White paper

State of AI Governance Regulations in the United States

A Comprehensive Analysis of Federal and State AI Regulatory Developments

March 2026 | Version 1.0

VerifyWise Thought Leadership Series

Executive Summary

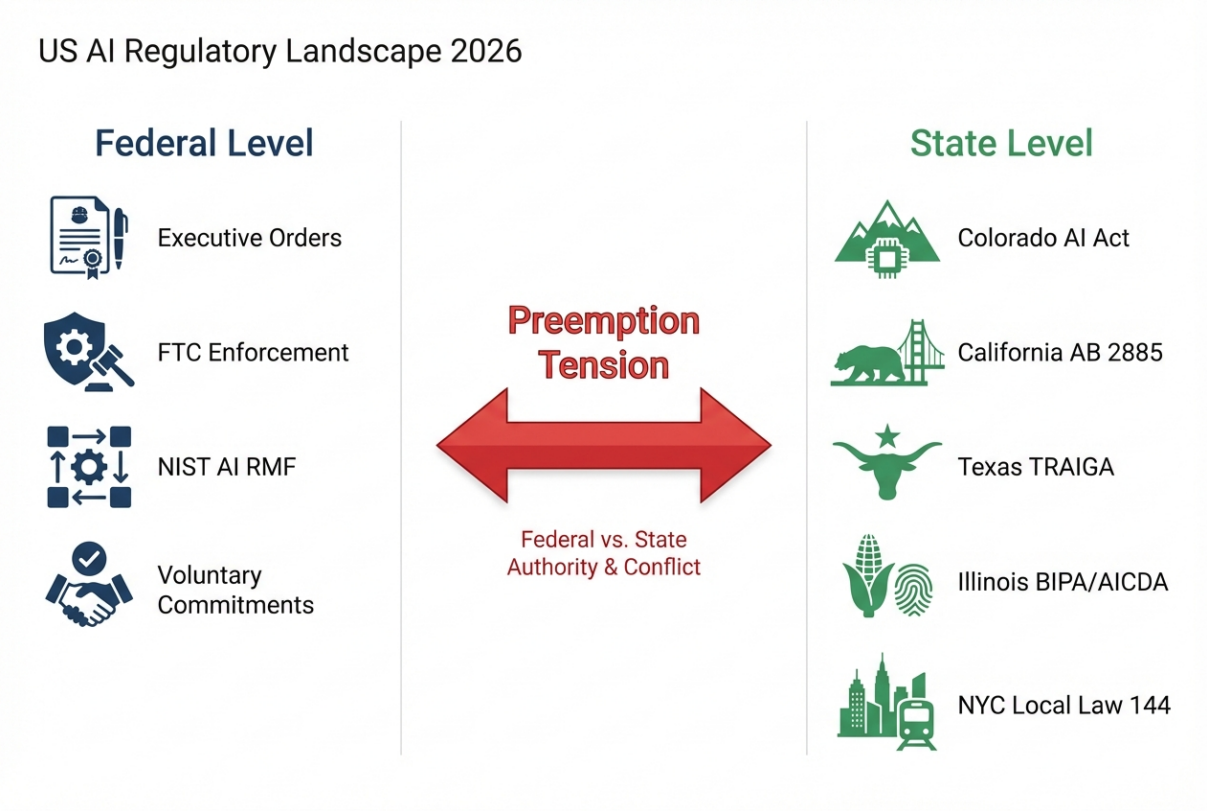

Figure: US AI regulatory landscape showing federal and state level governance

The United States artificial intelligence regulatory landscape in 2026 is defined by a complex and rapidly evolving interplay between federal policy priorities and an expanding patchwork of state-level legislation. Despite the increasingly central role AI plays in the economy, the U.S. still lacks a single comprehensive federal AI law. Instead, regulation has emerged from a combination of executive orders, federal agency enforcement actions under existing statutes, voluntary standards frameworks, and an unprecedented wave of state-level legislation taking effect in 2025 and 2026. This report provides a comprehensive analysis of the current regulatory environment, examining the federal government's deregulatory posture under the Trump administration, the patchwork of state laws that have emerged to fill the regulatory void, the role of voluntary frameworks such as the NIST AI Risk Management Framework, sector-specific enforcement activity by the Federal Trade Commission and other agencies, and the looming confrontation between federal and state authorities over preemption. The analysis is designed to inform compliance planning, strategic decision-making, and product development for organizations operating in the AI governance and compliance space.

The Federal Regulatory Landscape

Absence of Comprehensive Federal AI Legislation

As of March 2026, the United States does not have a comprehensive federal law governing the development, deployment, or use of artificial intelligence. While Congress has considered numerous proposals and held extensive hearings, no omnibus AI legislation has been enacted. Federal AI governance currently relies on a combination of executive orders, agency enforcement under existing consumer protection, civil rights, and sector-specific statutes, and voluntary guidelines and frameworks. This absence stands in sharp contrast to the European Union's AI Act, which represents a binding, comprehensive regulatory framework with tiered risk classifications and enforceable requirements across all member states. The lack of a U.S. federal equivalent has created a fragmented environment where compliance obligations vary significantly by state, sector, and use case.

Trump Administration Executive Orders and Policy Direction

The federal policy direction has shifted significantly since President Trump began his second term in January 2025. The administration has taken a deregulatory approach, revoking Biden-era AI safety requirements and signaling a strong intent to promote AI innovation with minimal regulatory burden.

