Act](#), into law, making Illinois the first state in the nation to mandate independent safety audits of the most powerful AI developers. The legislation passed the Illinois House 110–0 and the Senate with near-unanimous support, reflecting rare bipartisan consensus on the need for accountability guardrails on frontier AI systems before Congress establishes a national standard.

The law targets “large frontier developers” meaning companies with annual gross revenues exceeding **\$500 million** that train AI models using more than 10^{26} computing operations. In practice, this captures the largest AI labs in the country, including OpenAI and Anthropic, both of which supported the bill throughout its legislative process. Notably, the law is explicitly designed to interoperate with equivalent federal law when Congress acts, allowing developers to satisfy Illinois requirements by complying with a designated federal framework.

Key Requirements

The Act creates a layered compliance framework for large frontier developers operating in Illinois, with obligations beginning in 2027 and scaling through 2028:

Requirement	What It Requires	Deadline
Frontier AI Framework	Publish a documented framework describing how the developer assesses catastrophic risks, applies mitigations, uses third-party evaluators, secures model weights, and governs internal AI use. Must be updated at least annually; material changes published within 30 days.	January 1, 2028
Disclosure Statement + Fee	File a disclosure statement with IEMA identifying the developer, business addresses, ownership structure, and designated contacts. Renewed annually or upon material change. Failure: \$1,000/day civil penalty.	January 1, 2027
Transparency Report	Publish a transparency report before or concurrent with deploying any new or substantially modified frontier model. Must include model capabilities, intended uses, restrictions, and, for large developer, summaries of catastrophic risk assessments.	Before each model deployment
Independent Annual Audit	Retain a qualified, independent third party to audit compliance with the Frontier AI Framework. Auditor must have no financial interest in the developer. Summary and redacted report published within 30 days; transmitted to IEMA and AG.	Annually, beginning Jan. 1, 2028
Critical Safety Incident Reporting	Report any critical safety incident to IEMA and the AG within 72 hours of learning of it. If imminent risk of death or serious injury, report within 24 hours to appropriate law enforcement or public safety authority.	Ongoing (effective Jan. 1, 2027)

Civil penalties for non-compliance are up to \$1,000,000 for a first violation and up to \$3,000,000 per subsequent violation, enforced exclusively by the Illinois Attorney General. The Act does not create a private right of action.

Timeline

- July 6, 2026:** Governor Pritzker signs SB 315 into law.
- January 1, 2027:** Act takes effect. Large frontier developers must have a current disclosure statement filed with IEMA. Critical safety incident reporting obligations begin.

- **January 1, 2028:** Frontier AI Framework publication requirement and annual third-party audit requirement take effect. Quarterly catastrophic risk summary submissions to IEMA begin.
- **January 1, 2029:** IEMA and AG must publish first annual report on critical safety incidents and frontier model safety developments.
- **Ongoing:** Transparency reports required before or concurrent with each new frontier model deployment. Material changes to Frontier AI Framework must be published within 30 days.

What Does This Mean for Government?

For Illinois state government and agencies, SB 315 creates both new oversight functions and new technology procurement considerations:

- **IEMA as the AI regulatory hub:** The Illinois Emergency Management Agency and Office of Homeland Security becomes the primary regulator under this Act, receiving disclosure statements, incident reports, quarterly risk summaries, and audit reports. IEMA must build out a new regulatory infrastructure to manage this volume of highly technical information.
- **Attorney General enforcement:** The AG gains exclusive enforcement authority over civil penalties and must work with IEMA to review critical safety incident reports, issue annual public reports, and maintain developer disclosure registries.
- **Public sector AI procurement signal:** State and local agencies purchasing AI tools from covered developers can now expect those vendors to carry transparency reports and published frontier AI frameworks, creating new due diligence expectations for government procurement officers evaluating AI vendors.
- **Federal interoperability pathway:** The Act explicitly allows developers to satisfy Illinois requirements by complying with a designated equivalent federal standard, meaning if Congress acts, this law harmonizes automatically. Illinois agencies should monitor IEMA's website for designated federal frameworks.

What Does This Mean for Industry?

For technology vendors, AI developers, and solution providers operating in or selling to Illinois, SB 315 creates both compliance obligations and market opportunities:

- **Compliance infrastructure is now a product category:** The Act mandates annual third-party audits, internal governance programs, whistleblower systems, and machine-readable transparency reports. Vendors offering AI governance platforms, compliance tooling, audit services, and risk assessment frameworks have a direct new market driven by regulatory mandate.
- **Third-party auditor market emerges:** The law requires independent, qualified auditors with demonstrated AI safety expertise, and prohibits financial conflicts of interest between auditor and developer. This creates a new professional services category: AI safety auditing firms with technical frontier model expertise.
- **Model cards and system cards satisfy transparency requirements:** The Act explicitly states that developers who publish transparency disclosures as part of a larger system card or model card are deemed compliant, integrating with existing industry practices rather than requiring entirely new reporting infrastructure.
- **State-level patchwork risk:** Illinois joins New York (RAISE Act, June 2025) and California (Transparency in Frontier AI Act, September 2025) in enacting frontier AI oversight. Developers operating across multiple states face a growing compliance matrix, creating demand for unified AI governance platforms that can manage multi-state regulatory requirements from a single framework.
- **Cybersecurity for model weights:** The Act specifically requires large frontier developers to maintain cybersecurity practices to secure unreleased model weights against unauthorized modification or transfer, creating explicit procurement demand for advanced data loss prevention, access control, and insider threat detection tools scoped to AI development environments.