Davis Polk

America's AI Action Plan: Pillar 2 – Building American AI Infrastructure

August 8, 2025 | Client Update | 6-minute read

On July 23, the Trump administration released the AI Action Plan developed in accordance with Executive Order 14179. In this second update, we discuss Pillar II of the Plan.

Background

President Trump formally introduced America's AI Action Plan (the Plan) during his keynote speech at the "Winning the AI Race" summit on July 23, 2025. The Plan is structured as three pillars: (i) accelerating AI innovation, (ii) building American AI infrastructure, and (iii) leading in international diplomacy and security. Together, these three Pillars comprise over 100 federal policy actions for regulating, implementing and investing in artificial intelligence, of which approximately 30 are detailed in Pillar 2.

Our prior update focused on Pillar I. This update focuses on Pillar II.

Pillar 2 – Build American AI Infrastructure

The second pillar in the Plan concentrates its directives in two primary areas.

First, it focuses on accelerating development of the infrastructure needed to sustain the American AI industry, including chip factories, data centers, and energy infrastructure. Continuing the deregulatory trend discussed in our update on Pillar I, Pillar II reflects a clear mandate for federal agencies to identify development sites, streamline construction, and complete environmental permitting processes. It also details a series of policy recommendations to foster a domestic workforce with the appropriate skills and training to realize the Plan's vision.

Second, Pillar II focuses on data security foundations and practices, asserting that "promoting resilient and secure AI development and deployment should be a core activity of the U.S. government." Pillar II seeks to bolster the defensibility of AI-infused critical infrastructure through secure-by-design AI and facilitate the development of federal AI-specific incident response practices and frameworks for the public and private sectors.

To achieve these goals, Pillar II directs the following policy actions, among others:

Data centers and manufacturing

The Plan asserts that existing environmental permitting structures "make it almost impossible to build this infrastructure … with the speed that is required." To accelerate the construction of data centers and related power generation infrastructure, the Plan recommends the following policy actions, many of which are echoed in President Trump's Executive Order "Accelerating Federal Permitting of Data Center Infrastructure," which issued contemporaneously with the Plan:

- Direct federal agencies to proactively identify federal lands that are suitable for AI datacenter and energy infrastructure development projects
- Establish "Categorial Exemptions" for data center-related activity under the National Environmental Policy Act (NEPA), which otherwise requires federal agencies to assess the environmental impact of their proposed actions, thereby avoiding requirements to prepare Environmental Assessments or Environmental Impact Statements
- Make all data center and related energy projects eligible for the FAST-41 process under the Fixing America's Surface Transportation Act of 2015, which seeks to enhance interagency coordination, predictability and timeliness in conducting environmental reviews
- Explore adopting a nationwide Section 404 permit under the Clean Water Act for data centers – which is required for the discharge of covered waste materials into U.S. waters – and exempt data centers from providing Pre-Construction Notifications that would trigger U.S. Army Corps of Engineers review
- Streamline or reduce regulations under the Clean Air Act; the Clean Water Act; the Comprehensive Environmental Response, Compensation, and Liability Act; and other related environmental protection laws
- Increase the use of AI in the permitting process to expedite permit reviews

The Plan also recommends policies focused on repatriating the chip manufacturing industry, noting the national security benefits of technological leadership and supply chain protection. Recommended initiatives in this regard include:

- Removing all "extraneous policy requirements" and reducing regulations on semiconductor manufacturing projects funded under the CHIPS Act of 2022, and "focusing on delivering a strong return on investment for the American taxpayer," which presumably refers to the administration's ongoing efforts to renegotiate CHIPS grants with private sector participants
- Reviewing semiconductor grant and research programs to ensure that they accelerate the integration of advanced AI tools into semiconductor manufacturing

Improving energy infrastructure

Describing the power grid as "the lifeblood of the modern economy and a cornerstone of national security," the Plan recommends a three-part strategy to meet growing energy demands.

