

Illinois Artificial Intelligence Safety Measures Act Creates New Compliance Obligations for Frontier AI Developers

August 27, 2026

Authors

[Melissa K. Ventrone](#) , [Lauren M. Williams](#)

On July 6, 2026, Illinois enacted the [Artificial Intelligence Safety Measures Act](#) (the “Act”). The Act establishes a comprehensive governance framework for developers of the most advanced AI models. While the requirements may mirror recently enacted laws in California and New York, Illinois goes further by mandating annual independent third-party audits for certain developers in addition to its safety and transparency obligations. Companies that fall under the jurisdiction of the Act should begin assessing governance, documentation, and risk-management programs in advance of the Act’s phased implementation.

The Act takes effect in phases beginning January 1, 2027, although many of its most significant obligations, including the adoption of a frontier AI framework and annual independent third-party audits, do not take effect until January 1, 2028.

Who is Covered?

The Act applies to “frontier developers,” defined as companies that train or initiate the training of a “frontier model.” A frontier model is a general-purpose AI model trained using more than 10^{26} floating-point operations, a metric commonly used to measure the number of operations used to train an AI model. The Act also creates a narrower category of “large frontier developers,” defined as frontier developers that, together with their affiliates, generated more than \$500 million in annual gross revenue in the preceding calendar year. While certain requirements apply to all frontier developers, the Act reserves many of its most substantial governance and oversight obligations for large frontier developers.

The Act may apply to developers outside Illinois if they develop, deploy, or operate frontier models in Illinois.

Requirements for Frontier Developers

- **Transparency Reports.** Before or at the time a new or substantially modified frontier model is deployed, frontier developers must publish a transparency report containing basic information about the model. This includes the model's release date, supported languages and types of output, intended uses, applicable restrictions or conditions on its use, and a contact mechanism and website for the developer.
- **Critical Safety Incident Reporting.** Frontier developers must report "critical safety incidents" involving their models to the Illinois Emergency Management Agency and Office of Homeland Security (the "Agency") and the Illinois Attorney General within 72 hours of learning facts sufficient to establish a reasonable belief that an incident occurred. This reporting deadline shortens to 24 hours if the incident poses an imminent risk of death or serious injury. Covered incidents include harm resulting from catastrophic risk, loss of control of a frontier model causing death or injury, unauthorized access to or modification of the model weights, or a frontier model that "uses deceptive techniques" to undermine the developer's control and increases catastrophic risk. The Act defines "catastrophic risk" to include foreseeable and material risks that a model will lead to the death or injury of more than 50 people, cause more than \$1 billion in property damage, provide "expert-level" assistance in creating a weapon of mass destruction, engage in conduct without meaningful human oversight, or evade the control of the developer or user.
- **Whistleblower Protections.** The Act prohibits frontier developers from preventing or retaliating against "covered employees" who report potential violations of the Act or safety concerns. Frontier developers must also notify covered employees in monthly status updates and maintain an anonymous internal reporting channel.
- **False or Misleading Statements.** Frontier developers shall not make a materially false or misleading statement about catastrophic risk from its frontier models or about its management of catastrophic risk.

Additional Requirements for Large Frontier Developers

Large frontier developers are subject to the requirements above, along with additional obligations.

- **Frontier AI Frameworks.** Beginning January 1, 2028, large frontier developers must develop, implement, comply with, and publicly post a "frontier AI framework" describing how they assess, identify, and respond to catastrophic risks associated with their models. The framework must address risk mitigation measures, adoption of national, international, and industry standards, use of third-party evaluators, cybersecurity protections for unreleased model weights, internal governance, and

accountability mechanisms. The framework must be reviewed at least annually, and any material modifications must be published within 30 days.

