

## America's AI Action Plan: What's In, What's Out, What's Next

July 25, 2025

*Holland & Knight Alert*

[Sarah Starling Crossan](#) | [Miranda A. Franco](#) | [Misha Lehrer](#) | [Parker M. Reynolds](#) | [Marissa C. Serafino](#) | [Paul Stimers](#)

### Highlights

- The Artificial Intelligence (AI) Action Plan recommends that the executive branch take a series of actions to propel the entire U.S. AI ecosystem, including AI developers, data centers, energy sources and semiconductors.
- Despite a strong emphasis on reducing regulatory burdens, the Plan identifies some areas where standards, security and restrictions are appropriate, including export control enforcement for advanced AI compute.
- For companies with AI equities, these policy recommendations represent significant opportunities, as well as enhanced expectations or restrictions, that may warrant further review to determine the impact on such companies and how to comply or respond.

---

The White House [released "Winning the Race: America's AI Action Plan"](#) (Plan) on July 23, 2025, in accordance with President Donald Trump's Jan. 23, 2025, executive order on ["Removing Barriers to American Leadership in Artificial Intelligence."](#)

Specifically, the 28-page Plan details more than 90 federal policy actions the Trump Administration intends to implement over the next few years, emphasizing that the U.S. needs to "innovate faster and more comprehensively than our competitors in the development and distribution of new AI technology across every field, and dismantle unnecessary regulatory barriers that hinder the private sector in doing so."

The Plan envisions "a new golden age of human flourishing," marked by three simultaneous transformations: an industrial revolution, an information revolution and a renaissance in science and the arts. It is structured around three core pillars: 1) Accelerate AI Innovation, 2) Build American AI Infrastructure and 3) Lead in International AI Diplomacy and Security.

Cutting across these three pillars are three principles:

1. American workers are central to the Trump Administration's AI policy.
2. AI systems must be free from ideological bias and pursue objective truth.
3. The government must prevent advanced technologies from being misused or stolen and must monitor for emerging or unforeseen risks from AI.

The Plan is meant to be implemented via executive action in the near term. President Trump also signed three AI-related executive orders on the day the Plan was released:

- ["Preventing Woke AI in the Federal Government"](#)
- ["Accelerating Federal Permitting of Data Center Infrastructure"](#)
- ["Promoting the Export of the American AI Technology Stack"](#)

This Holland & Knight alert provides an overview of the Plan's policy actions, which provide a road map for

# Holland & Knight

organizations to identify opportunities and responsibilities for AI stakeholders.

## **Pillar I: Accelerate AI Innovation**

Pillar I lays out a sweeping federal deregulatory and development framework that aims to accelerate U.S. AI leadership by removing perceived policy barriers and incentivizing innovation and adoption. It directs major agencies – including the Office of Management and Budget (OMB), Federal Communications Commission (FCC), Federal Trade Commission (FTC) and Office of Science and Technology Policy (OSTP) – to identify and repeal rules that hinder AI deployment and factor state-level AI regulatory climates into federal funding decisions. The Plan also calls for excluding references to "misinformation," as well as diversity, equity and inclusion (DEI), and climate change from the National Institute of Standards and Technology's (NIST) AI risk guidance, along with establishing federal procurement standards to ensure only AI models deemed free of "ideological bias" are used.

The Plan also signals the Trump Administration's position on AI-related issues. For instance, it proposes encouraging open-source and open-weight AI for compute access, expanding research access to private-sector AI resources for startups and academia, and creating a sustainable federal infrastructure for AI testing and evaluation. This is a strong endorsement of open-source, which is a shift from the Biden Administration's more cautious approach.

Beyond deregulation, Pillar I promotes widespread AI adoption across sectors, including healthcare, defense, manufacturing and science. It proposes creating agency-specific regulatory sandboxes, domain-specific AI productivity benchmarks, evaluations of AI and national security assessments of AI usage. The Plan encourages investments in next-generation manufacturing to develop and scale manufacturing technologies using various federal programs, including the CHIPS research and development (R&D) programs, Other Transaction Authority (OTA), Title III of the Defense Production Act (DPA) and other small business programs. This effort also includes public-private partnerships related to supply chain challenges to American robotics and drone manufacturing. To enable AI development, the Plan also focuses on building world-class data sets, including setting minimum data quality standards for use in AI model training.

For defense specifically, the Plan outlines significant initiatives for the U.S. Department of Defense (DOD) designed to position the military at the forefront of AI innovation and implementation. This includes transforming senior military colleges into specialized hubs of AI R&D, integrating AI-specific curriculum across various academic majors to foster the next generation of military AI expertise, as well as urging DOD to continue refining its Responsible AI and Generative AI Frameworks, Roadmaps and Toolkits in collaboration with NIST and the Office of the Director of National Intelligence (ODNI) to ensure the military's AI development remains secure, ethical and aligned with national security objectives. Government contractors should also note that GSA is tasked with managing an AI procurement toolbox that facilitates uniformity across the federal enterprise to the greatest extent practicable and implementing an Advanced Technology Transfer and Capability Sharing Program.