Executive Order on Removing Barriers to AI Leadership (January 2025)

In January 2025, President Trump signed Executive Order 14179, which revoked the Biden administration's October 2023 executive order on AI safety. The new order directed federal agencies to remove barriers to U.S. AI leadership and update regulatory frameworks to encourage AI adoption rather than constrain it. This represented a fundamental reorientation from the previous administration's risk-focused approach.

Executive Order on National AI Policy Framework (December 2025)

On December 11, 2025, President Trump signed a second major executive order titled "Ensuring a National Policy Framework for Artificial Intelligence." This order represents the most aggressive federal assertion of authority over AI governance to date and establishes several mechanisms to challenge and potentially preempt state AI laws. Key provisions of the December 2025 Executive Order include:

- AI Litigation Task Force: The Attorney General is directed to establish a task force whose sole responsibility is to challenge state AI laws deemed inconsistent with federal policy, including on grounds of unconstitutional regulation of interstate commerce or federal preemption.
- State AI Law Evaluation: The Department of Commerce is directed to evaluate state AI laws that may conflict with federal objectives, including laws that require AI systems to alter truthful outputs or compel reporting that may violate First Amendment protections.
- Federal Funding Conditions: States with AI laws identified as “onerous” may be deemed ineligible for non-deployment funding under the Broadband Equity Access and Deployment (BEAD) program and other discretionary federal grants.
- FTC Guidance: The FTC is directed to issue a policy statement by March 2026 describing how the FTC Act applies to AI and when state laws requiring alteration of truthful outputs are preempted by federal prohibition on deceptive practices.
- FCC Proceedings: The FCC is directed to initiate a proceeding to determine whether to adopt a federal reporting and disclosure standard for AI that would preempt conflicting state requirements.

Carve-Outs from Federal Preemption

The Executive Order identifies specific categories of regulation that are not proposed for preemption. These include regulation of child safety in AI contexts, AI compute and data center infrastructure (except for generally applicable permitting reforms), and state government procurement and use of AI systems. Organizations operating in these areas should assume continued state enforcement authority unless further legal challenges are raised.

State AI Legislation: The Expanding Patchwork

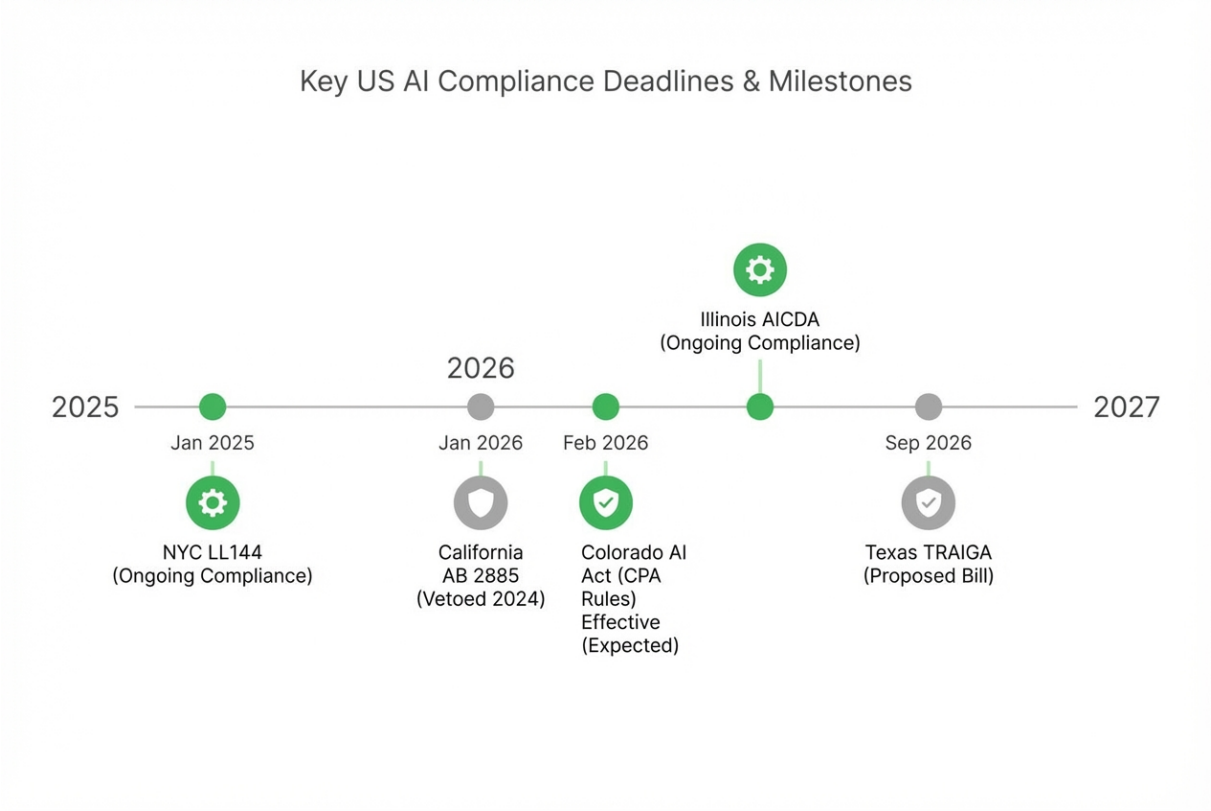

Figure: Key US AI compliance deadlines 2025-2027

In the absence of comprehensive federal guidance, states have emerged as the primary drivers of AI regulation in the United States. The pace of legislative activity has accelerated dramatically, with multiple major state AI laws taking effect on January 1, 2026, and others following throughout the year. This section examines the most significant state-level regulatory developments.

