WILSON SONSINI

Trump Administration Issues Executive Order on Advanced AI Innovation and Security

CONTRIBUTORS


Demian Ahn


Joshua F. Gruenspecht


Joseph (Tony) Misher


Kara D. Millard

ALERTS

June 11, 2026

Key Takeaways

- The Executive Order, Promoting Advanced Artificial Intelligence Innovation and Security (Order), directs the creation of a framework for developers of advanced frontier models to engage with the federal government for a voluntary pre-release review of the models.
- The Order also directs the Treasury Department, together with the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), to establish a clearinghouse to coordinate cyber vulnerability scanning, discovery, and patch distribution, in collaboration with private sector artificial intelligence (AI) and critical infrastructure companies.
- CISA must issue Binding Operational Directives (BODs) and other guidance to expedite cyber defense of civilian federal systems and expand use of AI-enabled defensive tools.
- The Order directs the Attorney General to prioritize prosecution of AI- and AI agent- facilitated computer crimes, identity theft offenses, and wire fraud schemes.
- Developers considering engagement with the federal government for model pre-release review will need to assess the scope of pre-release access and the safeguards available during the early access window.
- Companies seeking to become trusted partners should engage carefully with the U.S. government; those trusted partners may receive early access to covered frontier models, but also may be asked to disclose sensitive information and agree to continuing collaboration with the government.

Overview

On June 2, 2026, the White House issued the Order which announces that it is "the policy of the United States to promote AI innovation and security by working collaboratively with the private sector to modernize government and private sector information systems and harden them against external threats; to protect American ingenuity and intellectual property from exploitation and theft by adversaries; and to cultivate America's advanced AI-enabled capabilities."

The Order was issued at a time of heightened concern over the cybersecurity risks posed by frontier models with advanced cyber capabilities. The most advanced models have reportedly been used to discover security vulnerabilities with extraordinary speed—and such capabilities have enormous potential for both defensive and offensive use. Regulators around the world have reportedly expressed concern and raised questions about the risks posed by these technologies.

In this context, the Order directs the Departments of the Treasury, War, and Homeland Security, as well as the NSA, CISA, and the Attorney General, to take a more active role with respect to the risks posed by AI. However, the Order is consistent with the Trump administration's preference for

voluntary engagement with the private sector, and its policy of promoting AI innovation and managing the related risks without imposing "overly burdensome regulation."

Covered Frontier Models and the Voluntary Framework for Review

Section 3 of the Order requires the Secretary of the Treasury, the Secretary of War (through the NSA Director), and the Secretary of Homeland Security (through the Director of CISA), in consultation with the National Cyber Director, the Assistant to the President for Science and Technology, and the Secretary of Commerce (through the Director of the National Institute of Standards and Technology), within 60 days, to develop two related frameworks: a classified benchmarking process to identify "covered frontier models" and a voluntary pre-release engagement program for developers of such models.

The Classified Benchmark and Designation Process for Frontier Models

The Order mandates the creation and ongoing maintenance of a classified benchmarking framework to evaluate the "advanced cyber capabilities" of AI models and to determine when a system qualifies as a "covered frontier model." Notably, the authority to determine whether an AI model qualifies as a "covered frontier model" rests with the NSA Director, sitting under the Secretary of War (in consultation with other specified agencies), rather than with a civilian regulatory or standards-setting agency such as the Department of Commerce. This structure places the review of frontier models firmly within a national security and cyber defense framework, and the resulting process will likely operate as a classified intelligence function rather than being defined pursuant to a public rulemaking.

While the Order does permit developers to engage with the government on whether a given AI model is within scope, the threshold determination still poses practical difficulties. The Order does not define what constitutes "advanced cyber capabilities." Instead, that definition appears intended to emerge from within the classified process itself. The classified nature of this framework may create transparency challenges for AI developers, particularly because the Order provides that the assessment results will be shared with developers only "as appropriate." This phrasing leaves open the possibility that developers may receive limited insight into how their models are evaluated, and the Order sets no response timelines, which could introduce uncertainty into development planning and compliance efforts. Given the classified record and the absence of a defined designation standard, participating developers have limited ability to challenge a model's "covered frontier model" determination.

The Voluntary Pre-Release Framework

The Order directs the development of a voluntary framework under which a developer may take three steps: (1) ask the government to determine whether a model in development would qualify as a "covered frontier model;" (2) provide the federal government access to a covered frontier model for up to 30 days before planned release to other trusted partners; and (3) collaborate with the federal government to select those trusted partners who receive early access to promote secure innovation and the cybersecurity of critical infrastructure.

