

Vital Briefing

Illinois on the verge of enacting nation's toughest "frontier AI" safety law

By *Thomas Long, J.D.*

Both houses of the Illinois legislature have passed a bill that, [according to](#) Governor J.B. Pritzker, would represent "one of the strongest AI safety laws in the nation." The proposed "Artificial Intelligence Safety Measures Act" ([SB 315](#)) would require developers of "large frontier" AI models to assess catastrophic risks, report critical safety incidents, undergo independent third-party audits, and establish whistleblower protections for employees raising safety concerns. Large frontier developers would have to create, implement, publish, and annually update a frontier AI framework addressing catastrophic-risk assessment, mitigations, cybersecurity, internal governance, third-party evaluations, and risks from internal use of frontier models. The bill passed the Illinois Senate by a vote of 52 to 5 on May 21 and passed the state House of

Representatives unanimously on May 27. The governor has said that he intends to sign the bill.

The legislation would require frontier developers to report critical safety incidents to the Illinois Emergency Management Agency (IEMA) and the Office of the Attorney General within 72 hours or within 24 hours if the incident poses an imminent risk of death or serious physical injury. It also directs IEMA and the Office of Homeland Security to set up and administer reporting mechanisms for developers and the public.

The Illinois law, if enacted, would go farther than AI safety laws in California and New York—which require companies to provide information about safety guardrails and to publish incident reports—by mandating independent annual audits to assess compliance.

Key definitions. "Frontier model" is defined as a foundation model that was trained using computing power greater than 10^{26} integer or floating-point operations (FLOPs). This is significantly more computing power than current standard models, including enterprise AI models, although the rapid pace of development will make this figure more standard over time.

A "foundation model" is an AI model that is trained on a broad dataset; designed for generality of output; and adaptable to

a wide range of distinctive tasks. The bill specifies that a "large frontier developer" is a developer of frontier models that has annual gross revenues over \$500 million in the preceding calendar year.

"Frontier AI framework" refers to "documented technical and organizational protocols to manage, assess, and mitigate catastrophic risks."

The measure defines "catastrophic risk" as "a foreseeable and material risk" that could materially contribute to the death of or serious injury to more than 50 people or more than \$1 million in property damage from a single incident involving a frontier model doing any of the following:

1. providing expert-level assistance in the creation or release of a chemical, biological, radiological, or nuclear weapon;
2. engaging in conduct with no meaningful human oversight, intervention, or supervision that is either a cyberattack or, if the conduct had been committed by a human, would constitute the crime of murder, assault, extortion, or theft, including theft by false pretense; or
3. evading the control of its frontier developer or user.

Frontier AI framework. Large frontier developers would have to publish and begin complying with their frontier AI frameworks as of January 1, 2028. The framework must:

If enacted, SB 315 will require frontier AI developers to:

- Publish risk-assessment frameworks
- Comply with transparency requirements
- Subject models to annual third-party audits
- Report critical safety incidents
- File disclosure statements and pay fees

- Describe how the developer incorporates national, international, and industry standards into its development practices;
- Set forth thresholds for identifying catastrophic risks and apply mitigations to them;
- Use third parties to assess the potential for catastrophic risks and the effectiveness of mitigations;
- Establish cybersecurity practices to secure unreleased model weights; and
- Instituting internal governance practices to ensure implementation of these processes.

Transparency requirements. When a frontier developer deploys a new or modified frontier model, it would have to publish a transparency report containing contact information, the model's release date, its intended uses, and other technical details. The report also must include, in summary form, assessments of catastrophic risks and the results of those assessments; the extent to which third-party evaluators were involved; and other steps taken to fulfill the requirements of the frontier AI framework.

Fees. The legislation authorizes IEMA to charge and collect fees from large

frontier developers for the expenses of administering the statute. It provides that each large frontier developer must pay its pro rata share of this cost, as estimated by IEMA, for the current year and any deficit actually incurred in the administration of the statute in previous years.

Enforcement. An [amendment](#) to the legislation adopted before passage clarifies that the measure would create no private right of action. Instead, the law would be exclusively enforced by the attorney general. Violations would be subject to a civil penalty of up to \$1 million for the first violation and up to \$3 million for subsequent violations.

Whistleblower protections. The measure prohibits frontier developers from taking actions to prevent employees from disclosing information to state or federal authorities regarding violations of the statute or what the employee believes to be "specific and substantial danger to the public health or safety resulting from a catastrophic risk."

Support for the legislation. "Power has to be matched with wisdom, transparency and responsibility," [said](#) bill sponsor Senator

Mary Edly-Allen. "This bill is not about stopping innovation, but balancing the great promise of AI with its potential harms."

On May 27, shortly after passage of the bill by the House, Governor J.B. Pritzker indicated that he would sign the measure in a [post](#) on X. "Illinois is leading the nation in holding Big Tech accountable," he said. "As AI systems impact people's lives, we need safeguards in place. I look forward to signing SB 315 and working with the legislature so that AI, when used, is used responsibly." If the governor signs the bill, it will take effect January 1, 2027.

In a LinkedIn [post](#), Chris Lehane, Chief Global Affairs Officer at OpenAI, expressed support for the legislation. "We appreciated the chance to engage with Illinois policymakers as SB 315 took shape, and endorsed the bill before the first committee hearing about it," Lehane said. "The law goes further than other state-level frontier safety measures by requiring mandatory independent third-party audits. Companies developing the most capable AI models should not only have strong safety practices in place, but be accountable for demonstrating that they are following them."