Colorado AI Act

Colorado enacted the most comprehensive state-level AI governance law in the United States, targeting developers and deployers of “high-risk” artificial intelligence systems. The law establishes requirements for risk management, disclosures to consumers, and mitigation of algorithmic discrimination. High-risk AI systems are defined as those that are a substantial factor in making consequential decisions affecting education, employment, essential government services, healthcare, housing, insurance, or legal services. Originally scheduled to take effect on February 1, 2026, implementation was postponed to June 30, 2026. The delay followed significant industry pushback and the formation of a legislative commission to investigate implementation practicalities. The law’s future enforcement may face additional uncertainty given the federal government’s stated intent to challenge state AI laws deemed overly burdensome.

California: A Multi-Layered Compliance Environment

California has enacted the most extensive suite of AI-specific legislation of any state, creating a layered compliance environment with multiple laws taking effect on January 1, 2026. Key measures include:

- Transparency in Frontier AI Act (SB 53): Requires developers of large frontier AI models (trained using more than 10^26 FLOPS) to publish risk frameworks, report critical safety incidents, and implement whistleblower protections. Developers with annual revenue exceeding $500 million face enhanced obligations. Penalties can reach $1 million per violation.
- AI Training Data Transparency Act (AB 2013): Mandates that developers of generative AI systems publish high-level summaries of the datasets used to develop and train their models, including information about data sources, types, intellectual property, personal information, processing details, and relevant dates.
- AI Transparency Act (SB 942): Requires AI providers to disclose when content is AI-generated, including through watermarking and labeling mechanisms.
- AI Safety Act: Establishes whistleblower protections for employees reporting AI-related risks or critical safety concerns and creates the CalCompute public AI cloud consortium.
- Civil Rights Department Regulations: Restricts discriminatory use of AI in employment decisions, effective October 2025.
- CCPA Automated Decision-Making Regulations: Risk assessment requirements took effect January 1, 2026, with full automated decision-making provisions (pre-use notices, consumer opt-outs) scheduled for January 1, 2027.

Texas Responsible AI Governance Act (TRAIGA)

Texas enacted TRAIGA, which took effect on January 1, 2026. Although the original bill was modeled after the more expansive Colorado and EU approaches, the final version was significantly narrowed during the legislative process. The enacted law eliminates many private sector obligations such as impact assessments and consumer disclosures, and limits most compliance obligations to government use of AI. However, TRAIGA still imposes categorical restrictions on the development and deployment of AI systems for certain prohibited purposes, including behavioral manipulation, unlawful discrimination, infringement of constitutional rights, incitement of violence or self-harm, and the production of child sexual abuse material or deepfakes. The law also restricts state government entities from using AI for social scoring or biometric identification without consent, and establishes the Texas Artificial Intelligence Council and a regulatory sandbox program.

Illinois: AI in Employment

Illinois has enacted legislation requiring employers to notify job candidates when AI is used to analyze video interviews. Candidates must provide consent before AI-based evaluation occurs. The law also establishes data retention and destruction requirements, prohibiting employers from retaining AI-analyzed video indefinitely. These provisions took effect in February 2026.

New York City and New York State

New York City's Local Law 144, which requires bias audits for automated employment decision tools, continues as one of the most operationally significant local AI regulations. Building on this foundation, New York State has passed several additional AI-related bills, including the RAISE Act, social media warning requirements for AI-generated content, synthetic performer disclosure requirements, expanded publicity rights protections, and broader government oversight of automated decision tools.

Other Notable State Activity

- Connecticut: Requires AI impact assessments for state agencies deploying AI systems.
- Maryland and New Jersey: Have enacted restrictions on AI use in hiring decisions.
- Utah: Requires disclosure when consumers interact with generative AI and established an AI learning laboratory for regulatory experimentation through a sandbox approach.
- Tennessee: Enacted the ELVIS Act targeting audio deepfakes and voice cloning, the first enacted legislation specifically addressing AI simulation of image, voice, and likeness.

State Law Summary: Key Compliance Deadlines

State	Law / Regulation	Effective Date	Focus Area
Colorado	Colorado AI Act	Jun 30, 2026	High-risk AI governance
California	Frontier AI Act (SB 53)	Jan 1, 2026	Frontier model safety
California	Training Data Transparency (AB 2013)	Jan 1, 2026	Training data disclosure
California	AI Transparency Act (SB 942)	Jan 1, 2026	AI content disclosure
California	CCPA ADM Regulations	Jan 1, 2027	Consumer rights / ADM
Texas	TRAIGA	Jan 1, 2026	Prohibited AI uses / Gov use
Illinois	AI Video Interview Act	Feb 2026	Employment / AI hiring
NYC	Local Law 144	In effect	Bias audits / hiring

Utah	AI Policy Act	In effect	Consumer disclosure

Federal Agency Enforcement

Federal Trade Commission (FTC)

Despite the absence of AI-specific federal legislation, the FTC has been the most active federal agency in AI enforcement, relying on its broad authority under Section 5 of the FTC Act to prohibit unfair or deceptive acts and practices. The agency's approach to AI enforcement has evolved significantly with the change in administration, but enforcement activity has continued on a bipartisan basis.

