MINTZ

NY Enacts RAISE Act Amid Federal AI Security Push — AI: The Washington Report

February 12, 2026 | Article | By **Bruce D. Sokler**, **Alexander Hecht**, **Erek L. Barron**, **Christian Tamotsu Fjeld**, Nicole Y. Teo

VIEWPOINT TOPICS

- Artificial Intelligence
- AI: The Washington Report
- Antitrust and Federal Regulation
- ML Strategies

RELATED PRACTICES

- Antitrust and Federal Regulation
- Lobbying and Public Policy

RELATED INDUSTRIES

- Artificial Intelligence

Main Points

- On February 3, the Information Technology Industry Council (ITI) convened industry leaders, senior White House officials, and congressional lawmakers in Washington, DC for its technology and policy summit. During the event, White House National Cyber Director Sean Cairncross previewed an upcoming AI security policy framework aimed at embedding cybersecurity protections into US-led AI technology stacks.
- Director Cairncross indicated that the AI security framework is being developed in coordination with the Office of Science and Technology Policy, though no timeline for release was announced.
- At the conference, Director Cairncross mentioned that the "AI security policy framework" will be built to "ensure that security is not viewed as a friction point for innovation, but it is built into that system," reiterating the administration's pro-industry stance on AI. This objective aligns with Pillar II of the **White House AI Action Plan**, which calls for the creation of an AI-focused Information Sharing and Analysis Center linking the Center for AI Standards and Innovation (CAISI) and the Office of the National Cyber Director to support coordinated sharing of AI-related threat intelligence across critical infrastructure sectors.
- On December 19, New York became the second state to enact a targeted regulatory framework for large frontier AI developers, following California's Transparency in Frontier Artificial Intelligence Act (SB 53) in September. New York Governor Kathy Hochul signed the Responsible AI Safety and Education (RAISE) Act into law, imposing new transparency, safety, and incident-reporting obligations on developers of frontier AI models, along with civil penalties enforceable by the New York attorney general.
- The signing of the RAISE Act comes shortly after the December 11 White House Executive Order that indicated support for a "minimally burdensome" federal AI regulatory regime to preempt a patchwork of state AI laws, and called on the Department of Justice (DOJ) to challenge state laws that are deemed to conflict with that policy through its AI Litigation Task Force, as **we've previously written**.
- Although the DOJ AI Litigation Task Force has been established, there has yet to be any public indication that the Task Force has initiated enforcement actions or targeted specific state AI statutes.
- New York's RAISE Act will go into effect on January 1, 2027.

White House National Cyber Director Teases Upcoming AI Security Policy

On February 3, the Information Technology Industry Council (ITI) convened industry leaders, senior White House officials, and congressional lawmakers in Washington, DC for its technology and policy summit, The Intersect, focused on US technology policy and global competitiveness. During the event, White House National Cyber Director Sean Cairncross previewed an upcoming AI security policy framework aimed at embedding cybersecurity protections into US-led AI technology stacks.

Coordination Between ONCD and OSTP on National AI Cyber Strategy

Director Cairncross indicated that the AI security framework is being developed in coordination with the Office of Science and Technology Policy, though no timeline for release was announced. At the conference, Director Cairncross mentioned that the "AI security policy framework" will be built to "ensure that security is not viewed as a friction point for innovation, but it is built into that system," reiterating the administration's pro-industry stance on AI.

Framework Builds on Prior Signals from 2025 Public Appearances

Cairncross has referenced the forthcoming framework in prior public appearances throughout late 2025, including remarks at the Palo Alto Public Sector Ignite Conference and the Aspen Cyber Summit, where he outlined an administration-wide strategy centered on US competitiveness and the growing role of AI in cyber-enabled threats. The proposed framework is expected to advance the administration's broader goal of harmonizing federal cybersecurity policy and strengthening government-industry collaboration.

