HOW AI GOVERNANCE IS BEING BUILT IN REAL TIME, AND WHAT COMES NEXT

Date: 26 May 2026

US Policy and Regulatory Alert

By: Marne Marotta, Scott J. Gelbman, Liam J. Row, Guillermo S. Christensen, Finch Fulton, Varun M. Jain, Abby Dinegar

We have seen this pattern before. Washington debates, states move, and Congress eventually responds, often borrowing from what states have already built. Privacy may be heading back down that track, but the federal endpoint remains uncertain. Artificial intelligence (AI) is not waiting. Governance expectations are already hardening through agencies, procurement, standards, and state law, largely outside of Congress.

FEDERAL PREEMPTION WAS THE STRATEGY, BUT EXECUTION IS STILL INCOMPLETE

In December 2025, the Trump Administration issued Executive Order 14365 to halt state-by-state AI regulation and lay the groundwork for federal preemption. The order directed Department of Commerce, within 90 days, to identify and effectively triage “onerous” state AI laws, flagging those that distort “truthful outputs,” burden interstate commerce, or raise constitutional concerns for referral to a newly created AI Litigation Task Force (Task Force). The Department of Justice (DOJ) stood up that Task Force in January 2026, but key pressure points remain stalled, including Commerce's evaluation, the Federal Trade Commission's (FTC) policy statement on AI and “truthful outputs,” and the Federal Communication Commission's (FCC) disclosure-standard proceeding.

The result is familiar: clear federal intent, but incomplete execution. In the meantime, states continue to legislate, including Colorado's high-risk system deployer obligations, Utah's AI disclosure requirements, and Illinois's biometric and employment-related AI laws. For companies, that means ongoing state compliance pressure alongside shifting federal expectations.

THE NATIONAL AI POLICY FRAMEWORK SIGNALS DIRECTION, NOT RELIEF

The March 2026 National AI Policy Framework (Framework) is a four-page coordination document, not a compliance reset. It does not impose obligations, preempt state law, or resolve the hardest liability questions. Instead, it organizes legislative recommendations across seven themes and reinforces a consistent federal posture: preference for national uniformity, reliance on existing agencies rather than a new AI regulator, and skepticism of prescriptive rules that add compliance burden without clear payoff.

Two signals matter for business planning. First, on intellectual property, the Framework reflects the Administration's view that training AI models on copyrighted material does not violate copyright law and favors litigation, not mandatory licensing, to resolve fair-use disputes. Second, it previews the direction of travel for

©2005-2026 K&L Gates LLP. All Rights Reserved.

enforcement and legislation: a focus on demonstrable harms, clearer allocation of responsibility between developers and deployers, resistance to state laws viewed as regulating model development, and treatment of AI as economic and physical infrastructure.

FRONTIER AI AND PRE-MARKET OVERSIGHT

In early May 2026, after previews of Anthropic's Mythos model raised concerns around the speed at which cybersecurity vulnerabilities might be leveraged, reporting indicated that the Administration has been considering executive actions addressing broad cyber security risks from advanced AI, including a pre-deployment vetting regime that would require government clearance before releasing certain frontier models. National Economic Council Director Kevin Hassett publicly compared the concept to an Food and Drug Administration-style review process. At the same time, the National Institute of Standards and Technology's (NIST) Center for AI Standards and Innovation has begun entering voluntary agreements with developers to conduct unclassified evaluations focused on national security risks such as cybersecurity, critical infrastructure, biosecurity, and chemical weapons.

The contemplated executive order could also restrict private-sector efforts to block government use of AI models and tighten contracting and termination standards for federal vendors. If adopted, a clearance-style regime would mark a meaningful shift toward pre-market oversight for certain systems and is a development companies should plan around now, not after the rules are final. But pre-market oversight for frontier models is only one dimension of a broader shift already underway.

FOUR CHANNELS DRIVING AI GOVERNANCE NOW

Even while Congress deliberates, governance expectations are solidifying through four channels:

1. FTC enforcement: Consumer protection law is already being applied to AI claims, including representations about accuracy, business growth, and safety, making substantiation a present-tense issue.
2. Civil rights enforcement: DOJ and Equal Employment Opportunity Commission enforcement turns on outcomes, not intent, and vendor sourcing does not shift responsibility away from deployers.
3. Standards: Frameworks like the NIST AI Risk Management Framework remain voluntary, but increasingly function as a baseline in procurement, diligence, and contracting.
4. Procurement: Federal contracting continues to convert policy into enforceable obligations, which often migrate into broader market expectations.

The through-line is straightforward: operational governance is becoming the price of entry, regardless of whether or when Congress acts.

NEAR TERM LEGISLATIVE VEHICLES

Comprehensive AI legislation remains unlikely in the near term. Instead, Congress appears more inclined toward narrowly targeted bills addressing discrete risks. The TAKE IT DOWN Act (Pub. L. 119-12), which criminalizes the

©2005-2026 K&L Gates LLP. All Rights Reserved.

nonconsensual distribution of AI-generated intimate images, was signed into law in May 2025 with strong bipartisan support, underscoring congressional appetite for focused measures. Other pending proposals follow a similar pattern: the bipartisan CHATBOT Act (H.R. 7985 / S. 4407) and the GUARD Act (S. 3062) target protections for minors, with the GUARD Act advancing out of the Judiciary Committee in May. Taken together, these efforts suggest that near-term legislative movement is more likely to concentrate in specific areas like child safety, transparency, fraud prevention, and government use of AI than to coalesce into a comprehensive regulatory framework.

