KPMG

Regulatory Alert

Regulatory Insights

February 2026

State AI Safety Laws: California and New York

KPMG Regulatory Insights:

- ***Landmark Convergence:*** *Though California's TFAIA was the first state law to address potentially catastrophic risks from AI, it is highly notable that the New York governor chose to adopt the bulk of the California provisions to create a "unified benchmark" among the states.*
- ***Large Developers/Models:*** *Currently only a few companies and models may meet the revenue and compute thresholds; these thresholds will be subject to annual evaluation and may be revised based on technology and/or standards developments.*
- ***Unclear Future:*** *Some state AI laws may be challenged/preempted under EO 14365; it is unclear whether the option to defer to federal laws/guidance may alleviate some or all of this risk.*

Late in 2025, California and New York each enacted laws to impose protections for the safe deployment of large "frontier AI models." The laws are similar in that they aim to mitigate catastrophic risks from these powerful models (as defined in the laws) by requiring the developers to publish information about their safety protocols, including risk assessments, and to report critical safety incidents to the state.

California's law, the "*Transparency in Frontier Artificial Intelligence Act*" (TFAIA), was signed by the governor on September 29, 2025, and went into effect January 1, 2026. New York's law, the "*Responsible AI Safety and Education Act*" (RAISE Act), was signed on December 16, 2025, and will go into effect January 1, 2027. This Regulatory Alert focuses on the key similarities and differences between the two laws.

Two additional points are especially notable:

- The White House issued Executive Order 14365, "*Ensuring a National Policy Framework for Artificial Intelligence*," on December 11, 2025. The EO sets forth directives to establish a federal policy framework for AI laws and regulations while limiting regulatory fragmentation and "onerous and excessive" AI laws and regulations across the states that may inhibit innovation (see the related KPMG Regulatory Alert.) It is not yet clear whether the California and New York AI safety laws will be challenged under the provisions of EO 14365.
- The final version of the RAISE Act agreed to by the New York governor differs substantially from the version passed by the New York legislature. In New York, before signing, the governor has the option to negotiate with legislative leaders to make changes, referred to as "chapter amendments," to a bill. The governor then signs the original bill and the "chapter amendments" are subsequently introduced as a separate piece of legislation that implements the changes. In this instance, the negotiated changes to the RAISE Act were designed to align with many of the provisions in California's TFAIA. On January 6, 2026, the legislature introduced NY A 9449 and S 8828 to incorporate the negotiated chapter amendments and they are currently moving through the voting process. The Regulatory Alert is based on the provisions in NY A 9449/S 8828.

Key Provisions & Comparison of CA and NY Laws

Provision	Text	CA TFAIA	NY RAISE Act
Core Requirement	**Frontier AI Framework:** A set of **documented technical and organizational protocols** that a large developer must write, implement, and publish regarding how it will **manage, assess, and mitigate catastrophic risks** (as defined in the law; see "Risk" below).	●	●
Models	The law covers a: — **"Frontier model,"** defined as a **foundation model trained with over 10^{26} operations.** — **"Foundation model"** defined as a model that is ALL of the following: - Trained on a broad data set - Designed for generality of output - Adaptable to a wide range of distinctive tasks.	●	●
Developers	The definition of a "developer" includes: — **"Frontier developer,"** defined as "a person who has trained, or initiated the training of, a frontier model, with respect to which the person has used, or intends to use, at least as much computing power to train the frontier model" as required by the law. — **"Large frontier developer,"** defined as a frontier developer that together with its affiliates had more than **$500 million in annual gross revenue in the preceding year.**	●	●
	Developer **explicitly excludes**: — **Accredited colleges and universities** engaged in **academic research,** — The **Empire AI** consortium or institute as defined in New York law.	✕	●
Risk	**"Catastrophic risk,"** is defined as a foreseeable and material risk that a frontier developer's development, storage, use or deployment of a frontier model will materially contribute to **death of/injury to >50 people, OR >$1 billion in damage** arising from a single incident involving a frontier model that is: 1. **Providing expert-level assistance** for creating or releasing **a chemical, biological, radiological or nuclear weapon** 2. Engaging in **cyberattacks** with **no meaningful human oversight**, or **conduct that would**, if committed by a human, **constitute murder, assault, extortion, or theft, including theft** by false pretenses, 3. **Evading** the **control** of its frontier developer or user.	●	●
Lead State Agency or Agencies	**California:** — Office of Emergency Services (CA OES) for **reporting**. - The CA Attorney General's office may also transmit "reports of critical safety incidents and reports from covered employees." — Department of Technology for **updating definitions**, annually, based on developments in technology and national/international standards. — **CalCompute consortium** for a public cloud initiative that will be created within the CA Government Operations Agency.	●	✕

