Barnes & Thornburg

America's AI Action Plan

What You Need to Know

AUGUST 2025

Executive Summary

The White House has released *Winning the Race: America's AI Action Plan* (July 2025), a strategic memorandum that addresses pathways to secure U.S. leadership in artificial intelligence (AI) and ensure national competitiveness.

The Action Plan emphasizes AI's transformative potential. It is expected to fuel breakthroughs across science, defense, education, and commerce — while positioning the United States as the global standard-setter for AI innovation, infrastructure and security.

Structured around three strategic pillars, the Action Plan outlines a broad federal commitment to:

1. **Accelerate AI Innovation** – Removing regulatory barriers, promoting open-source development, driving AI adoption across sectors, and ensuring systems reflect American values of free speech and objectivity

2. **Build American AI Infrastructure** – Scaling energy capacity, expanding semiconductor manufacturing, and constructing secure data centers to support AI growth

3. **Lead in International AI Diplomacy and Security** – Strengthening export controls, countering adversarial influence, and aligning technology protection measures with allies

This report provides insight into several cross-cutting themes for businesses and legal stakeholders, with a focus on:

Privacy and Security Perspectives – Data governance, cyber-resilience and legal considerations for AI-related privacy frameworks

Intellectual Property Perspectives – IP protection for AI models, datasets and innovations; enforcement against malicious actors

Infrastructure, Education, and Robotics – Regulatory updates on data centers, chip manufacturing, energy requirements, and AI workforce development

A Focus on Potential Liability – Synthetic media risks, biosecurity obligations, international AI compliance strategies, and consideration of potential liability for AI labs/system users and developers

Pillar I – Accelerate AI Innovation

Perspectives on Privacy and Security

KEY INSIGHTS

- Federal cybersecurity initiatives may impact operational costs and compliance timelines. Companies should prepare for new AI Information Sharing and Analysis Center (AI-ISAC) requirements and unfunded security mandates.
- State-level regulatory friction with federal funding criteria could affect grant eligibility and contract opportunities. Organizations should assess exposure in states with comprehensive AI regulations.
- International data transfer frameworks must accommodate both AI export promotion and privacy protection requirements. Companies should review cross-border partnerships and vendor agreements.

The Action Plan establishes a new approach to AI governance that emphasizes innovation and competitiveness while addressing privacy and security considerations. It directs the National Institute of Standards and Technology (NIST) to eliminate references to diversity, equity, inclusion and climate change from its AI Risk Management Framework, representing a departure from previous bias mitigation approaches. Federal agencies have been directed to review existing Federal Trade Commission (FTC) investigations and enforcement actions to identify those that may "unduly burden AI innovation," signaling reduced federal privacy oversight.

Federal agencies are tasked with creating "the world's largest and highest quality AI-ready scientific datasets" while maintaining commitments to uphold privacy and civil liberties. To achieve this goal, agencies must develop **data quality standards for biological, materials science, chemical, physical and other scientific data modalities** used in AI model training. The Department of Commerce and other agencies will establish protocols for secure data sharing among federal entities, research institutions and private sector partners while implementing appropriate privacy safeguards.

Regarding cybersecurity, a new **AI Information Sharing and Analysis Center (AI-ISAC)** will be established under the Department of Homeland Security. Critical infrastructure operators in sectors such as healthcare, financial services and energy will be subject to new obligations, including sector-specific incident response protocols. The Department of Defense is also charged with developing “secure-by-design” technical standards for AI systems supporting sensitive government workloads.

Federal funding decisions will now explicitly consider state-level AI regulations, allowing agencies to limit funding to states deemed out of alignment with federal AI objectives. This approach notably conflicts with congressional sentiment, as the Senate recently rejected a direct moratorium on state AI laws by a 99-1 vote, suggesting ongoing constitutional and political challenges. **This creates immediate compliance challenges for organizations in states like California and New York**, which are advancing comprehensive AI governance frameworks that may conflict with federal priorities.

Healthcare organizations must reconcile Health Insurance Portability and Accountability Act (HIPAA) requirements with new federal AI procurement standards, while financial institutions face similar challenges under the Gramm-Leach-Bliley Act (GLBA) and state privacy laws.

Perspectives on Privacy and Security

Internationally, regulatory divergence is growing. The European Union (EU) AI Act's risk-based framework contrasts with the United States' emphasis on minimal federal oversight, creating complex compliance challenges for cross-border data transfers and AI system documentation. To address this, the Department of Commerce and State will develop **frameworks for secure AI technology exports** that account for global privacy and data security obligations.

