POLSINELLI

Publications

December 19, 2025 • Updates

New Executive AI Order Mandates Minimally Burdensome Approach by States

Key Takeaways

- **A new executive order seeks to preempt state AI laws viewed as inconsistent with administration AI policies and establishes a Litigation Task Force to challenge them.**
- **State courts will be a battleground for determining the viability of state laws and establishing new "industry standards" as legal duties for AI technologies.** State AI laws that include safe harbors or mitigation mechanisms, or that are narrowly tailored to specific risks like protecting children, may be acceptable under the new EO.
- **The net effect of the new EO's directives remains to be seen as evaluations and policies are executed, published and potentially challenged** — but a patchwork of laws, regulations and industry standards will likely remain absent Congressional action.

As 2025 winds down, it may be looked back upon as a year where the foundation for laws, regulations and industry standards pertaining to AI governance — the combination of principles, laws and policies that relate to AI's development and deployment — achieved considerable early-stage development. But 2026 will be like no other in this burgeoning area of law.

This year alone, an AI executive order (EO) has been repealed and replaced, an AI Action Plan has been revealed and even more AI EOs have been released. Now, after several weeks of rumors, the EO titled *Ensuring a National Policy Framework for Artificial Intelligence* was ratified and published in mid-December.

This latest EO is toned down from the leaked draft. It removes references to unspecified state AI laws that are "fear-based" but still singles out Colorado's AI Act for potential ideological bias. The new EO's underlying policy is to sustain and enhance "AI dominance through a minimally burdensome national policy framework for AI."

What's Next? Key 2026 Deadlines Under the New AI Executive Order

Related People

- Jennifer Bauer
- Taryn A. Elliott
- Romaine C. Marshall
- Matt A. Todd

Related Capabilities

- Artificial Intelligence & Machine Learning
- Privacy & Cybersecurity
- Executive Orders

By Jan. 11, 2026, an AI Litigation Task Force will be established to challenge state laws that are inconsistent with the new EO's policy. By March 11, 2026, the Secretary of Commerce, the Special Advisor for AI and Crypto and others will publish an evaluation of those state laws in conflict with that policy.

As with prior executive orders, the new EO permits withholding federal funding to states whose AI laws conflict with the new EO's policy. By March 11, 2026, a policy notice specifying the conditions under which states may be eligible for certain types of discretionary funding will be published.

In addition, by March 11, 2026, the Federal Communications Committee is to initiate a proceeding on whether to adopt a federal reporting and disclosure standard for AI models to preempt state AI laws, and the Federal Trade Commission (FTC) is to issue a policy statement explaining which laws requiring alterations to truthful outputs of AI models are preempted.

Looking Back to Move Forward: How Past Guidance May Shape AI Governance

When March rolls around, one of several burning questions will be whether and how organizations should align AI governance with the new EO's evaluations, policy notes and policy statements —in other words, whether the new direction establishes industry standards or best practices that not only support the new EO's "minimally burdensome" policy but also make practical sense.

Setting aside the various bases for challenging the legality of the new EO,[1] there are other data governance contexts that can be looked at to ascertain what legal duties may arise from the New EO. Federal agencies have routinely issued guidance, like policy statements, in the context of healthcare, financial services and consumer protection and could feasibly take this same path to help establish AI governance expectations and best practices.

For example, from 2010-2020, the FTC resolved at least 50 cases involving cybersecurity incidents or data privacy violations and simultaneously released guidance. One such instance was in August 2016, in which the FTC cross-referenced specific cybersecurity standards with cases where organizations failed to implement industry standards, stating that had they done so, they may not have been found liable.[2]

Fast-forward to 2025, and those same cybersecurity standards — the National Institute of Standards and Technology's (NIST) Cybersecurity Framework — are now part of several state statutes and provide safe harbor protection from data breach lawsuits. Similarly, several states have implemented NIST's standards for managing AI risks and providing safe harbor protections.[3]

State Courts as AI Battlegrounds: Litigation Trends Could Define Industry Standards

No matter if, when or how the new EO policies override state AI laws, state courtrooms will still be forums where the public will closely assess and scrutinize companies' use of AI. Already, cases involving AI systems have been filed for issues ranging from chatbot misrepresentations to loss of control to negligent financial decision cases.

Between 2010 and 2020, numerous cases involving cybersecurity incidents were filed alleging purported failures to protect customers' identities. Some of these cases resulted in establishing certain data governance procedures as industry standards, such as cybersecurity incident response plans, risk assessments and security programs.

Fast-forward to 2025 again, and cases alleging harm caused by AI are quickly emerging to once again establish industry standards. For example, in recent cases relating to the use of AI chatbots or companions, there are attempts to establish that warnings about unknown dangers, including warnings about an AI system's risk that it may validate a user's delusional, false or paranoid beliefs, are required. But this rationale would limit the need to heed warnings and personal responsibility to users.

According to the new EO, these standards might be considered onerous — but they are outside the purview of an AI Litigation Task Force, special advisors or federal government agencies and squarely within the purview of courts, juries and other fact-finders.

Readiness for AI's Foreseeable Risks: Practical Steps to Align with the New EO

As recently noted, many of the state AI laws that we have covered in 2025 include recommendations that organizations should consider to mitigate risks associated with AI, both holistic and specific, and emphasize data collection practices. These practices will be further developed throughout the first quarter of 2026, due in part to the new EO.

For now, next steps to consider include:

- Reviewing existing AI governance policies for alignment with existing and emerging federal standards such as the NIST AI RMF, discussed here.
- Consideration of new guidance set forth in NIST's Cybersecurity Framework Profile for AI released this week for public comment.
- Preparing for potential challenges to AI State laws by March 2026, including the AI laws passed in California and Colorado, and considering how your organization, including its insurance coverage, might be required to adapt.

For questions, please contact the authors of this article.

[1] *See, e.g.,* OpenAI's submission to the White House Office of Science and Technology Policy dated March 13, 2025, stating that "Federal preemption over existing or prospective state laws will require an act of Congress."

[2] *See* The NIST Cybersecurity Framework and the FTC, by the FTC's Andrea Arias https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-ftc (last visited December 18, 2025).

[3] *See* AI Risk Management in the United States: Looking Ahead, February 3, 2025.