Provision	Text	CA TFAIA	NY RAISE Act
	New York: — "An office" to be designated within the NY Department of Financial Services tasked with implementation of the RAISE Act, including updating definitions based on developments in technology and national/international standards.	✗	●
Incident Definition	**"Critical Safety Incident,"** defined to include events such as the **unauthorized access to a model's weights that results in death or bodily injury, the materialization of a catastrophic risk, or a model using deceptive techniques to subvert its developer's controls.**	●	●
Incident Reporting	Report "critical safety incidents" to: — The OES within **15 days** — Law enforcement or public safety agencies when incidents pose imminent risk of death or serious injury within **24 hours**.	●	✗
	Report "critical safety incidents" to: — The DFS office within **72 hours** — Law enforcement or public safety agencies when incidents pose imminent risk of death or serious injury within **24 hours injury**.	✗	●
Public Disclosure	Must publish the full **"Frontier AI Framework"** and a **"Transparency Report"** for **each new model**.	●	●
Third-Party Review	— The developer's **Frontier AI Framework must describe its approach to using third parties for risk assessment.** — The **Transparency Report** for a model **must state the extent to which third-party evaluators were involved**.	●	●
Primary Penalties	The state's Attorney General's office may bring a civil action to enforce the law against violations.	●	●
	— Up to **$1 million** per violation.	●	✗
	— Up to **$1 million** for the **first** violation. — Up to **$3 million** for **subsequent** violations.	✗	●
Whistleblower Protections	— Protects **"covered employees," defined as those responsible for assessing, managing, or addressing risk of critical safety incidents**, for reporting to an authority. — Requires an **anonymous internal reporting process**. — **An employee may sue for injunctive relief** and be awarded **reasonable attorney's fees.**	●	✗
Scope	Explicitly applies to **any frontier model developed, deployed, or operating, in whole or in part, within the state.**	●	●
Severability Clause	If any part of the Act is held invalid, the remaining provisions will stay in effect.	●	●

Provision	Text	CA TFAIA	NY RAISE Act
Deference/ Preemption	**Permits frontier developers to comply with federal laws/guidance** regarding critical incident reporting provided the federal laws/guidance are intended to assess, detect, or mitigate catastrophic risk and the requirements for reporting are the same or more stringent than the state law.	●	●
	Preempts local laws or ordinances passed after January 1, 2025, that regulate the same subject.	●	✕
Prohibition of False Statements	Explicitly prohibits developers from making **materially false or misleading statements about risk or compliance.**	●	●
Confidentiality	**Reporting of critical safety incidents and risk assessments** submitted to OES are **exempt from the California Public Records Act to protect trade secrets and public safety.**	●	✕
Annual State Report	**Beginning on January 1 of the year after the law goes into effect, the relevant state office will produce an annual public report containing** anonymized and aggregated information from critical safety incident reports it has reviewed.	●	●
Internal Use Reporting	**Requires large developers to transmit summaries of catastrophic risk assessments** from the internal use of their models to the relevant state office **every three months**.	●	●

●: provision appears in law; ✕: provision does NOT appear in law

For more information, please contact Laura Byerly, John Kemler or Bryan McGowan.

Contact

Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com

Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com