Emerging privacy challenges related to **synthetic media and deepfakes** receive specific attention. The National Institute of Standards and Technology (NIST) will expand its forensic guidelines for detecting manipulated content while the Department of Justice is directed to develop evidentiary standards for AI-generated materials in legal proceedings. These measures aim to protect individuals from privacy violations while maintaining judicial integrity.

The convergence of reduced federal privacy oversight and enhanced cybersecurity mandates creates novel risk profiles for AI-deploying organizations, particularly those handling sensitive data or operating across multiple jurisdictions.

Immediate Actions (0-90 Days):

- Assess AI systems for alignment with federal priorities
- Review contract terms for exposure to regulatory change
- Evaluate readiness for AI-ISAC participation
- Document current privacy safeguards
- Revisit vendor agreements for liability provisions

Strategic Planning (3-12 Months):

- Develop flexible compliance frameworks accommodating multiple jurisdictions
- Strengthen due diligence for global AI partnerships
- Create AI-specific incident response protocols
- Build relationships with regulators and industry groups
- Prepare for international AI regulations if operating globally

Long-Term Risk Management:

- Monitor evolving federal and state policies
- Prepare for divergent U.S. and international compliance obligations
- Strengthen privacy safeguards to manage operational risk
- Develop governance frameworks addressing regulatory uncertainty
- Position for potential future legislative changes

Organizations should prioritize building **flexible AI governance frameworks** that can adapt to this shifting regulatory landscape while maintaining competitive positioning. Given the Action Plan's emphasis on rapid implementation across 90+ federal actions, early preparation and stakeholder engagement will be critical for success.

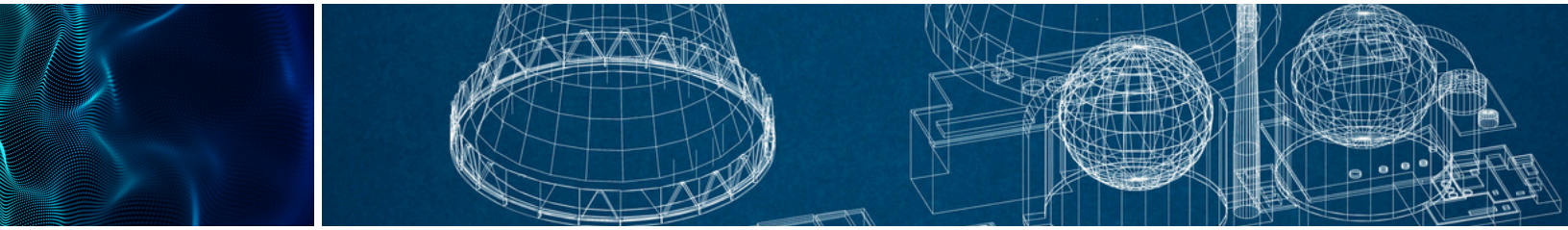
Pillar II – Build American AI Infrastructure

Initiatives: Infrastructure, Education & Robotics

The Action Plan outlines a comprehensive strategy to streamline regulatory frameworks in order to accelerate the **development of AI-related infrastructure**, enhance the **resilience of the electric grid**, and **reshore semiconductor manufacturing**. It also calls for the establishment of new security standards for high-stakes AI environments, significant investments in workforce training, and strategic support for advanced robotics technologies. Together, these measures aim to preserve the United States' competitive advantage in the global AI ecosystem while safeguarding critical systems and supply chains.

To expedite infrastructure development, the Action Plan proposes **simplifying permitting processes** for data centers and related facilities. This may include amendments to key statutes such as the Clear Air Act, the Clean Water Act and the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) among others.

In addition, it underscores the importance of making federal lands available for data center construction and for building out the necessary power generation infrastructure to support them. **Security remains a core concern**: the Action Plan stresses the need to maintain stringent guardrails to prevent adversaries from embedding sensitive inputs into AI infrastructure and to ensure that the domestic AI computing stack is based on American-made components, free from foreign adversary technologies or influence.



Modernizing and stabilizing the electric grid is another major priority. The Action Plan calls for the **protection of existing energy assets**, the **prevention of premature decommissioning** of power generation resources, and the **optimization of current infrastructure performance**. To ensure long-term energy resilience, it advocates for robust investment in frontier energy technologies, including enhanced geothermal systems, nuclear fission, and nuclear fusion.

On semiconductor manufacturing, it reaffirms the urgency of reshoring production to shield the U.S. supply chain from foreign disruptions. The Action Plan recommends that the Department of Commerce continue leveraging the CHIPS Program Office to eliminate regulatory barriers that hinder domestic semiconductor manufacturing efforts.