The Plan's policy actions also focus on the impact of AI. For instance, security and risk mitigation related to AI are prioritized through public-private partnerships and guidelines for deepfake detection and evidence standards. Concerning workforce and labor, the Plan recommends the U.S. Department of the Treasury issue guidance clarifying that many AI literacy and skill programs may qualify as eligible education assistance under the Internal Revenue Code, allowing employers to offer tax-free reimbursement and incentivizing private-sector investment in AI upskilling.

In addition to the broad deregulatory and adoption-focused recommendations, Pillar I also aims to limit state-level AI policies seen as impediments to innovation. Specifically, OMB is expected to work with federal agencies that have AI-related discretionary funding programs to consider a state's AI "regulatory climate" when making funding decisions. Though the Plan does not offer specifics on this point, state-level regulation that could be within scope includes existing AI laws, such as the Colorado AI Act, and enforcement of those laws. It could also include broader industry-

# Holland & Knight

specific regulations such as patient disclosures or restrictions on the use of AI in prior authorization.

## Key Takeaways

- Particularly for government contractors, assess AI governance models to align with the planned federal procurement standards that emphasize "ideological bias" requirements while preparing for a regulatory environment that may deemphasize misinformation, DEI and climate change considerations in AI risk frameworks.
- Develop strategies to leverage the Trump Administration's strong endorsement of open-source and open-weight AI models, including preparing to participate in regulatory sandboxes and public-private partnerships that could provide competitive advantages in AI development and deployment.
- Prepare for the release of a new National AI R&D Strategic Plan and engage with standard-setting leaders, including NIST's Center for AI Standards and Innovation (CAISI).

## Pillar II: Build American AI Infrastructure

This section focuses on enabling and securing the necessary infrastructure in the public and private sectors to support AI development and adoption. It features opportunities for stakeholders in the AI supply chain to address long-standing barriers, such as grid capacity, but also suggests high standards for AI cybersecurity and design that are notable for developers and deployers. The Plan elevates the role of CAISI at the NIST to create various standards and guidance related to AI.

For the private sector, Pillar II focuses on unlocking data center, semiconductor manufacturing and energy infrastructure. The Plan streamlines permitting to establish new categorical exclusions under the National Environmental Policy Act (NEPA) for data centers, expand the Fixing America's Surface Transportation (FAST-41) Act process to cover data center and data center energy projects, explore a nationwide Clean Water Act (CWA) permit process, make federal lands available for construction and expedite permitting under the CWA and other environmental statutes. The Plan also maintains security guardrails and ensures that the domestic AI computing stack is American-made and free from foreign adversary information and technology.

For energy infrastructure, the Plan focuses on upgrading and stabilizing the grid by ensuring the grid is in compliance with nationwide standards for resource adequacy and sufficient power generation capacity, implementing strategies to enhance the efficiency and performance of the transmission system, and prioritizing interconnection to embrace new energy sources such as nuclear fusion and fission.

For compute, the Plan encourages the U.S. Department of Commerce's (DOC) revamped CHIPS Program Office to continue focusing on investing and "removing all extraneous policy requirements" for CHIPS-funded semiconductor manufacturing projects. DOC and other relevant federal agencies are also expected to collaborate to streamline regulations that slow semiconductor manufacturing efforts.

This Pillar also focuses on U.S. government AI infrastructure from defense and national security perspectives, such as building high-security data centers for defense and intelligence purposes and promoting secure-by-design approaches to AI. These facilities will be developed according to new technical standards created through collaboration between the DOD, U.S. Intelligence Community (IC), National Security Council (NSC) and NIST to ensure resistance against sophisticated nation-state attacks. The Plan further emphasizes advancing agency adoption of classified compute environments to support scalable and secure AI workloads, allowing intelligence agencies to leverage AI capabilities without compromising sensitive data.

The Plan also proactively identifies AI security concerns with respect to critical infrastructure and cybersecurity and, therefore, recommends the U.S. Department of Homeland Security (DHS) issue and maintain guidance to private sector entities on remediating and responding to AI-specific vulnerabilities and threats and establish an information-

# Holland & Knight

sharing center for critical infrastructure sectors.

## Key Takeaways

- Prepare for new technical standards developed through a government collaboration that will establish secure-by-design approaches for AI systems, potentially creating new voluntary benchmarks but also competitive advantages for compliant providers.
- Anticipate new cybersecurity standards through the AI Information Sharing and Analysis Center (AI-ISAC) requiring proactive vulnerability management and threat intelligence sharing.
- Prepare for grid optimization initiatives and nationwide resource adequacy standards in energy-intensive AI operations.
- Identify new opportunities in semiconductor grant and research programs and prepare for removal of extraneous requirements from CHIPS-funded projects.

## Pillar III: Lead in International AI Diplomacy and Security

The final section of the Plan lays out a multipronged strategy to secure U.S. leadership in global AI by aggressively exporting the full AI technology stack to allies, countering adversarial influence in international governance and tightening export controls on advanced AI compute and semiconductor manufacturing.