Operation AI Comply

Launched in September 2024 under the Biden administration, Operation AI Comply targets companies making unsubstantiated or misleading claims about AI-powered products and services. The initiative has continued under the Trump administration, signaling bipartisan consensus that AI marketing claims warrant heightened scrutiny. The FTC has brought multiple enforcement actions against companies engaged in "AI washing" — the practice of making exaggerated claims about AI capabilities. Key enforcement actions include:

- Workado (Content at Scale AI): The FTC found that the company advertised its AI content detection tool as 98 percent accurate, when testing showed it performed at approximately 53 percent accuracy in general settings. A consent order was issued requiring cessation of unsubstantiated claims.
- Air AI Technologies: Sued in August 2025 for allegedly deceptive claims about business growth and earnings potential tied to AI products. The case remains pending.
- Growth Cave: Resolved in January 2026, involving allegations that the company misrepresented its AI software's ability to automate online course operations.
- DoNotPay: Settled in January 2025 for marketing an AI chatbot as "the world's first robot lawyer" without adequate testing or substantiation.

Shift in Enforcement Philosophy Under the Current FTC

The current FTC leadership has signaled a narrower approach to AI enforcement compared to the previous administration. Chairman Andrew Ferguson has emphasized that the agency aims for "circumspect and appropriate enforcement of existing laws to prevent fraudulent conduct" while ensuring consumers benefit from new technologies. Key shifts include:

- Rytr Consent Order Reversal: In December 2025, the FTC voted 2-0 to reopen and set aside its 2024 consent order against Rytr, a generative AI writing tool provider. The Commission found the original complaint did not satisfy Section 5 requirements and that the “means and instrumentalities” theory of liability should not extend to neutral tool providers simply because their tools could potentially be misused.
- Reduced Focus on AI Safety: The agency has deprioritized enforcement actions focused on discriminatory effects of automated decision-making and the use of personal data for model training.
- Continued Focus on Youth Protection: The FTC launched a Section 6(b) inquiry into AI chatbots marketed as companions, issuing orders to multiple firms seeking information about advertising, safety, and data handling practices related to minors.

Other Federal Agency Activity

- Department of the Treasury: In February 2026, Treasury released a sector-specific operational framework for financial services AI risk management, translating NIST AI RMF principles into 230 mapped control objectives. The framework is designed to integrate with existing governance programs.
- Equal Employment Opportunity Commission (EEOC): Continues to apply Title VII of the Civil Rights Act, the ADA, and the ADEA to AI-driven employment decisions, asserting that algorithmic discrimination constitutes unlawful employment practices.
- Consumer Financial Protection Bureau (CFPB): Has issued guidance on the use of AI in consumer financial services, particularly regarding credit decisions and automated underwriting.

Voluntary Frameworks and Standards

NIST AI Risk Management Framework (AI RMF 1.0)

The NIST AI Risk Management Framework, released in January 2023, has become one of the most influential voluntary AI governance frameworks globally. Developed through a collaborative process involving hundreds of stakeholders across academia, industry, and government, the AI RMF provides a structured approach for organizations to identify, assess, mitigate, and monitor AI risks throughout the system lifecycle. The framework is built on four core functions:

- Govern: Establishes organizational structures, policies, accountability, and risk management culture for AI systems.
- Map: Identifies and documents the context, risks, and impacts of AI systems.
- Measure: Assesses and analyzes identified risks using quantitative and qualitative methods.
- Manage: Implements risk treatment, mitigation, and monitoring strategies.

While the AI RMF is voluntary, its influence extends far beyond optional adoption. It is increasingly referenced in state legislation, federal procurement requirements, and international regulatory frameworks. Federal contractors are expected to follow NIST-aligned governance requirements, and the framework is widely used as a technical companion for EU AI Act compliance.

Recent NIST Developments

- Generative AI Profile (NIST-AI-600-1): Released in July 2024, this companion document helps organizations identify risks unique to generative AI systems and proposes aligned risk management actions.
- Cyber AI Profile (NIST IR 8596): A preliminary draft released in December 2025 provides guidelines for using the NIST Cybersecurity Framework 2.0 to manage AI-related cybersecurity risks. The comment period closed January 30, 2026.
- Control Overlays for Securing AI Systems (COSAiS): Under development alongside the Cyber AI Profile to provide implementation-level guidance for AI-related security controls.
- AI RMF 1.1: NIST is expected to release updated guidance addenda, expanded profiles, and more granular evaluation methodologies through 2026.

Industry Voluntary Commitments

In 2023, the White House secured voluntary commitments from leading AI companies to ensure responsible AI development. Initial participants included major technology companies, with additional

firms joining subsequently. These voluntary commitments cover internal and external security testing before public release, information sharing on AI risk management, cybersecurity protections, watermarking of AI-generated content, public reporting on AI system capabilities and limitations, and prioritization of research on societal risks. While these commitments lack enforcement mechanisms, they have influenced industry norms and continue to serve as a baseline expectation for responsible development practices.