- **Additional Transparency Reporting.** Large frontier developers must include additional information in the transparency reports required of all frontier developers. This includes summaries and results of their catastrophic risk assessments, the involvement of third-party evaluators, and steps taken to comply with their frontier AI framework. Notably, large frontier developers may not make materially false or misleading statements about their implementation of, or compliance with, their frontier AI framework.
- **Internal Use Risk Reporting.** Large frontier developers 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.
- **Annual Independent Third-Party Audits.** Beginning January 1, 2028 (or within 90 days after becoming a large frontier developer), large frontier developers must retain an independent third-party to conduct annual compliance audits. The audit must assess substantial compliance with the Act and internal controls. Auditors must have demonstrated frontier-model safety expertise and be independent and free from financial conflicts. A high-level summary and a redacted audit report must be publicly posted and submitted to the Agency and Illinois Attorney General within 30 days after receipt.
- **Disclosure and Registration.** Beginning January 1, 2027, large frontier developers may not develop, deploy, or operate a frontier model, in whole or in part, in Illinois without maintaining a current disclosure statement with the Agency and paying the required fees. The required disclosures must include corporate identity information, Illinois offices, certain ownership interests, and designated governmental contracts. The filing must be renewed annually and when certain material changes occur. If a large frontier developer develops, deploys, or operates a frontier model in Illinois without a current disclosure statement, submits false information in a filing, or fails to pay required assessments, the Agency may impose penalties of \$1,000 per day and may recover unpaid assessments and fees. A limited “safe harbor” applies to statements made in good faith and reasonable under the circumstances.

Enforcement and Penalties

The Illinois Attorney General has exclusive authority to enforce the Act, and there is no private right of action. Large frontier developers may face civil penalties of up to \$1 million for a first violation and up to \$3 million for each subsequent violation for failing to publish or submit required reports or disclosures, making prohibited false or misleading statements about catastrophic risk, failing to obtain required independent audits, or failing to report critical safety incidents.

Notably, enforcement is tied not only to the Act’s requirements, but also to compliance with a developer’s published frontier AI framework, potentially exposing companies to liability when their

practices diverge from their published commitments.

Implications for AI Developers

As Illinois joins California and New York in regulating frontier AI models, developers should assess whether existing compliance efforts can be adapted to meet Illinois' new requirements. For large frontier developers, this means that compliance cannot only exist on paper. The policies, procedures, and controls described in a frontier AI framework will need to be implemented in practice and supported by records sufficient to demonstrate compliance during an annual independent third-party audit. Put differently, the audit requirement adds a new level of accountability by shifting from self-reported compliance to independent verification of a developer's safety practices.

If you have questions about AI regulations or need further assistance, contact [Melissa Ventrone](#), [Lauren Williams](#), or the [Clark Hill Data Privacy, Protection & Cybersecurity team](#).

This publication is intended for general informational purposes only and does not constitute legal advice or a solicitation to provide legal services. The information in this publication is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional legal counsel. The views and opinions expressed herein represent those of the individual author(s) only and are not necessarily the views of Clark Hill PLC or Clark Hill Solicitors LLP. Although we attempt to ensure that postings on our website are complete, accurate, and up to date, we assume no responsibility for their completeness, accuracy, or timeliness.



Related Practice Areas

Data Privacy, Protection & Cybersecurity

Related



Legal Updates

SBA Proposes Sweeping Overhaul of Small-Business Size Standards: Prepare for a Shifting Competitive Landscape

The SBA's proposed rule would restructure small business size standards, expand competition, and reshape federal contracting eligibility requirements.

Legal Updates

DHS Proposes \$103,265 Fee for H-1B Cap Petitions

DHS proposes a \$103,265 fee for H-1B cap petitions, shifting immigration system costs to employers and raising concerns over workforce planning impacts.

Legal Updates

NPE Attorney Liable for Defendant's Attorney Fees

Federal Circuit affirms attorney fee award against patent NPE, highlighting how abusive litigation tactics and repeat settlement-driven lawsuits can trigger sanctions.

Also of Interest:

[Empower Your Professional Success](#)

[We Practice The Law As It Should Be: Simply Smarter.](#)

[Other Services](#)



The Clark Hill approach is equally pragmatic and growth-minded, which is why we understand our clients' toughest business challenges. Our multidisciplinary, global team of advisors focuses on smart legal solutions, delivered simply.

[Contact Us](#)

[Policies & Disclaimers](#)

[Client Log-in](#)

[Payments](#)



© 2026 Clark Hill PLC.