Finally, the Action Plan addresses the deployment of AI by U.S. military and intelligence agencies to manage the government's most sensitive data. In response to escalating threats from advanced nation-state actors, it recommends the **development of rigorous technical standards** —led by the Department of Defense — for high-security AI data centers. It also calls for broader adoption of classified computing environments across agencies to enable scalable, secure AI workloads.

Initiatives: Infrastructure, Education & Robotics

Regarding education, the Action Plan calls for workforce investments to build, operate, and maintain the AI infrastructure, including electricians and advanced HVAC technicians. It recommends that the Department of Labor and the Department of Commerce create a "national initiative to identify high-priority occupations essential to the buildout of AI-related infrastructure," by convening employers, industry groups and other workforce stakeholders to develop **national skill frameworks** and **competency models** for these roles. It also encourages collaboration with state and local governments and workforce systems to align training programs with AI infrastructure needs.

In robotics, the Action Plan urges the federal government to prioritize investment in emerging technologies, asserting the strategic importance of making the United States and its allies global leaders in autonomous drones, self-driving cars and advanced robotic systems. It recommends convening industry and government stakeholders to **identify and rectify supply chain challenges** to American robotics and drone manufacturing.

KEY TAKEAWAYS

- Evaluate how anticipated regulatory streamlining may impact your infrastructure projects.
- Plan for increased power needs and explore partnerships with utility and energy providers.
- Track CHIPS Program developments for opportunities to engage in collaborative efforts to strengthen domestic supply chains.
- Robotics and drone manufacturers should prepare for increased federal investment and collaboration opportunities and review supply chain resilience and consider strategic partnerships to secure essential components.

Pillar III – Lead in International AI Diplomacy and Security

IP Perspectives: Protection for AI Models, Datasets and Innovations

The Action Plan frames proprietary AI models, datasets, and supporting infrastructure as **critical national assets**, urging heightened IP protection and enforcement coordination. It identifies proprietary AI technologies as critical national assets and calls for collaborative efforts between the Department of Commerce, Department of Defense, Department of Homeland Security and the intelligence community to safeguard AI models and infrastructure.

Action Plan Insights:

- Developing high-security data centers for sensitive government AI workloads
- Implementing secure-by-design AI systems
- Leveraging advanced cybersecurity measures to mitigate risks from cyberattacks, insider threats and adversarial manipulation

Federally funded researchers must now **disclose non-sensitive datasets**, encouraging transparency but raising unresolved copyright and ownership questions — particularly as open-source and open-weight models gain prominence. These models, while spurring innovation and standardization, also raise concerns around license compliance and unauthorized derivative works.

Regarding enforcement, the Action Plan addresses the proliferation of synthetic media and AI-generated deepfakes, which threaten evidentiary integrity and IP rights. The government proposes **expanding the NIST's "Guardians of Forensic Evidence" program** into formal guidelines and exploring amendments to the Federal Rules of Evidence to ensure the admissibility and authentication of digital content.

Additionally, the TAKE IT DOWN Act, officially known as the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, and future legislative measures aim to combat the unauthorized creation and dissemination of non-consensual AI-generated content, signaling **potential expansion of statutory remedies** under copyright and related rights.

Together, these initiatives reflect a dual policy priority: **facilitating open innovation of AI** while **fortifying IP protections** against misappropriation and misuse. For rights holders, this environment underscores the need for robust trade secret protocols, proactive IP enforcement strategies and compliance frameworks for data and AI use. For copyright law, the Action Plan foreshadows evolving guidance on authorship, derivative works and liability in the context of generative AI systems, all issues that are expected to shape litigation and licensing strategies in the years ahead.

IP Perspectives: Protection for AI Models, Datasets and Innovations

KEY TAKEAWAYS

- Implement robust trade secret and cybersecurity measures to prevent theft or misuse of proprietary models and datasets.
- Conduct compliance audits before adopting or releasing models under open-source licenses to ensure compliance with derivative works.
- Review data-sharing agreements and IP clauses in research collaborations prior to distribution.
- Consider registering core content and implementing proactive monitoring strategies for unauthorized uses.
- Review supply chain agreements and licensing structures for compliance with emerging U.S. export control regimes.

A Focus on Potential Liability

The Action Plan emphasizes adoption and innovation but **does not specifically address liability protections** for organizations deploying or building AI systems.

Deepfakes and Legal Accountability

The Action Plan specifically highlights the **emergence of "deepfakes"** and their potential use in the legal system, noting that the Department of Justice and other legal stakeholders must work to develop rules and guidelines to ensure that these materials are not relied upon in adjudicating disputes. However, the Action Plan does not address whether there is recourse against the AI systems that generate these deepfakes.