Renewal of CISA 2015 Reinforces Focus on Cyber Threat Information Sharing

These comments come as Congress renewed the Cybersecurity Information Sharing Act of 2015 (CISA 2015) through September 30, 2026, as part of the spending package signed into law on February 3. CISA 2015 provides liability protections to facilitate information sharing between the public and private sectors on cyber threats and defensive measures, an approach that appears closely aligned with the administration's emerging AI security strategy.

White House Aims to Address Patchwork of Cybersecurity Requirements

The forthcoming framework appears designed to address what the administration has characterized as a "patchwork" of cybersecurity requirements affecting industry. This objective aligns with Pillar II of the **White House AI Action Plan,** which calls for the creation of an AI-focused Information Sharing and Analysis Center linking the Center for AI Standards and Innovation (CAISI) and the Office of the National Cyber Director to support coordinated sharing of AI-related threat intelligence across critical infrastructure sectors.

State AI Laws Drive Momentum for a More Unified Federal Approach

While details remain limited, the goal of the to-be-unveiled five-page national cybersecurity strategy is to unite the "current patchwork of cybersecurity regulations" to reduce the burden on industry. This effort comes as states such as California and New York have enacted transparency- and safety-focused AI laws, including New York's RAISE Act, which reflect ongoing state activity in the absence of a comprehensive federal AI framework.

New York Enacts RAISE Act, Deepening the State Frontier AI Framework

On December 19, New York became the second state to enact a targeted regulatory framework for large frontier AI developers, following California's Transparency in Frontier Artificial Intelligence Act (SB 53) in September. Governor Kathy Hochul signed the Responsible AI Safety and Education (RAISE) Act into law, imposing new transparency, safety, and incident-reporting obligations on developers of frontier AI models, along with civil penalties enforceable by the New York attorney general.

RAISE Act Mirrors Key Elements of California's SB 53, with Notable Narrowing

Like SB 53, the RAISE Act applies not only to publicly deployed models but also to frontier models used exclusively for internal purposes, signaling an intent to regulate development practices themselves, not merely consumer-facing AI applications. The law ultimately adopts SB 53's narrower definition of "large developers," covering companies with more than $500 million in annual revenue, narrowing from earlier proposals that had a broader definition of large developers as those who had spent over $100 million in compute costs to train frontier models. See our **previous newsletter covering California's first-of-its-kind legislation**.

Safety Protocols and Catastrophic?Risk Mitigation Requirements

The New York legislation includes safety protocols and incident reporting for frontier models and imposes fines up to $30 million, enforceable by the attorney general. Large developers must develop, maintain, and publicly disclose safety and security protocols addressing catastrophic risks, defined as incidents involving at least 100 deaths or serious injuries or $1 billion in damages. Required protocols must cover risk mitigation measures, cybersecurity protections, testing procedures, and safeguards designed to prevent unreasonable risks of critical harm. Developers must retain unredacted versions of these materials for the duration of a model's deployment and for five years thereafter, while submitting redacted public versions to the New York attorney general and the Division of Homeland Security and Emergency Services.

Stricter Safety Incident Reporting: New York's 72?Hour Requirement

New York's incident reporting regime is notably more stringent than California's. Developers must report qualifying safety incidents, or even situations where they reasonably believe an incident may have occurred, within 72 hours of discovery, compared to California's 15-day window and higher threshold for confirmed incidents. Enforcement authority rests exclusively with the attorney general, with civil penalties capped at $1 million for a first violation and $3 million for subsequent violations, significantly lower than the legislature's original proposal but broadly aligned with California's framework.

RAISE Diverges from SB 53: Missing Whistleblower Protections and New Governance Structure

Despite its close alignment, the RAISE Act is not an exact copy of SB 53. Unlike the Californian law, there are no whistleblower protections that are the cornerstones of SB 53, likely reflecting New York's reliance on existing state whistleblower statutes. At the same time, RAISE goes further institutionally by creating a new Office of Digital Innovation, Governance, Integrity, and Trust (DIGIT), housed within the Department of Financial Services. DIGIT will receive company reports, assess fees on covered developers, issue implementing regulations, and publish annual AI safety reports, centralizing AI oversight within the state in a way California did not.

