Davis Polk

America's AI Action Plan: Pillar 3 – Leading in International AI Diplomacy and Security

August 15, 2025 | Client Update | 5-minute read

On July 23, the Trump administration released the AI Action Plan developed in accordance with Executive Order 14179. In this third update, we discuss Pillar III 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 16 are detailed in Pillar III.

Prior updates focused on Pillar I and Pillar II. This update focuses on Pillar III.

Pillar 3 – Leading in International AI Diplomacy and Security

The Plan's third pillar focuses on establishing American primacy in the international market for AI-related technology and strengthening controls on the export and diffusion of American AI technology. Similar to the first two pillars, the third pillar focuses on national security risks presented by the prospect of foreign "adversary" nations obtaining access to advanced technology. Pillar III thus articulates policies to control that access and to mitigate the influence of other nations on international AI governance bodies and the world stage.

To achieve these goals, the Plan recommends the following policy actions, among others:

Exporting the American AI technology stack

Pillar III contemplates the creation of "AI export packages" – inclusive of hardware, models, software, applications, and standards – to meet international demand and displace rival nations' products.

The Plan calls for the Department of Commerce (DOC) to operationalize this "American AI Exports Program" by soliciting, selecting and ultimately marketing proposals from industry groups regarding full-stack AI packages for export. The desire is to offer "turnkey" solutions to foreign customers, and the DOC is already fielding proposals for the American AI Exports Program related to:

- Chips and servers
- Data center storage
- Cloud services and networking

- Data pipelines and labeling systems
- AI models and programs
- Security and cybersecurity systems
- AI applications for specific use cases, including software engineering, education, healthcare, agriculture and transportation

U.S. federal financial support for AI export packages could include the use of direct loans, loan guarantees, equity investments, co-financing, political risk insurance, credit guarantees, and other available means.

The Plan contemplates involvement in the AI export package strategy by a wide variety of agencies – including the Department of State, the Export-Import Bank, the U.S. Trade and Development Agency, and the U.S. International Development Finance Corporation – signaling the administration's position that the whole of government is responsible for maximizing the dissemination of American AI technology abroad.

Export controls

In parallel to this aggressive export strategy, the Plan also sets policies to reduce the likelihood that sensitive American AI technology ends up in high-risk destinations.

Among other things, it directs the DOC to develop new, more granular export controls on components and sub-systems in semiconductor manufacturing, rather than only complete systems. The Plan also directs federal agencies to collaborate with the private sector on enhancing chip location verification technology, and it directs coordination among federal agencies and the U.S. intelligence community to monitor emerging AI technology developments abroad. Contemplated results of this monitoring include broadened geographic export restrictions and enhanced end-use monitoring.

Also, the Plan envisions that the U.S. will actively participate in multilateral AI governance and standards-setting bodies, and engage in robust diplomatic efforts, in order to counter the influence of "adversary" nations. In support of the Plan's overall strategy, federal agencies are directed to develop a "technology diplomacy strategic plan for an AI global alliance," through which the U.S. would not only incentivize the adoption of its own technology, but also seek to prevent other nations from supplying "adversaries" with restricted technologies. For instance, where U.S. trading partners diverge from U.S. control frameworks, the Plan directs use of the Foreign Direct Product Rule and secondary tariffs in order to lengthen the government's reach beyond only its domestic production.

Notably, remotely accessible AI-related services such as compute capacity or cloud storage, may implicate the Plan's national security concerns insofar as they can be accessed surreptitiously by state-affiliated actors. This presents potential customer monitoring and compliance challenges for companies offering these services.

Security concerns

The Plan also proposes policy actions focused on evaluating AI systems for national security. The DOC's recently rebranded AI Safety Institute – now known as the Center for AI Standards and Innovation (CAISI) – is directed to build national security-focused AI evaluations and lead federal efforts to assess vulnerabilities arising from the use of "adversary" AI technology in critical infrastructure and "elsewhere in the American economy." CAISI is likewise designated to lead public-private coordination with frontier AI developers on assessing national security risks presented by those systems.

Finally, the Plan recognizes the risk that malicious actors may misuse AI's biological applications to create pathogens or other bioweapons. To address this risk, the Plan proposes a multitiered approach designed to screen for malicious actors among the customers of certain sophisticated biological tools and providers.

Takeaways

- Companies should continue to monitor developments in export controls and policy and prioritize compliance in this area. While the current administration has elsewhere signaled a reluctance to regulate the AI industry, the Plan suggests the same may not be true for AI-related export controls.

- Companies with relevant technology offerings may want to consider participating in the American AI Exports Program, particularly where advantageous financial or risk-reducing transaction structures backed by the federal government may be available.
- Companies that develop frontier models, or that provide compute capacity or cloud storage services, should ensure national security risks are accounted for in their risk assessments.

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