PUBLICATION

Emerging Federal AI Policy: What To Know and How To Prepare

Authors: Michael J. Halaiko, Alisa L. Chestler, Alexandra P. Moylan
April 01, 2026

Two significant and related developments recently may accelerate the federal government's push to establish a comprehensive national artificial intelligence (AI) governance regime. First, the Trump administration released its National Policy Framework for Artificial Intelligence (the Framework), a set of legislative recommendations that outlines seven core objectives: child protection, community safety, intellectual property, free speech, innovation, workforce development, and federal preemption of state AI laws. Second, U.S. Senator Marsha Blackburn (R-Tenn.) unveiled a section-by-section summary of proposed legislation that would codify President Trump's executive order creating a single federal rulebook for AI (the Act). Together, these two developments represent the most coordinated federal action on AI to date and hold some promise for companies struggling with the increasing number of state legislative activities.

Importantly, businesses should also be aware of key federal deadlines arising from President Trump's December 11, 2025, Executive Order (*Ensuring a National Policy Framework for Artificial Intelligence*), which set in motion several agency actions that will shape the regulatory landscape in the coming months.

For businesses, the stakes are high. AI is embedded across the economy, and both the Framework and the Act would reshape the legal landscape – introducing new liability theories, mandatory bias audits, and transparency obligations. Companies should assess how these proposals may affect their AI compliance and product development strategies.

Overview of the Framework's Stated Objectives

1. Protecting Children and Empowering Parents. The Framework calls on Congress to establish commercially reasonable, privacy-protective age-assurance requirements for AI platforms and services likely to be accessed by minors, including through parental attestation mechanisms. AI platforms accessible to children would be required to implement features that reduce risks of sexual exploitation and self-harm. The Framework directs Congress not to preempt state laws that are generally applicable and designed to protect children, such as prohibitions on AI-generated child sexual abuse material, while at the same time advising against legislation that would create "open-ended liability" and "give rise to excessive litigation."

2. Safeguarding and Strengthening Communities. The Framework also directs Congress to protect residential ratepayers from increased electricity costs arising from new AI data center construction – a position formalized through the Ratepayer Protection Pledge – while simultaneously streamlining federal permitting for AI infrastructure to allow developers to generate on-site and behind-the-meter power. Congress is called upon to augment existing law enforcement tools to combat AI-enabled impersonation scams and fraud targeting vulnerable populations, including senior citizens.

3. Respecting IP Rights/Supporting Creators. The administration takes the position that training AI models on copyrighted material does not violate copyright laws, but "it acknowledges arguments to the contrary exist and therefore supports allowing the Courts to resolve this issue." The Framework proposes that Congress consider enabling collective licensing frameworks, allowing rights holders to negotiate compensation from AI providers without antitrust liability, though without mandating when or whether such licensing is legally

required. Congress is also encouraged to consider establishing a federal framework protecting individuals from the unauthorized distribution or commercial use of AI-generated digital replicas of their voice, likeness, or other identifiable attributes, with carveouts for parody, satire, and news reporting.

4. Preventing Censorship/Protecting Free Speech. The Framework directs Congress to prevent the federal government from "coercing technology providers, including AI providers, to ban, alter, or compel content based on partisan or ideological agendas."

5. Enabling Innovation/Ensuring American Dominance. Perhaps the most commercially significant provision, the Framework calls on Congress to establish regulatory sandboxes for AI applications "to unleash American ingenuity" and further U.S. leadership in AI development and deployment. Congress is encouraged to make federal datasets accessible in AI-ready formats for industry and academia use in model training. The Framework explicitly provides that no new federal AI rulemaking body should be created, and that AI deployment should instead be supported through existing sector-specific regulatory bodies with subject matter expertise and through industry-led standards. Note, as described below, the Act takes a different approach and sets up several new oversight agencies.

6. Educating Americans/Developing an AI-Ready Workforce. The Framework calls for incorporating AI training into existing education programs, expanding federal studies of workforce realignment driven by AI, and bolstering capabilities at land-grant institutions to launch demonstration projects and youth AI development programs.