RAISE also explicitly attempts to mitigate duplicative compliance burdens. Borrowing from SB 53, the law allows New York regulators to deem certain federal standards equivalent to state transparency requirements, enabling companies to satisfy state obligations by complying with a designated federal rule if one emerges.

Federal Preemption and the Emerging State Consensus

New York Governor Kathy Hochul's signing of the RAISE Act comes shortly after the December 11 White House Executive Order that support for a "minimally burdensome" federal AI regulatory regime to preempt a patchwork of state AI laws, and called on Department of Justice (DOJ) to challenge state laws that are deemed to conflict with that policy through its AI Litigation Task Force, as **we've previously written**. As the only concrete example, the EO cites Colorado's **Artificial Intelligence Act (SB 24-205)** as one that, in the administration's view, departs from its preferred deregulatory approach to AI oversight. Perhaps notably, the final EO omits the **California-specific SB 53** reference included in the leaked initial draft.

Colorado's Consumer?Focused AI Act Draws Federal Attention

Colorado's AI Act illustrates why it may have drawn scrutiny: unlike New York's RAISE Act and California's SB 53, which focus on transparency, safety, and governance of frontier models, Colorado's law is narrowly tailored toward consumer protection and mitigating discriminatory impacts in AI-assisted decision-making. Colorado's narrower, consumer-focused scope may explain why it was called out in the December EO, particularly in the context of the Trump administration's broader "Anti-Woke AI" agenda, as specified in the AI Action Plan and the July EO on "**Preventing Woke AI in the Federal Government**," which signals a desire to limit state measures perceived as embedding social policy considerations into AI oversight. By contrast, RAISE and SB 53 adopt a model-centered and safety-driven regulatory framework, which may be less vulnerable to federal pushback, particularly given the December EO's carve-outs that preserve certain state law categories, such as child safety protections, from preemption.

Federal Preemption Faces Legal and Statutory Constraints

Nevertheless, absent legislation from Congress, federal agencies face significant legal constraints in displacing state requirements on AI, particularly given the lack of clear statutory authority outside narrow measures like the **TAKE IT DOWN Act**, which criminalizes the publication of non-consensual intimate imagery (NCII), including AI-generated deepfakes. It remains uncertain whether laws, like New York's RAISE Act, that focus on transparency and safety requirements, will become primary targets of federal preemption, despite the EO's scrutiny of state AI legislation.

States Move Toward a Shared Frontier AI Framework

With California and New York now aligned around a transparency-driven frontier AI framework, early signs point toward an emerging state-level consensus rather than a patchwork of irreconcilable rules. Similar proposals are already surfacing in other states, such as Utah's Artificial Intelligence Policy Act (UAIPA) and its 2025 amendments (SB 226, HB 452).

Uncertainty Around DOJ's AI Litigation Task Force

While the DOJ AI Litigation Task Force has been established, per an internal memo circulated within the Justice Department, there has yet to be any public indication that the Task Force has initiated enforcement actions or targeted specific state AI statutes, leaving questions about how aggressively the Department intends to pursue AI-related litigation in the near term. New York's RAISE Act will go into effect on January 1, 2027.

Authors

Bruce D. Sokler, Member / Co-Chair, Antitrust Practice

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, ML Strategies - Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Erek L. Barron, Member / Chair, Crisis Management and Strategic Response Practice

Erek L. Barron, a Member at Mintz, is a nationally respected former United States Attorney and seasoned litigator with more than two decades of experience handling complex criminal, civil, and regulatory matters, including leading significant white collar crime, cybercrime, and national security cases.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Nicole Y. Teo

Nicole Y. Teo is a Mintz Senior Project Analyst based in Washington, DC.