POLSINELLI

Publications

November 25, 2025 • Updates

White House Draft EO Targets State AI Laws as New EO Emphasizes Security

Key Takeaways

- **White House draft EO proposes overriding state AI laws with a uniform national standard.** A leaked executive order targets over 1,000 state-level AI bills, including laws in California and Colorado, and calls for a centralized federal approach to AI governance.
- **The draft EO signals a potential shift toward federal preemption of state consumer protection laws**. If implemented, it could limit states' ability to regulate AI, disrupt existing compliance strategies and create new litigation exposure for developers and deployers.
- **Organizations should assess AI governance policies and prepare for evolving federal enforcement.** Review internal protocols for alignment with likely federal standards, monitor preemption risks and consider how the Genesis Mission's security directives may impact partnerships.

Last Tuesday, a draft executive order (EO) from the White House overriding states' artificial intelligence (AI) laws was leaked. The draft EO was a surprise, considering that a moratorium on state AI laws was voted down 99-1 by the U.S. Senate on July 1, and the White House then said on July 10 that the federal government would not interfere with states' rights if they pass "prudent AI laws."

While the White House stated last week that another AI-related EO was only speculation, the leaked draft EO raises several issues for AI governance — the combination of principles, laws and policies that relate to AI's development and deployment — and the extent to which states' rights may eventually be challenged or allowed.

Yesterday, the White House pivoted from the draft EO to issue a fact sheet to "accelerate AI for scientific discovery" and an EO launching the Genesis Mission, an integrated platform designed to harness datasets for AI-accelerated innovation. The new EO includes directives to combine efforts with the private sector and incorporate security standards.

Related People

- Romaine C. Marshall
- Pavel (Pasha) A. Sternberg
- Spencer R. Wood
- Jennifer Bauer

Related Capabilities

- Artificial Intelligence & Machine Learning
- Privacy & Cybersecurity
- US State Privacy Laws
- Executive Orders

Draft EO Claims 1,000+ State AI Bills Threaten Innovation

The draft EO reiterates the AI Action Plan edict that "national security demands that we win this [AI] race" and asserts that state legislatures have introduced over 1,000 AI bills that threaten to undermine the country's innovative culture. The draft declares that the White House "will act to ensure that there is a minimally burdensome national standard — not 50 discordant state ones."

Of the more than "1,000 AI bills" the draft EO threatens to override, it calls out two consumer privacy AI laws — California's Transparency in Frontier Artificial Intelligence Act (i.e., Senate Bill 53) and the Colorado AI Act (CAIA) — as introducing "catastrophic risk" and "differential treatment or impact" standards that hinder innovation.

For context, California's Senate Bill 53 covers large frontier models and developers and includes detailed governance and transparency requirements. Covered entities, for example, must outline how they identify, assess and mitigate catastrophic risks and describe how they will integrate national/international standards and best practices.

As explained more fully here, CAIA requires that deployers and developers meet certain criteria to ensure they understand what is required to protect consumers from known or foreseeable risks. In addition to a risk management policy and program, covered entities must complete impact assessments at least annually and in some instances within 90 days of a change to an AI system.

Proposed AI Litigation Task Force Would Target State-Specific Rules

The draft EO outlines how the California and Colorado consumer privacy laws would be challenged by an "AI Litigation Task Force" overseen by the U.S. Attorney General, focused on eliminating:

- Subjective safety standards that hinder necessary AI development;
- Patchworks of laws that force compliance with the lowest common denominator;
- Restrictive states from dictating AI policy at the expense of America's innovation and global leadership (i.e., "domination"); and
- Initiatives that are not aligned with a uniform national AI policy framework.

The draft EO outlines an evaluation process of state laws to be conducted by the Secretary of Commerce, the Special Advisor for AI and Crypto and others. Reports would then be published that address "onerous" state laws — those requiring AI models to alter truthful outputs or compelling AI developers or deployers to disclose information in violation of free speech rights.

The draft EO also outlines a process by which the Federal Trade Commission would explain the circumstances under which state laws are preempted by the FTC Act's prohibition on engaging in deceptive acts or practices affecting commerce.

As with prior executive orders, the draft EO states that federal funding could be withheld for continuing to effectuate or enforce a state law that is deemed noncompliant.

New Executive Order Launches Genesis Mission with Cybersecurity Mandates

Notably, the Genesis Mission EO places a strong emphasis on security standards. The EO directs the Secretary of Energy, in operating the platform, to meet security requirements consistent with its national security and competitiveness mission, including

supply chain security and federal cybersecurity standards and best practices.

The EO also sets strict data access, cybersecurity and governance requirements for datasets, models and computing environments used in collaboration with nongovernment and private sector organizations, including measures requiring compliance with classification, privacy and export-control requirements.

That security baseline matters. The EO aims to train scientific foundation models and AI agents while aligning American scientists and businesses — efforts that demand incident response planning, risk assessments and robust security programs.

Draft and New EOs Reflect Growing Threat of Agentic AI

Organizations analyzing AI's impacts have recently noted a surge in AI-enabled incidents. A recent cyberthreat snapshot by the House Committee on Homeland Security reported that one in six data breaches in 2025 involved AI-driven cyberattacks. A database tracking and detailing AI-enabled incidents across multiple industries and jurisdictions is up to incident No. 1275.

In its annual threat-hunting report, CrowdStrike revealed that AI-powered social engineering attacks through voice phishing are likely to double by year-end. CrowdStrike also reported that 320-plus organizations were infiltrated by a single AI-enabled threat actor this year, doubling last year's total.

These figures only tell part of the story about what's coming. Two weeks ago, the *Wall Street Journal* reported how hackers from China jail-broke code belonging to AI frontier model Claude and were able to automate 80-90% of multiple, multi-stage cyberattacks. As a result, 30 organizations were subjected to a wide variety of attacks.

These examples illustrate the Institute for AI Policy's recent conclusion that "[a]s AI systems become more powerful and widespread, the probability of crisis scenarios increases while the complexity of required responses grows." A new era of attacks by Agentic AI is also imminent, including permission escalation, hallucination or memory manipulation attacks and multi-agent attacks.

Action Steps for Aligning with Emerging Federal AI Standards

As the White House signals a more centralized approach to AI oversight, organizations should take stock now — especially those operating in states with active AI laws like California and Colorado. We have previously provided recommendations that organizations should consider to mitigate risks associated with AI, both holistic and specific, emphasizing data collection practices.

Additional steps to consider include:

- Review existing AI governance policies for alignment with emerging federal standards;
- Prepare for potential preemption challenges to the California and Colorado laws; and
- Monitor the Genesis Mission security standards as they evolve; and
- Consider how your organization, including its insurance coverage, might be required to adapt.

For questions, please contact the authors of this article, Matt Todd or Taryn Elliott.