The Federal-State Preemption Showdown

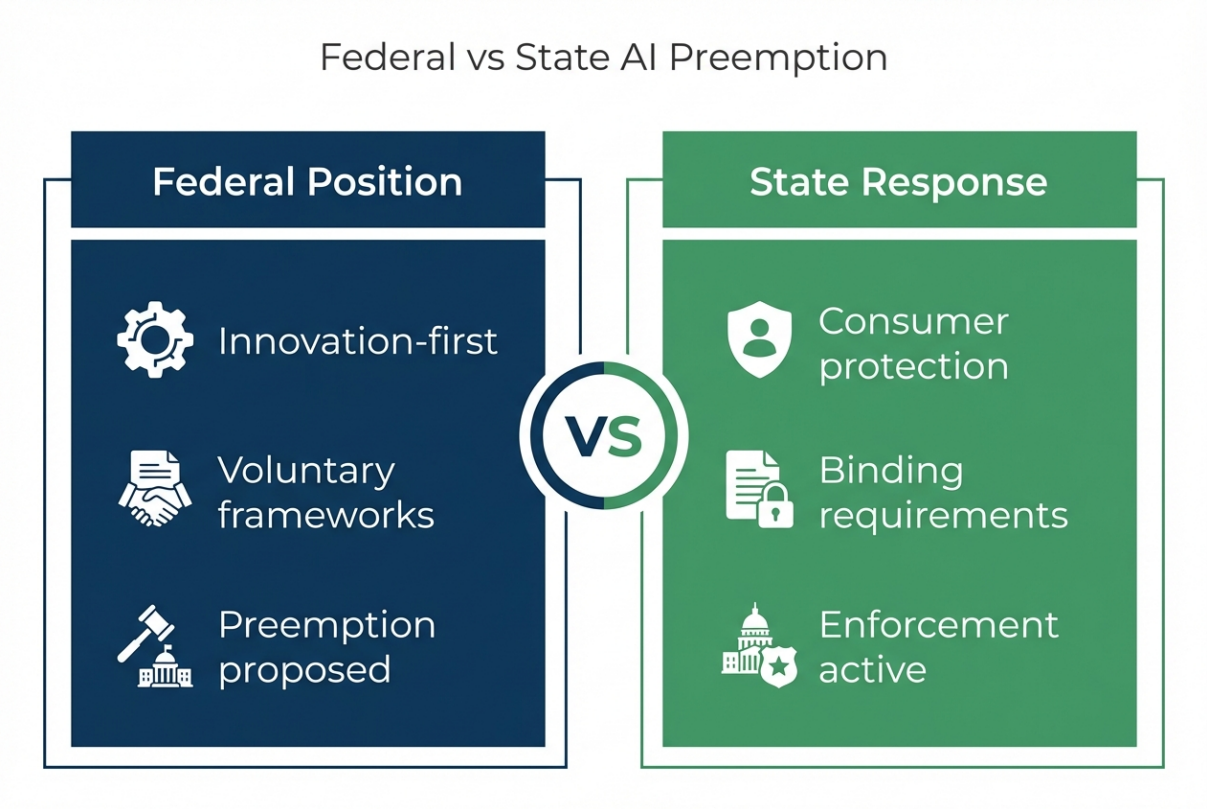

Figure: Federal vs State AI preemption positions

Perhaps the most consequential development in U.S. AI governance is the emerging confrontation between the federal government and the states over regulatory authority. This tension has the potential to fundamentally reshape the compliance landscape for all organizations operating AI systems in the United States.

The Federal Position

The Trump administration has articulated a clear position that state-by-state AI regulation creates unworkable compliance challenges and threatens U.S. competitiveness. The December 2025 Executive Order identifies three primary concerns: that a patchwork of fifty different regulatory regimes makes compliance disproportionately burdensome, particularly for startups; that certain state laws may force AI systems to produce inaccurate results to satisfy anti-discrimination requirements; and that some state laws impermissibly regulate beyond state borders, impinging on interstate commerce.

The State Response

State officials and consumer advocates have responded aggressively, arguing that the Executive Order overreaches on states' traditional police powers and consumer protection authority. Multiple states have signaled their intent to contest the Executive Order's directives and continue enforcement of their AI laws. Importantly, even if specific AI statutes face federal challenges, state attorneys general retain the ability to pursue enforcement actions under generally applicable consumer protection and anti-competition statutes for alleged deceptive, misleading, or discriminatory AI practices.

Congressional Activity

Congress has also entered the debate, with competing proposals reflecting the same federal-state tensions. In May 2025, House Republicans inserted a clause into a tax and spending bill that would have banned state AI laws for ten years. The proposal was met with strong opposition from nonprofit organizations, elected officials, and public policy experts, and ultimately did not advance in that form. The legislative debate continues, with the scope and structure of any eventual federal AI law remaining deeply uncertain.

