New Executive Order Addressing Early Government Access to Frontier AI Models

JUNE 2, 2026

Today, President Donald Trump announced a new executive order (EO) on how the federal government will collaborate with frontier artificial intelligence (AI) models to "modernize government and private sector information systems and harden them against external threats." The White House has hailed this EO as an important step in strengthening cybersecurity protections in light of new opportunities and risks presented by increasingly advanced AI models. The EO's central element is a voluntary framework for AI developers to work with the government in scrutinizing the cybersecurity implications of their new models before they are released to the general public. In the context of the Trump administration's generally deregulatory, "hands-off" approach to AI development, as reflected in key previous documents such as the July 2025 "America's AI Action Plan" and the December 2025 EO "Ensuring a National Policy Framework for Artificial Intelligence," this new EO marks a notable turn toward greater US government concern for the safety and security implications associated with continued AI maturation and sophistication.

This EO arrives against a backdrop of growing concern about the cybersecurity implications associated with the offensive capabilities of newly released frontier AI models. The latest models from leading US companies reportedly can identify and exploit software vulnerabilities at speeds previously unseen. That capacity, if kept in the hands of cyber defenders, can assist significantly in cybersecurity efforts; yet that same capacity, in the hands of malign cyber actors, can worsen the already challenging cyber threat environment.

The new EO represents a notable step in the wake of "America's AI Action Plan," which proclaimed the goal of enhancing America's "global AI dominance" in the AI race with China and other global rivals. The action plan identified three core pillars through which federal agencies are directed to support domestic AI development: (1) accelerating AI innovation; (2) building American AI infrastructure; and (3) leading in international AI diplomacy and security. Collectively, these pillars of the action plan emphasized expanding the availability of critical inputs for AI development, including facilitating the construction of data centers and supporting access to emerging energy sources such as nuclear fission and fusion, while also improving federal procurement processes for key AI technologies. The action plan further underscored the importance of "secure-by-design" development principles to ensure that AI innovation appropriately accounts for national security

considerations.

Today's EO also follows other AI-focused policies advanced by the Trump administration. These include its March 2026 "National Policy Framework for Artificial Intelligence," which outlines recommendations to guide Congress in developing a unified federal approach to AI regulation, its December 2025 EO that seeks to counter the state-level AI regulatory landscape and its January 2025 EO that articulated the administration's approach to reducing regulatory burdens and promoting AI innovation.

The order is organized around two principal components: a section addressing upgrading cybersecurity "for advanced AI" and a section governing the voluntary disclosure of what the EO terms "covered frontier models" prior to public release.

The section addressing upgrading US cybersecurity capabilities directs federal agencies to take accelerated action, within 30- and 60-day deadlines, to prioritize and strengthen the cybersecurity of national security, civilian federal and Department of War systems. Critically, the cybersecurity component of the EO is structured around a voluntary "clearinghouse" formed by the Treasury Department, other federal agencies and participating AI companies to identify and address security vulnerabilities in unreleased AI models. The EO requires the Department of Homeland Security and other official agencies to issue binding operational guidance, expand existing cybersecurity information-sharing programs to incorporate AI developers and facilitate access to advanced tools, including frontier AI models, for federal agencies, state and local governments, and critical infrastructure operators such as hospitals and banks, while prioritizing the cyber defense of national security, civilian federal and Department of War systems. In addition, the EO directs the Office of Management and Budget to assess whether existing federal grant programs can be leveraged to fund applicants developing advanced AI vulnerability detection capabilities, while also calling for additional hiring at the US Tech Force, the body of engineers recruited to modernize federal computer systems.

The frontier-model component of the EO directs the federal government to establish a classified, multilayered benchmarking review process—led by national security agencies—to determine which systems qualify as "covered frontier models" and to assess such models prior to public release. Under this voluntary framework, AI developers are invited to engage with the federal government to evaluate whether models under development meet the covered model designation and, if so, to provide prerelease access for a period of up to 30 days, subject to appropriate confidentiality, cybersecurity, insider risk and intellectual property protections. The framework further contemplates that such access may extend beyond federal agencies to include government-selected "trusted partners," enabling coordinated early access "to promote secure innovation and strengthen the cybersecurity of critical infrastructure." Critically, the EO stops short of imposing licensing requirements, mandatory safety testing or any government veto over launch decisions. Participating developers retain control over the timing of public release.

Lastly, the EO directs the attorney general to prioritize enforcement of federal criminal laws against actors who use AI to gain unauthorized access to, damage or exploit computer systems or data, including where AI tools are used to facilitate or further other criminal activity.

The EO builds on publicly reported voluntary testing arrangements between the Department of Commerce and several leading AI developers, including Anthropic, OpenAI, Microsoft, xAI and Google. The EO also adds a layer of classified evaluation by national security agencies that was not part of those earlier arrangements.

Notably, the EO represents a meaningful shift from the Trump administration's prior deregulatory posture toward AI while remaining materially less prescriptive than the regulatory regimes the European Union and China have adopted. The framework is voluntary rather than compulsory, relies on participation incentives rather than statutory enforcement authority and does not condition public release on government approval. The Office of the National Cyber Director reportedly briefed leading AI developers—including OpenAI, Anthropic and Reflection AI, along with representatives of cloud providers and semiconductor manufacturers—in advance of the EO's release, and the White House sought participation from AI company chief executives at today's signing ceremony, signaling that the administration views early industry buy-in as central to the framework's success.

For clients developing or releasing frontier AI models, the EO creates an immediate decision point: whether, when and on what terms to participate in the voluntary prerelease review framework. Companies should expect that the criteria defining a "covered frontier model" will be a focal point of agency rulemaking and stakeholder engagement in the coming months, and that the contours of prerelease information sharing—including the scope of materials provided, the handling of trade secrets and model weights, the duration of any prerelease window, and the identity of recipients (whether federal agencies alone or also critical infrastructure operators)—will require careful negotiation. Developers with existing voluntary arrangements with the Department of Commerce's Center for AI Standards and Innovation should evaluate how the new framework interacts with and potentially supplements those agreements.

For enterprise deployers, government contractors and operators of critical infrastructure, the EO may affect access to and the timing of new frontier model releases, the cybersecurity expectations attached to AI-enabled systems and the contours of information-sharing relationships with federal agencies through the Treasury-led clearinghouse. Although the EO's initiatives are framed as voluntary, its provisions may well migrate into procurement standards, sectoral cybersecurity guidance and contractual requirements over time, particularly for clients in regulated industries or those doing business with the federal government.

WilmerHale's Artificial Intelligence, Cybersecurity and Privacy and Defense and National Security practices continue to analyze the EO and stand ready to advise clients on engagement with the new framework, evaluation of participation risks and benefits, and the interaction between this EO and the broader patchwork of federal and state AI requirements. For further insights on emerging technologies and WilmerHale's analysis of the Trump administration's various AI and cyber policies, we encourage you to visit our AI Solutions resource.

Authors

Arianna Evers

PARTNER

arianna.evers@wilmerhale.com

+1 202 663 6122

Matthew G. Olsen

PARTNER

Chair, Defense, National Security and Government Contracts Practice

matthew.olsen@wilmerhale.com

+1 202 663 6359

Joshua A. Geltzer

PARTNER

joshua.geltzer@wilmerhale.com

+1 202 663 6404

Matthew R. Lewis

SENIOR ASSOCIATE

matthew.lewis@wilmerhale.com

+1 212 295 6505

Samson F. Cohen

SENIOR ASSOCIATE

samson.cohen@wilmerhale.com

+1 202 663 6175