7. Federal Policy Framework/Preemption. This is arguably the most consequential directive. The Framework expressly calls on Congress to preempt state AI laws that impose "undue burdens," establishing a single, minimally burdensome national standard consistent with the Framework's recommendations. However, the called-for preemption would not extend to: state police powers to enforce generally applicable laws against AI developers and users (including child protection and fraud prevention laws); state zoning laws governing placement of AI infrastructure; or requirements governing a state's own use of AI in procurement or public services.

Key Federal Deadlines from the December 2025 Executive Order

President Trump's December 11, 2025, Executive Order established several near-term deadlines that will shape the federal AI landscape:

- **January 10, 2026:** DOJ AI Litigation Task Force established (completed). The Task Force is charged with challenging state AI laws that conflict with federal policy on grounds including unconstitutional regulation of interstate commerce and federal preemption.

- **March 11, 2026:** Department of Commerce must publish its evaluation of state AI laws identifying "onerous" laws that conflict with federal policy. This evaluation will identify which state laws may be referred to the DOJ Task Force for challenge. No public announcement has been made as of the date of this alert.

- **March 11, 2026:** FTC must issue a policy statement on the application of Section 5 of the FTC Act (unfair and deceptive practices) to AI models, including when state laws requiring alterations to AI outputs may be preempted. No public announcement has been made as of the date of this alert.

- **March 11, 2026:** Commerce Department must issue a BEAD Program Policy Notice specifying that states with "onerous" AI laws may be ineligible for certain broadband funding. No public

announcement has been made as of the date of this alert.

- **90 days after Commerce Department evaluation:** FCC to initiate a proceeding on whether to adopt a federal AI reporting and disclosure standard that would preempt conflicting state laws.

These deadlines create a compressed timeline for federal action. The Commerce Department's evaluation will be particularly significant, as it will identify specific state laws that the administration views as problematic. State laws most likely to face scrutiny include Colorado's AI Act (effective June 30, 2026), which requires reasonable care to prevent algorithmic discrimination; California's SB 53 (Transparency in Frontier AI Act); and New York's RAISE Act (signed December 2025). The Executive Order explicitly criticizes Colorado's law as potentially compelling AI models to "produce false results."

The Trump America AI Act

While the Framework articulates policy goals, Senator Blackburn's Trump America AI Act *would* create the statutory mechanism to implement them. The Act is structured around protecting Senator Blackburn's "4 Cs" – children, creators, conservatives, and communities – and is broader than the Framework in several important respects.

Notably, the Act proposes the following in a new federal law:

- **Title I** of the Act places a statutory duty of care on AI developers in the design, development, and operation of AI platforms to prevent and mitigate foreseeable harm to users – a significant departure from the Framework's more advisory posture. AI platforms would be required to conduct regular risk assessments of how algorithmic systems, engagement mechanics, and data practices contribute to psychological, physical, financial, and exploitative harms. The Federal Trade Commission (FTC) would be empowered to promulgate rules establishing minimum reasonable safeguards.

- **Title VI** requires large frontier developers to draft and implement protocols to manage and mitigate catastrophic risk, publish transparency reports disclosing information about their frontier models, and establish regular reporting to the Department of Energy (DOE).

- **Title IV** would extend protections to users under 17, requiring covered platforms – including social media platforms, video games, messaging applications, and video streaming services – to implement tools and safeguards protecting minors from sex trafficking, suicide, and other abuses. Covered platforms would also be required to notify users when algorithms are in use and permit users to switch to an algorithm that does not rely on user-specific data.

- **Title VII** is among the Act's most consequential provisions from a litigation standpoint, enabling the U.S. Attorney General, state attorneys general, and private actors to bring suit against AI system developers for harms caused by AI systems under theories of defective design, failure to warn, express warranty, and unreasonably dangerous or defective product.

- **Title IX** would establish the Center for Artificial Intelligence Standards and Innovation within the National Institute of Standards and Technology (NIST), charged with developing voluntary best practices for AI system assessments, supporting AI red-teaming and blue-teaming, and coordinating testbeds with allies and international partners.