Sector-Specific Regulatory Considerations

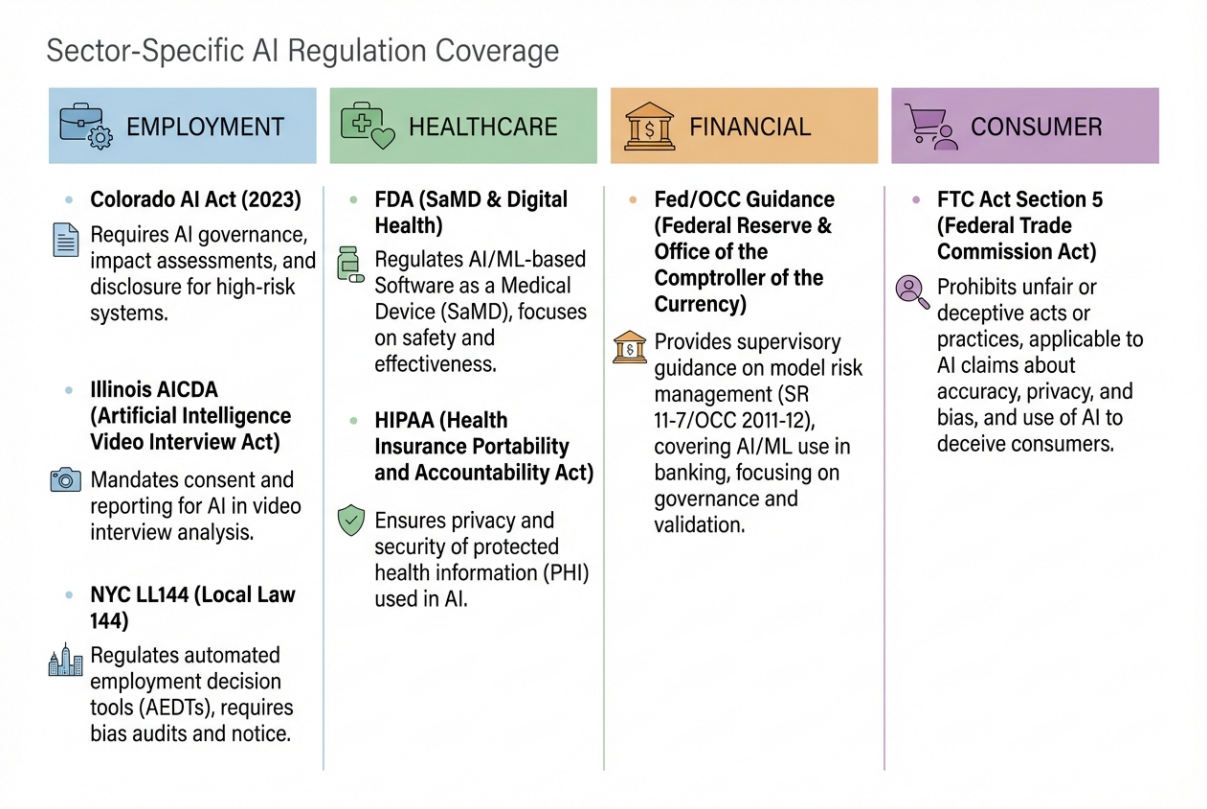

Figure: Sector-specific AI regulation coverage

Employment and Hiring

AI use in employment decisions is one of the most heavily regulated areas. Organizations deploying AI in hiring, promotion, or workforce management must navigate overlapping obligations including NYC Local Law 144's bias audit requirements, Illinois's video interview notification and consent provisions, Maryland and New Jersey restrictions on AI in hiring, California's civil rights department regulations on discriminatory AI use, and federal anti-discrimination statutes (Title VII, ADA, ADEA) as applied to algorithmic decision-making.

Healthcare

California's Health Care Services AI Act requires healthcare providers using generative AI for patient communications to disclose that the communication was generated by AI and to provide instructions for contacting a human provider. Several states are considering additional regulations for AI in clinical decision support, insurance claims processing, and medical device applications.

Financial Services

The financial services sector faces among the most mature regulatory expectations for AI governance. The Treasury Department's February 2026 framework provides 230 control objectives mapping NIST AI RMF principles to operational controls specific to financial institutions. The framework addresses model lifecycle governance, identity resolution, data governance, and integration with existing compliance programs including SOC 2 and the NIST Cybersecurity Framework.

Consumer Protection

Multiple states have enacted or proposed requirements for consumer-facing AI interactions, including chatbot disclosure requirements, safety protocols for high-risk uses involving minors or self-harm, and restrictions on the use of personal data in algorithmic pricing. Utah, Illinois, New York, and California have all adopted varying forms of these requirements.

Looking Ahead: Key Dates and Developments to Watch

Date / Timeframe	Development
March 2026	FTC policy statement on application of FTC Act to AI (directed by December 2025 EO)
March 2026	Commerce Department evaluation of state AI laws that may conflict with federal objectives
May 2026	TAKE IT DOWN Act notice-and-takedown provisions take effect
June 30, 2026	Colorado AI Act implementation begins (delayed from February 2026)
January 2027	California CCPA Automated Decision-Making provisions take full effect
2026 (ongoing)	DOJ AI Litigation Task Force activities and potential challenges to state AI laws
2026 (ongoing)	NIST AI RMF 1.1 addenda, expanded profiles, and evaluation methodologies
2026 (ongoing)	Congressional debate on comprehensive federal AI legislation

