SB3444

LRB104 15770 SPS 28959 b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB3444

Introduced 2/4/2026, by Sen. Bill Cunningham

SYNOPSIS AS INTRODUCED:

New Act

Creates the Artificial Intelligence Safety Act. Provides that a developer of a frontier artificial intelligence model shall not be held liable for critical harms caused by the frontier model if the developer did not intentionally or recklessly cause the critical harms and the developer publishes a safety and security protocol and transparency report on its website. Provides that a developer shall be deemed to have complied with these requirements if the developer: (1) agrees to be bound by safety and security requirements adopted by the European Union; or (2) enters into an agreement with an agency of the federal government that satisfies specified requirements. Sets forth requirements for safety and security protocols and transparency reports. Provides that the Act shall no longer apply if the federal government enacts a law or adopts regulations that establish overlapping requirements for developers of frontier models.

LRB104 15770 SPS 28959 b

A BILL FOR

AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Artificial Intelligence Safety Act.

Section 5. Definitions. In this Act:

"Artificial intelligence model" means an engineered or machine-based component of a system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

"Critical harm" means the death or serious injury of 100 or more people or at least $1,000,000,000 of damages to rights in property caused or materially enabled by a frontier model, through either:

(1) the creation or use of a chemical, biological, radiological, or nuclear weapon; or

(2) engaging in conduct that:

(A) acts with no meaningful human intervention; and

(B) would, if committed by a human, constitute a criminal offense that requires intent, recklessness, or negligence, or the solicitation or aiding and

abetting of such a crime.

"Developer" means a person or organization that has trained, or initiated the training of, at least one frontier model.

"Frontier model" means an artificial intelligence model that: (1) is trained using greater than 10^26 computational operations, such as integer or floating-point operations; or (2) has a compute cost that exceeds $100,000,000.

Section 10. Frontier model transparency.

(a) A developer shall not be held liable for critical harms if the developer did not intentionally or recklessly cause the critical harms and the developer:

(1) published a safety and security protocol on its website that satisfies the requirements of Section 15 and adhered to that safety and security protocol prior to the release of the frontier model;

(2) published a transparency report on its website at the time of the frontier model's release that satisfies the requirements of Section 20.

The requirements of paragraphs (1) and (2) do not apply if the developer does not reasonably foresee any material difference between the frontier model's capabilities or risks of critical harm and a frontier model that was previously evaluated by the developer in a manner substantially similar to this Act.

(b) If a developer has produced a safety and security protocol in a manner substantially similar to this Act, then the developer shall be deemed to have complied with subsection (a) if the developer:

(1) agrees to be bound by the safety and security requirements adopted under Article 56 of the European Union's Artificial Intelligence Act; or

(2) enters into an agreement with an agency of the federal government that:

(A) enables the agency to access the developer's frontier models for the purposes of conducting research and evaluations;

(B) facilitates the evaluation of frontier models, such as an assessment of cyber and biological risks; and

(C) allows for the federal government to release information related to evaluations of frontier models that have been publicly released.

(c) A developer that enters into an agreement with an agency of the federal government under paragraph (2) of subsection (b) shall file a certification with the Attorney General, in a manner prescribed by the Attorney General, attesting that the developer has entered into an agreement that satisfies the requirements of paragraph (2) of subsection (b). It is a violation of this Act to make a materially false or misleading statement, or to omit a material fact, in any

certification submitted under this subsection.

Section 15. Requirements for safety and security protocols.

(a) In order to satisfy the requirements of paragraph (1) of subsection (a) of Section 10, a developer shall create a safety and security protocol that documents a developer's technical and organizational protocols to manage, assess, and mitigate risk of critical harm arising from the use and distribution of its frontier models. It shall include a high-level summary of:

(1) testing procedures that the developer uses to assess risk of a reasonably foreseeable critical harms arising from the deployment of a frontier model;

(2) thresholds used by the developer to identify and assess whether a frontier model poses a critical risk, including:

(A) how the developer will assess whether a threshold has been attained, which may include multiple tiered thresholds; and

(B) an illustrative summary of the potential actions the developer may take if each threshold is attained;

(3) the mitigations that a developer takes to mitigate reasonably foreseeable critical harms and how the developer assesses the effectiveness of those mitigations;

(4) whether and how a developer will use third parties to assess risk of critical harm and capabilities or the effectiveness of mitigations of critical harms;

(5) the developer's cybersecurity practices relating to frontier models and how the developer secures unreleased frontier model weights from unauthorized modification or transfer by internal or external parties;

(6) to the extent that the frontier model is deployed by the developer, a description of how the developer will monitor for critical harm and how a developer would respond; and

(7) the process by which the developer determines when a frontier model presents material new risks such that it should be subject to additional assessments.

(b) A developer may make appropriate redactions to the information required under subsection (a), as necessary, to maintain model security and integrity, trade secrets, and proprietary information.

Section 20. Requirements for transparency reports.

(a) In order to satisfy the requirements of paragraph (2) of subsection (a) of Section 10, a developer shall create a transparency report that:

(1) identifies the frontier model that is the subject of the transparency report; and

(2) provides a summary of the results of assessments

conducted in accordance with the developer's safety and security protocol and the steps taken to address any identified risks.

(b) A developer may make appropriate redactions to the information required under subsection (a), as necessary, to maintain model security and integrity, trade secrets, and proprietary information.

Section 25. Application of the Act.

(a) This Act shall no longer apply if the federal government enacts a law or adopts regulations that establish overlapping requirements for developers of frontier models.

(b) A developer shall be deemed to be in compliance with this Act if the developer is in compliance with another state's substantially similar frontier model safety and security framework.