- First, the Plan recommends "safeguard[ing] existing assets" by stabilizing the current electric grid, such as by preventing the decommissioning of existing power generation resources and using available backup power sources to bolster reliability. In a shift from the Plan's broader deregulatory trendlines, Pillar II also recommends ensuring that "every corner" of the U.S. power grid complies with national reliability and resource adequacy standards, and foreshadows increased federal scrutiny of state utilities
- Second, the Plan recommends taking action to enhance the current system through upgraded electrical grid hardware and advanced grid management technologies
- Third, the Plan recommends embracing new or experimental energy generation sources, including advanced nuclear and geothermal techniques

The Plan also discusses reforming power markets "to align financial incentives with the goal of grid stability," without specifying what means might be used to accomplish this alignment. Possible actions under this directive could include further indexing payment structures with grid operators to desirable reliability attributes, creating or enhancing credits for participation in energy demand stabilization programs, or incentivizing the siting of AI-related infrastructure in locations that optimize for grid stability.

Critical infrastructure security

The Plan also focuses on protecting critical infrastructure from U.S. foreign adversaries. In July 31 remarks at the Center for Strategic and International Studies, Michael Kratsios, Director of the White House Office of Science and Technology Policy (OTSP), explained that the Plan's security recommendations were directly informed by challenges encountered during the first Trump administration in persuading stakeholders to "rip and replace" banned technology sourced from foreign adversary nations.

Security-related recommendations in Pillar II address the use of domestic technology in the infrastructure supply chain, public-private partnerships in sharing AI threat intelligence, and building out official guidance and frameworks. Recommended policy actions include:

- "[P]rohibit[ing] adversaries from inserting sensitive inputs" into critical AI data center and energy infrastructure, ensuring that the domestic AI computing stack is built using American products, and avoiding the use of technology and communications products and services from foreign adversaries in AI-supportive infrastructure such as energy and telecommunications
- Creating an AI Information Sharing and Analysis Center (AI-ISAC) led by Department of Homeland Security (DHS), in collaboration with other agencies, to promote the sharing of AI-security threat information relevant to critical infrastructure
- Updating existing AI frameworks, such the National Institute of Standards and Technology's (NIST) Responsible AI and Generative AI Frameworks, and issuing new guidance on remediating and responding to AI-specific vulnerabilities and threats
- Publishing an intelligence community-driven Standard on AI Assurance
- Taking steps to prepare for breach and failure of critical AI systems, including by directing federal agencies to partner with the private sector on AI incident response standards, and updating the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Incident & Vulnerability Response Playbook. The Plan specifically recommends that CISA incident response protocols be updated to require that Chief Information Security Officers consult with government agencies, creating a possible new source of compliance risk during AI-related security crises.

Workforce training

The Plan also details policies focused on training the workers that will build, operate, and maintain the AI ecosystem. Examples include:

- Establishing a national initiative to identify priority occupations and develop or modify credentialing systems
- Involving federal agencies not only in industry-driven workforce training program development, but in seeking to impact curricula in educational settings as early as middle and high school.

Takeaways

- The Plan reflects skepticism of foreign-sourced technology used in AI infrastructure, and companies can expect enhanced regulatory scrutiny around AI technology procurement. Consider reviewing vendor and supplier policies and practices to minimize data security risks and the use of foreign products or services, especially from "adversary" nations.
- Companies – particularly those in critical infrastructure sectors – should ensure that risk assessments include AI-specific factors, and that those assessments address related cybersecurity threats and resilience. Consider additional efforts to document risk assessments and mitigations where foreign technology or services remain deployed.
- While the Plan directs agencies to exempt data centers and power infrastructure from cornerstone environmental laws where possible, companies should be mindful of private litigation, business or reputational risks that could arise from projects that remain highly visible and resource-intensive.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

David I. Feinstein
+1 212 450 3293
david.feinstein@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

David Lisson
+1 650 752 2013
david.lisson@davispolk.com

Howard Shelanski
+1 202 962 7060
howard.shelanski@davispolk.com