- **Title X** establishes the National Artificial Intelligence Research Resource (NAIRR), making computing resources, massive datasets, and advanced AI infrastructure available as a shared resource for

students, researchers, non-profits, small businesses, and academic institutions.

- **Title XV** addresses AI training and copyright, clarifying that unauthorized reproduction or computational processing of copyrighted works for AI training, fine-tuning, or development does not constitute fair use. The bill also establishes that AI-generated derivative works produced without authorization of the copyright owner shall be deemed infringing. Title XIII (the TRAIN Act) enables copyright holders to subpoena AI developers for disclosure of training materials used to train generative AI models. These provisions have significant implications for companies using copyrighted content in AI development.

- **Title XII** codifies a version of the NO FAKES Act holding individuals and companies liable for producing unauthorized digital replicas of individuals in performances, and holding platforms liable for hosting such replicas with actual knowledge of their unauthorized nature. First Amendment carve-outs for parody, satire, and news reporting would be preserved.

Among the most important structural differences between the Act and the Framework is the Act's approach to preemption. While the Framework calls on Congress to broadly preempt state AI laws that impose undue burdens on AI development and deployment, Title XVII of the Act takes a different approach, providing that the Act does not preempt any generally applicable law, including state common law and sectoral governance schemes that may address AI. Certain discrete provisions – such as Title VI's preemption of state laws regulating frontier AI developer catastrophic risk management, and Title XII's preemption of state digital replica laws – do provide targeted federal displacement of state law, but the summary of the Act does not appear to provide for general preemption comparable to what the Framework envisions. This divergence is consequential: companies that anticipated relief from state AI compliance burdens should not assume the Act will necessarily deliver the sweeping preemption the Framework contemplates.

Implications for Businesses

The interplay between the Framework and the Act raises critical considerations for organizations developing, deploying, or using AI systems.

Sector-Specific Regulatory Oversight Remains Primary – But New Federal Layers May Be Coming

Existing sector regulators (SEC, DOT, FTC, etc.) remain the primary AI oversight bodies. However, the Act introduces cross-sector federal oversight through the Center for Artificial Intelligence Standards and Innovation (within NIST) and DOE's Advanced AI Evaluation Program, which may layer onto existing regulatory frameworks for companies deploying frontier AI models.

New Liability Exposure Under the Duty of Care and Products Liability Provisions

Title I's duty of care, and Title VII's products liability provisions hold significant importance for businesses. For companies deploying AI in customer-facing applications, decision-making systems, or automated processes, the Act's imposition of a statutory duty to prevent and mitigate foreseeable harm – paired with a federal private right of action for defective design and failure to warn – represents a fundamentally new liability framework that practitioners and compliance officers must integrate into AI governance programs. The availability of defective design and failure-to-warn claims against AI developers signals that Congress may extend traditional tort law frameworks to AI in high-stakes commercial settings. Companies that develop, deploy, or substantially modify AI systems should immediately assess whether their indemnification, quality management, risk disclosure, and AI risk management documentation are robust enough to defend against claims under Title VII.

Copyright and Training Data Transparency Obligations

The Title XV copyright and training data provisions have direct and material implications for businesses across all sectors. Title XV clarifies that unauthorized use of copyrighted works for AI training does not constitute fair use, and AI-generated derivative works may be deemed infringing. Title XIII (the TRAIN Act) empowers copyright holders to subpoena AI developers for disclosure of training materials. Businesses that use AI models trained on licensed content, user-generated data, or proprietary datasets should assess whether their data licensing agreements, terms of service, and content acquisition practices establish adequate authorization for AI training purposes. The ability of copyright holders to compel disclosure of training data creates both compliance and litigation exposure.

Mandatory Bias Audits for High-Risk AI Systems

The Title VIII bias audit requirement for high-risk AI systems is directly applicable across all industries. AI systems used in employment decisions, credit determinations, insurance eligibility, housing decisions, educational assessments, and other consequential contexts could qualify as high-risk under the Act's definition, subjecting them to regular bias evaluations and mandatory AI ethics training requirements for covered entity personnel.