The 30-day early access window, which reportedly was 90 days in earlier drafts, places a pre-release copy of a frontier model in federal government hands. The Order conditions that access on "appropriate confidentiality, cybersecurity, insider-risk, and intellectual-property protection." Robust safeguards will be critical given that the models subject to review will represent both commercially sensitive proprietary technology as well as technologies having significant national security implications. The Order does not specifically cover how the government might consider obtaining a model and its underlying data, if at all, in the event that a developer declines to participate. Despite the Order's focus on voluntary compliance, the inclusion of the Secretary of Commerce in the participating group is a reminder that the President retains the authority to demand information from the private sector on commercial capabilities with national security implications. The Biden administration previously required model-makers to provide such information to the Department of Commerce via the Defense Production Act.

Still, for now, the Order expressly disclaims any authority to impose a mandatory licensing, preclearance, or permitting regime for the development, publication, release, or distribution of new AI models, including frontier models. The carveout preserves the framework's voluntary character, but does not speak to export controls. A model designated as a "covered frontier model" for its advanced cyber capabilities is a strong candidate for regulation under U.S. export controls, consistent with prior efforts to control certain AI model weights and software through the AI Diffusion Rule, which was rescinded in 2025, with a replacement rule expected.

A New Cyber Defense Hub: Federal Directives and Public-Private Collaboration

Section 2(d) directs the Secretary of the Treasury, in consultation with the NSA Director and the Director of CISA, to establish an AI cybersecurity clearinghouse in voluntary collaboration with AI developers and critical infrastructure operators. The clearinghouse will operate as a central hub for coordinating and deconflicting vulnerability scanning, discovering, and validating software vulnerabilities, and supporting the prioritization and distribution of remediation and patching efforts. Participation is voluntary and the clearinghouse's practical impact will hinge upon industry engagement and agency protocols governing information sharing and vulnerability disclosure.

Section 2(c) directs CISA to issue BODs and guidance to: (1) expedite cyber defense of federal information systems; (2) expand access to programs that support AI-enabled defensive tools; and (3) facilitate access to cybersecurity services, including, where appropriate, covered frontier models, for federal, state, and local authorities, and critical infrastructure operators. The third objective is notable because it positions the federal government as a potential conduit for critical infrastructure operators to access frontier AI capabilities, though its practical effect will depend on CISA's forthcoming guidance. Because BODs are legally binding on federal agencies and frequently incorporated into contracting requirements, companies with current or prospective federal contracts should closely review new BODs to assess whether additional cybersecurity obligations could arise. Relevant monitoring channels include Federal Risk and Authorization Management Program (FedRAMP) updates, agency-issued cybersecurity notices, and federal cybersecurity alerts.

Criminal Enforcement of AI-Enabled Crimes

Section 4 of the Order requires the Attorney General to prioritize enforcement of applicable federal criminal laws in the prosecution of offenses where AI tools are used or leveraged in furtherance of unlawfully accessing, damaging, or interfering with computer systems. Distinctively, the Order expressly encompasses the deployment of AI agents to unlawfully access data that is subsequently exploited for criminal or otherwise unlawful purposes. This provision reflects the federal government's recognition of the distinct risks posed by autonomous systems, positions agentic AI as a force multiplier for cybercriminal activity and establishes a clear directive for federal law enforcement to prioritize the investigation and prosecution of AI assisted offenses.

Cyber Strategy Synergies

The Order gives effect to several core pillars of the Trump administration's Cyber Strategy for America (Strategy) by translating strategic priorities into specific operative directives. The mandates set forth in Section 2—to harden national security, defense, and federal civilian information systems, and to expand AI-enabled defensive capabilities—directly advance Pillar Three: Modernize and Secure Federal Government Networks. Section 2 also supports Pillar Four: Secure Critical Infrastructure by directing CISA to issue guidance that facilitates critical infrastructure operators' access to cyber tools and covered frontier models, complemented by the Treasury-led AI cybersecurity clearinghouse. Finally, the enforcement priorities set forth in Section 4 reinforce the Strategy's emphasis on disrupting adversaries' cyber campaigns and uprooting criminal infrastructure. Both the Order and Strategy illustrate a growing need to address the evolving role of AI in amplifying the scale, speed, and sophistication of cyberattacks.

Wilson Sonsini routinely helps companies navigate complex issues pertaining to AI and Machine Learning. For more information or assistance, please contact any member of the Data, Privacy, and Cybersecurity or National Security and Trade practices at Wilson Sonsini.