But targeted bills are not the only legislative strategy taking shape. In April 2026, Reps. Jay Obernolte (R-CA) and Ted Lieu (D-CA) introduced the American Leadership in AI Act (H.R. 8516), a bipartisan legislative package that consolidates more than 20 prior proposals and recommendations from the bipartisan House Task Force on Artificial Intelligence–a separate congressional body chartered by Speaker Johnson and Leader Jeffries to develop guiding principles and policy proposals on AI–into a single framework. The package spans standards and evaluation, research infrastructure, federal adoption and procurement, workforce development, and safeguards against AI enabled harms. Unlike the issue-specific measures described above, the bill represents an attempt to organize fragmented congressional efforts into a more coherent legislative architecture.

Importantly, the proposal does not yet resolve core structural questions, including federal preemption, liability allocation, or the scope of mandatory requirements. Instead, it reflects an emerging congressional strategy: aggregating areas of bipartisan consensus into modular legislation that could serve as a foundation for more comprehensive action over time. While the package is not a near-term compliance driver, it is a meaningful indicator of how Congress may begin to organize a broader AI policy framework.

The incremental approach is also evident in parallel efforts to build a national data-privacy framework. Congress continues to negotiate baseline questions about data rights, profiling, and automated decision-making. The House Republican SECURE Data Act (H.R. 8413) would create opt-out rights for profiling, treat children's data as sensitive, establish a data broker registration regime, and preempt much of state privacy law. It does not include explicit AI provisions, impact assessments, or a private right of action, limiting its immediate utility as an AI governance vehicle even as it reshapes the data-rights landscape. The companion GUARD Financial Data Act (H.R. 8398) would add tailored requirements for financial institutions' use of automated decision-making.

PRACTICAL TAKEAWAYS FOR STAKEHOLDERS

This is a moment to engage deliberately:

- Expect governance to continue forming outside Congress. FTC enforcement, civil rights liability, NIST standards, and federal procurement are already converting policy into operational obligations. If a pre-market clearance regime for frontier models moves forward, it will add a new and significant compliance layer—companies developing or deploying advanced systems should begin scenario-planning now.
- Plan for continued state-law compliance pressure. Executive Order 14365 signaled clear preemption intent, but Commerce's evaluation of state AI laws, the FTC's policy statement, and the FCC's disclosure proceeding remain incomplete. Until federal preemption is operational, obligations under laws like Colorado's deployer requirements, Utah's disclosure rules, and Illinois's biometric and employment-related AI statutes remain in effect.

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Assume privacy and AI governance will keep converging. The SECURE Data Act's profiling opt-out rights, sensitive-data classifications, and data broker registration requirements would reshape the data-rights landscape even without explicit AI provisions. Companies should assess how emerging data-privacy frameworks interact with their AI systems, automated decision-making processes, and vendor relationships.
- Engage early to shape outcomes. Congressional strategy is shifting from one-off bills to modular frameworks like the American Leadership in AI Act, and agency guidance, contract terms, and enforcement positions are hardening quickly. The window to influence standards, preemption scope, and liability allocation is now—not after the rules are final.

BOTTOM LINE

AI governance is not waiting for Congress. Federal preemption remains the stated objective, but execution has lagged—Commerce's evaluation, the FTC's policy statement, and the FCC's disclosure proceeding are all incomplete. In the interim, operational obligations are forming through enforcement, procurement, standards, and state law simultaneously. A pre-market clearance regime for frontier models, if adopted, would add a significant new compliance layer. The American Leadership in AI Act signals that Congress is beginning to organize fragmented efforts into modular frameworks, and the SECURE Data Act could reshape the data-rights landscape in ways that intersect directly with AI governance. Companies should plan for a period in which compliance expectations continue to harden across multiple channels, national security considerations may override pro-innovation defaults, and the window to influence outcomes is narrowing.

Our team is tracking these developments in real time—from frontier AI oversight and federal preemption to state compliance obligations and emerging data privacy frameworks—and translating them into practical guidance. We are happy to discuss how these shifts may affect your AI governance program, data practices, vendor relationships, and regulatory exposure, and what steps you can take now to prepare. Please feel free to reach out for a targeted readiness assessment, a legislative strategy briefing, or a gap analysis.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



MARNE MAROTTA
PARTNER

WASHINGTON, DC
+1.202.778.9202
MARNE.MAROTTA@KLGATES.COM



LIAM J. ROW
GOVERNMENT AFFAIRS ANALYST

WASHINGTON, DC
+1.202.778.9250
LIAM.ROW@KLGATES.COM



FINCH FULTON
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.4565
FINCH.FULTON@KLGATES.COM



ABBY DINEGAR
GOVERNMENT AFFAIRS ANALYST

WASHINGTON, DC
+1.202.778.4562
ABBY.DINEGAR@KLGATES.COM



SCOTT J. GELBMAN
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.9067
SCOTT.GELBMAN@KLGATES.COM



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



VARUN M. JAIN
OF COUNSEL

WASHINGTON, DC
+1.202.778.9030
VARUN.JAIN@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.