Strategic Recommendations for Organizations

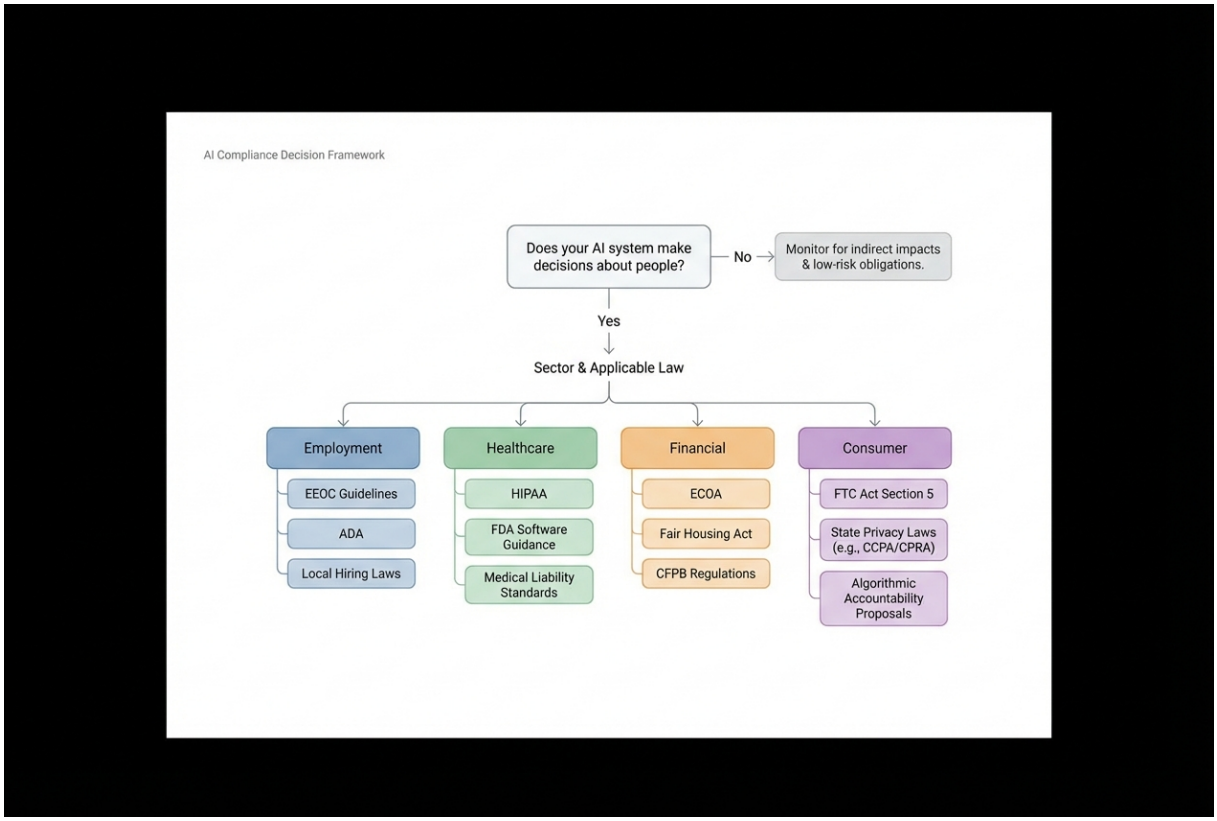

Figure: AI compliance decision framework

Based on the current regulatory landscape, organizations developing, deploying, or governing AI systems should prioritize the following actions:

- Maintain comprehensive AI system inventories: Document all AI systems in use, including ownership, deployment context, risk classification, and governance status. This is increasingly a baseline expectation across multiple state laws and voluntary frameworks.
- Build jurisdiction-aware compliance programs: Map applicable state and federal requirements to each AI system based on where it is developed, deployed, and used. Given the fragmented landscape, organizations cannot rely on a single compliance standard.
- Adopt the NIST AI RMF as an operational foundation: The framework is emerging as the de facto standard for AI risk management in the U.S. and provides a structured approach that aligns with both current state requirements and anticipated federal standards.
- Prepare for federal preemption uncertainty: Develop compliance programs that can adapt quickly to changes. Continue complying with all existing state laws while monitoring DOJ Task Force activities, Commerce Department evaluations, and Congressional developments.
- Implement robust documentation practices: Maintain evidence of risk assessments, bias testing, impact assessments, transparency disclosures, and governance decisions.

Documentation is the common thread across nearly all current and proposed AI regulations.

- Substantiate all AI-related marketing claims: The FTC's bipartisan focus on AI washing means that every claim about AI capabilities, accuracy, or performance must be supported by rigorous, documented evidence.
- Monitor sector-specific developments: Financial services, healthcare, employment, and consumer-facing sectors face the most immediate and specific compliance obligations. Organizations in these sectors should track applicable guidance closely.

Conclusion

The U.S. AI governance landscape in 2026 is characterized by dynamic tension: between federal deregulatory ambitions and aggressive state-level lawmaking, between voluntary frameworks and enforceable mandates, and between the desire to promote innovation and the need to protect consumers and civil rights. For organizations in the AI space, this environment demands proactive governance, comprehensive documentation, and flexible compliance strategies. The absence of a comprehensive federal law does not mean AI is unregulated. Between state statutes, federal agency enforcement under existing authorities, and the growing influence of voluntary standards like the NIST AI RMF, organizations face a complex web of obligations that will only continue to expand. The organizations best positioned to navigate this landscape will be those that treat AI governance not as a compliance burden but as a strategic capability — one that builds trust with customers, regulators, and stakeholders alike.

Disclaimer: This report is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel regarding specific compliance obligations. Information is current as of March 2026 and is subject to change as the regulatory environment continues to evolve.

References

[1] The White House. “Ensuring a National Policy Framework for Artificial Intelligence.” Executive Order, December 11, 2025. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

[2] Baker Botts LLP. “U.S. Artificial Intelligence Law Update: Navigating the Evolving State and Federal Regulatory Landscape.” January 2026. https://www.bakerbotts.com/thought-leadership/publications/2026/january/us-ai-law-update

[3] Gunderson Dettmer. “2026 AI Laws Update: Key Regulations and Practical Guidance.” 2026. https://www.gunder.com/en/news-insights/insights/2026-ai-laws-update-key-regulations-and-practical-guidance

[4] King & Spalding LLP. “New State AI Laws are Effective on January 1, 2026, But a New Executive Order Signals Disruption.” 2025. https://www.kslaw.com/news-and-insights/new-state-ai-laws-are-effective-on-january-1-2026-but-a-new-executive-order-signals-disruption

[5] White & Case LLP. “AI Watch: Global Regulatory Tracker – United States.” 2026. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

[6] National Law Review. “What the Regulations of 2025 Could Mean for the AI of 2026.” 2026. https://natlawreview.com/article/2026-outlook-artificial-intelligence