AI Adoption and Innovation

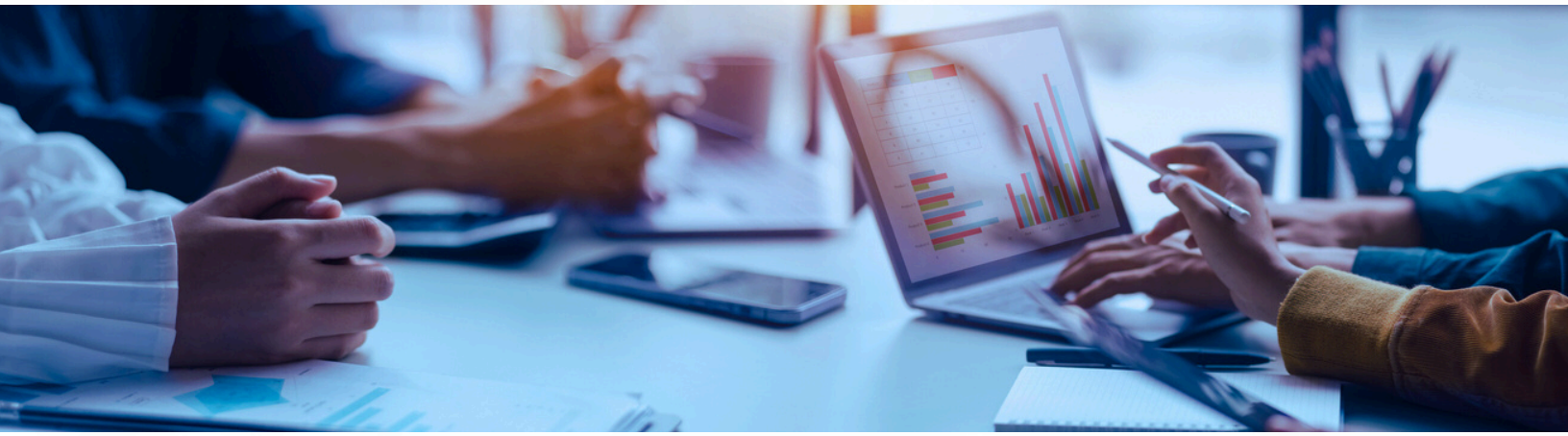
The Action Plan notes that "the inner workings of frontier AI systems are poorly understood. Technologists know how LLMs work at a high level but often cannot explain why a model produced a specific output." While acknowledging this, the Action Plan calls for **rapid adoption of AI technology in the industrial and manufacturing sectors.**

To meet the mandate of the Action Plan — "scaling foundational and translational manufacturing technologies" — manufacturers will need to ensure **oversight and quality assurance protocols** are implemented. These safeguards should be in place at both the AI input level and the finished product stage of the process to ensure that the manufacturing process is properly programmed and that it is operating as intended to produce compliant finished products.

The Action Plan also envisions the expansion of AI adoption in fields such as materials science, engineering and chemistry as "AI systems can already generate models of protein structures, novel materials and much else." Yet, adoption of AI to generate new materials may be hampered by concerns over potential liability.

KEY INSIGHTS

- Deepfake-related harm may be actionable under existing law, but AI creators may need statutory clarity or safe harbors to foster innovation
- Manufacturers relying on AI outputs must implement strong quality assurance protocols and maintain documentation to avoid design defect claims.



Preparing for What's Next

Organizations should evaluate how the Action Plan will impact compliance, procurement, infrastructure strategy, risk management and long-term AI adoption. In particular, businesses operating in regulated sectors or across jurisdictions should begin developing adaptive governance frameworks now in anticipation of evolving federal and international AI rules.

About Barnes & Thornburg's Artificial Intelligence Practice

B&T's Artificial Intelligence group helps clients across industries — ranging from healthcare and insurance to international trade and corporate operations — effectively deploy and use AI while managing compliance, privacy, IP, and liability risks. Our multidisciplinary team delivers tailored counsel on AI development, procurement, governance frameworks, regulatory navigation, intellectual property, data security, and commercial transactions.

We are closely tracking developments in generative AI technologies, platform offerings, and the legal and ethical frameworks emerging around them. Our thought leaders, who are immersed in these issues and the underlying technology, can provide practical and legal advice. Barnes & Thornburg is ready to help you navigate the AI landscape, mitigate risks, and leverage AI effectively and compliantly. We can help you reach your objectives in a cost-effective and timely fashion with our multidisciplinary approach.

Contributors

Nicholas Sarokhanian
Chair, Artificial Intelligence Practice
Email

Kaitlyn Stone
Partner
Email

Brian McGinnis
Co-Chair, Data Security and Privacy
Email

Lyric D. Menges
Associate
Email

William Carlucci
Associate
Email