Specifically, the Plan calls for DOC to develop and implement a full-stack AI export program in concert with other trade-related industries, consistent with security requirements. Several proposals are aimed at countering the influence of global competitors and adversaries, such as leveraging international diplomatic and standard-setting organizations. Proposals to enhance AI chip controls include location verification and export control monitoring in high-risk regions and for previously untracked semiconductor manufacturing subsystems. The Plan also seeks to harmonize export controls and technology protection measures with allies by jointly developing export controls, sharing technology protection measures, discouraging backfilling, and imposing secondary tariffs or other penalties where necessary.

Finally, the Plan underscores the importance of rigorous national security and biosecurity measures by recommending robust risk evaluations of frontier AI models and screening protocols for biotechnology research, signaling a proactive approach to emerging threats at the intersection of AI, national security and global standards-setting. The Plan includes recommendations to expand security assessments of U.S. and foreign AI capabilities, prioritize federal recruitment of leading AI researchers and enhance national security-related AI evaluation tools. With respect to biosecurity, the Plan recommends layers of screening for malicious actors.

## Key Takeaways

- Companies involved in the development, export or integration of AI systems, hardware or software should anticipate increased federal assistance in exporting to allies.
- As the Trump Administration takes action to implement the Plan in the coming months, companies will need to reassess supply chains, partnership structures and compliance programs to ensure they do not inadvertently facilitate access to controlled technologies by adversaries or entities of concern.
- Companies may be able to access new resources for assessing risk and detecting malicious activity.
- Companies in the biotechnology and research sectors receiving federal funding may face new biosecurity mandates.

---

Information contained in this alert is for the general education and knowledge of our readers. It is not designed to be, and should

# Holland & Knight

not be used as, the sole source of information when analyzing and resolving a legal problem, and it should not be substituted for legal advice, which relies on a specific factual analysis. Moreover, the laws of each jurisdiction are different and are constantly changing. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. If you have specific questions regarding a particular fact situation, we urge you to consult the authors of this publication, your Holland & Knight representative or other competent legal counsel.

---



**Sarah Starling Crossan** is a public affairs advisor in Holland & Knight's Washington, D.C., office and a member of the firm's Public Policy & Regulation Group. Ms. Crossan's practice focuses on regulatory and legislative healthcare policies, including physician payment, administrative burden and prior authorization, optimizing patient care coordination, social determinants of health (SDOH) metrics, and value-based payment model development.

+1.202.469.5656 | Sarah.Crossan@hklaw.com



**Miranda Franco** is a senior policy advisor in Holland & Knight's Washington, D.C., office, where she has been a key member of the firm's Public Policy & Regulation Group since 2013. In this capacity, Ms. Franco helps clients navigate the complexities of federal reimbursement policy and address challenges and opportunities that impact healthcare quality and delivery. She regularly engages with federal agencies under the U.S. Department of Health and Human Services (HHS) and collaborates with prominent health policy advisors both within the agencies and in congressional offices.

+1.202.469.5259 | Miranda.Franco@hklaw.com



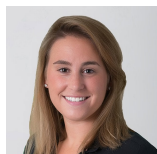
**Misha Lehrer** is a Washington, D.C., public policy professional and member of Holland & Knight's National Security & Defense Industry Sector Group. With more than a decade of collective experience in politics and public policy in both the public and private sectors, Mr. Lehrer develops and implements strategies with clients navigating Capitol Hill and federal agencies, in particular the congressional defense committees and U.S. Department of Defense (DOD).

+1.202.469.5539 | Misha.Lehrer@hklaw.com



**Parker Reynolds** is an attorney in Holland & Knight's Washington, D.C., office and a member of the firm's Public Policy & Regulation Group. Ms. Reynolds focuses her practice primarily on legislative and regulatory issues related to healthcare and technology. She also has a deep understanding of matters related to the U.S. Food and Drug Administration (FDA), privacy, energy, financial services, political law and compliance.

+1.202.469.5606 | Parker.Reynolds@hklaw.com



**Marissa Serafino** is an attorney and policy professional in Holland & Knight's Washington, D.C., office and member of the firm's Public Policy & Regulation Group. Ms. Serafino helps clients navigate increasingly complex regulatory landscapes and engage with the U.S. Congress, executive branch and independent agencies on technology issues across industries. Clients rely on Ms. Serafino for strategic counsel on legal and policy matters and investigations impacting their organizations.

+1.202.469.5414 | Marissa.Serafino@hklaw.com



**Paul Stimers** is a Washington, D.C., attorney and a member of Holland & Knight's Public Policy & Regulation Group. He is the leader of the group's Space Policy Team. Mr. Stimers focuses his policy

# Holland & Knight



advocacy efforts on matters related to emerging technologies such as commercial spaceflight, quantum technology and artificial intelligence (AI), and advises a wide range of companies and industry associations in pursuing legislation and representing their interests before Congress and federal agencies.

+1.202.469.5612 | [Paul.Stimers@hklaw.com](mailto:Paul.Stimers@hklaw.com)