[7] Drata. “Artificial Intelligence Regulations: State and Federal AI Laws 2026.” 2026. https://drata.com/blog/artificial-intelligence-regulations-state-and-federal-ai-laws-2026

[8] Software Improvement Group. “AI Legislation in the US: A 2026 Overview.” January 28, 2026. https://www.softwareimprovementgroup.com/blog/us-ai-legislation-overview/

[9] National Institute of Standards and Technology (NIST). “AI Risk Management Framework.” Released January 26, 2023; updated 2024–2025. https://www.nist.gov/itl/ai-risk-management-framework

[10] NIST. “Draft NIST Guidelines Rethink Cybersecurity for the AI Era.” NIST IR 8596 (Preliminary Draft), December 17, 2025. https://www.nist.gov/news-events/news/2025/12/draft-nist-guidelines-rethink-cybersecurity-ai-era

[11] National Law Review. “NIST Issues Preliminary Draft of Cyber AI Profile, a Framework Poised to Alter Security Operations in the AI-Driven Threat Landscape.” December 2025. https://natlawreview.com/article/nist-issues-preliminary-draft-cyber-ai-profile-framework-poised-alter-security

[12] Nemko Digital. “NIST AI Risk Management Framework 2025: Secure Your AI Now.” 2025. https://digital.nemko.com/regulations/nist-rmf

[13] Lowenstein Sandler LLP. “Financial Services AI Risk Management Framework: Operationalizing the 230 Control Objectives Before the Market Wakes Up.” March 2026. https://www.lowenstein.com/news-insights/publications/client-alerts/financial-services-ai-risk-management-framework-operationalizing-the-230-control-objectives-before-the-market-wakes-up-data-privacy

[14] Federal Trade Commission. “Artificial Intelligence.” FTC enforcement and policy page. https://www.ftc.gov/industry/technology/artificial-intelligence

[15] Perkins Coie LLP. “Privacy Law Recap 2025 – FTC Enforcement.” January 2026. https://perkinscoie.com/insights/blog/privacy-law-recap-2025-ftc-enforcement

[16] American Bar Association. “The FTC Turns Up the Heat on AI: Enforcement, Inquiry, and Messaging From the Top.” 2025. https://www.americanbar.org/groups/antitrust_law/resources/newsletters/ftc-turns-up-heat-ai-enforcement-inquiry-messaging-from-the-top/

[17] Benesch, Friedlander, Coplan & Aronoff LLP. “One Year In, FTC’s ‘Operation AI Comply’ Continues Under New Administration, Signaling Enduring Enforcement Focus.” January 9, 2026.

https://www.beneschlaw.com/insight/one-year-in-ftcs-operation-ai-comply-continues-under-new-administration-signaling-enduring-enforcement-focus/

[18] Mintz LLP. “Emerging Federal AI Strategy: FTC Sets Aside Rytr Consent Order; and Uncertainty Looms with BEAD Funding and State AI Laws.” February 13, 2026. https://www.mintz.com/insights-center/viewpoints/54731/2026-02-13-emerging-federal-ai-strategy-ftc-sets-aside-rytr

[19] Hogan Lovells LLP. “White House Issues Executive Order to Establish a Federal AI Policy and Preempt State Laws.” December 2025. https://www.hoganlovells.com/en/publications/white-house-issues-executive-order-to-establish-a-federal-ai-policy-and-preempt-state-laws

[20] DLA Piper (Lexology). “FTC Resolves Another Case Involving ‘AI-Washing.’” February 5, 2026. https://www.lexology.com/library/detail.aspx?g=88dedbb3-b82a-4a7d-8079-c396c25d5b26

[21] Frankfurt Kurnit Klein & Selz (Advertising Law). “No More Rytr’s Block: FTC Reverses Course on AI Enforcement.” December 2025. https://advertisinglaw.fkks.com/post/102lz36/no-more-rytrs-block-ftc-reverses-course-on-ai-enforcement

[22] Lathrop GPM LLP. “Transparency and AI: FTC Launches Enforcement Actions Against Businesses Promoting Deceptive AI Product Claims.” May 2025. https://www.lathropgpm.com/insights/transparency-and-ai-ftc-launches-enforcement-actions-against-businesses-promoting-deceptive-ai-product-claims/

[23] LogicGate. “Understanding the NIST AI RMF Framework.” March 12, 2026. https://www.logicgate.com/blog/understanding-the-nist-ai-rmf-framework/

[24] Wikipedia. “Regulation of Artificial Intelligence in the United States.” Last updated March 2026. https://en.wikipedia.org/wiki/Regulation_of_artificial_intelligence_in_the_United_States

Disclaimer: This report is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel regarding specific compliance obligations. Information is current as of March 2026 and is subject to change as the regulatory environment continues to evolve.

Key Takeaway

. 2026 is a pivot year for AI regulation in the U.S. Multiple state laws are now in effect, federal preemption efforts are intensifying, and organizations need documented evidence of governance and control across jurisdictions, not just awareness of pending bills.

Important Limitation

. The December 2025 Executive Order does not establish any federal AI standards or regulations on its own. Absent further Congressional action, it represents a statement of policy principles and a set of enforcement tools rather than a binding regulatory framework. Existing state AI laws remain in effect unless successfully challenged.

Compliance Implication

. Until courts resolve preemption disputes and Congress acts, organizations must maintain compliance with all existing state AI requirements. The Executive Order itself does not suspend or invalidate any state law. Companies should develop flexible compliance programs capable of adapting to rapid changes in the regulatory environment.