Preemption Uncertainty and the Complex Jurisdictional Landscape

The Framework's broad preemption approach and the Act's more limited approach create jurisdictional uncertainty. State data privacy laws – including the CCPA, Colorado Privacy Act, and state AI-specific statutes – likely survive under the Act's reservation of generally applicable state law. Companies should conduct careful jurisdictional analyses rather than assuming preemptive relief.

NAIRR as a Research Catalyst

The NAIRR could substantially reduce cost and access barriers for AI research by making computing resources, datasets, and infrastructure available to researchers, non-profits, small businesses, and academic institutions. Companies with research partnerships should monitor NAIRR's governance structure under OSTP and NSF oversight.

Recommended Action Steps for Businesses

In light of the Framework and the Act, businesses developing, deploying, or using AI systems should consider the following priority actions:

1. **Conduct a comprehensive AI training data audit.** Title XV's clarification that unauthorized AI training on copyrighted works does not constitute fair use, combined with Title XIII's subpoena provisions enabling copyright holders to compel disclosure of training materials, creates significant exposure for companies relying on copyrighted content. Companies should immediately audit their data acquisition practices, content licensing agreements, and AI development workflows to assess whether they have adequate authorization for AI training purposes. The ability of copyright holders to subpoena training data records means that unauthorized use may be discovered through litigation, creating material legal risk.

2. **Integrate AI products liability risk into governance and vendor management programs.** Title VII's creation of federal products liability claims against AI developers – and against deployers who substantially modify or misuse AI systems – requires immediate integration into risk management, indemnification, and vendor contracting frameworks. Businesses should review AI vendor agreements for adequate indemnification coverage, strengthen product documentation and safety disclosure practices, and ensure that internal quality systems are sufficient to support a liability

defense. Organizations with existing quality management system (QMS) infrastructure should evaluate whether those systems can be extended to cover AI-specific risks, including algorithmic drift, data integrity, and model validation.

3. **Map and prepare for high-risk AI bias audit obligations.** Title VIII's bias audit requirement will capture many AI systems used in employment, credit, insurance, housing, educational, and other consequential decisions. Organizations should evaluate whether their AI deployments fall within the Act's high-risk definition and begin planning for audit-ready documentation and AI ethics training programs. Given that Title VIII includes political affiliation as a protected characteristic, legal counsel should be involved in designing the audit methodology from the outset.

4. **Do not assume preemption – maintain state compliance programs.** The Act expressly does not preempt generally applicable state law. Until legislation is finalized, state AI obligations remain operative. Organizations should map their state compliance obligations and resist deprioritizing them in anticipation of federal relief.

5. **Engage proactively with sector-specific regulators.** Both the Framework and Act direct AI deployment to be governed through existing regulatory bodies. Businesses should engage with their relevant regulators (SEC, FTC, HHS, DOT, DOL, DOE, etc.) as they develop AI-specific guidance. Early engagement creates an opportunity to shape guidance before it becomes binding.

6. **Leverage the NIST AI RMF as a governance foundation.** The NIST framework's voluntary, outcome-based structure provides a practical compliance foundation consistent with both the Framework's preference for industry-led standards and the Act's Center for Artificial Intelligence Standards and Innovation. Alignment also provides a defensible governance record in the event of regulatory examination or litigation.

7. **Monitor the legislative process and engage early.** Neither the Framework nor the Act is final, and both will change before enactment. Key issues still in flux include preemption scope, training data provisions, private rights of action, and products liability contours. Organizations should engage through trade associations and direct congressional outreach to shape the final text. The Act's 180-day post-enactment effective date leaves a compressed compliance window.

For further analysis tailored to your sector and compliance footprint, please contact the authors – Alisa Chestler, CIPP/US, QTE; Michael Halaiko, CIPP/E; Alexandra Moylan, CIPP/US, AIGP; or another member of Baker Donelson's AI Team.