Skadden | AInsights

June 9, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

New AI Executive Order Calls for Frontier Model Security, Early Government Access and AI-Enabled Cyber Defense

Executive Summary

- **What's new:** On June 2, 2026, President Trump issued an executive order directing U.S. government agencies to accelerate AI-enabled cybersecurity initiatives to design a voluntary framework for engagement with developers of frontier AI models before broader release, and to prioritize criminal enforcement against AI-enabled cyberattacks.
- **Why it matters:** The EO signals that frontier models with advanced cyber capabilities may require closer public-private coordination. Although the framework is voluntary, it could provide a foundation for more substantial federal oversight of AI model development.
- **What to do next:** Frontier AI model developers and critical infrastructure companies should consider monitoring forthcoming guidance from CISA, preparing for the classified benchmarking process and determining whether product release timelines should account for a potential government access period of up to 30 days

On June 2, 2026, President Donald Trump issued an executive order (EO), "Promoting Advanced Artificial Intelligence Innovation and Security." The EO directs U.S. government departments and agencies to accelerate AI-enabled cybersecurity initiatives to:

- Design a voluntary framework for engagement with developers of frontier AI models before broader release of such models to trusted partners.
- Prioritize criminal enforcement against AI-enabled cyberattacks.

The EO signals the administration's recognition that frontier models with advanced cyber capabilities may require closer public-private coordination. Notably, the EO does not impose requirements related to licensing or preclearance.

Although the contemplated framework would be "voluntary," it could lead to a more structured process for federal engagement with frontier AI model developers, particularly with respect to advanced cybersecurity focused AI models, and could provide a foundation for more substantial federal oversight of AI model development.

While some commentators have welcomed this measured approach, others have warned it could prove a stepping stone to more prescriptive regulation. Still others have asserted the voluntary approach is insufficient given the threats presented by certain AI models.

New AI Executive Order Calls for Frontier Model Security, Early Government Access and AI-Enabled Cyber Defense

AI developers — particularly those building frontier models — as well as critical infrastructure companies and other companies using AI-enabled cybersecurity tools should consider monitoring U.S. government actions related to this EO, such as the forthcoming guidance from the Cybersecurity and Infrastructure Security Agency (CISA).

In addition, frontier AI model developers may want to:

- Be prepared to evaluate whether their models meet the forthcoming "covered frontier model" designation.
- Prepare for the classified benchmarking process.
- Consider whether product release timelines should account for a potential government access period of up to 30 days.

Background

The EO follows a series of administration actions promoting U.S. AI leadership, including the January 2025 EO "Removing Barriers to American Leadership in Artificial Intelligence," the December 2025 EO "Ensuring a National Policy Framework for Artificial Intelligence" and other initiatives aimed at accelerating AI adoption and reducing regulatory burdens.

The most recent EO continues this trend while also introducing "new national security considerations that require coordinated action across executive departments and agencies."

Although the EO pointedly contrasts the Trump administration's approach with that of the Biden administration, there are elements of continuity. In 2023, the Biden White House secured voluntary commitments from leading AI developers to test the safety and security of their systems before public release.

The current EO's voluntary framework can be seen as a continuation of that approach, now reoriented around cybersecurity and national security concerns.

Key Provisions

Upgrade American Systems for Advanced AI

The EO imposes a series of 30- and 60-day deadlines on federal agencies to bolster cyber defenses across government systems. Specifically:

- The **Committee on National Security Systems** is instructed to prioritize the cyber defense of National Security Systems within 30 days. The secretary of War must similarly prioritize cyber defense of **Department of War**[1] information systems within the same time frame.
- The secretary of **Homeland Security**, through the director of CISA, is directed to release Binding Operational Directives to expedite cyber defense of civilian federal systems, expand federal cybersecurity programs that enhance AI-enabled defensive tools and facilitate access to cybersecurity tools — including covered frontier models — for agencies, state and local authorities, and critical infrastructure operators such as rural hospitals, community banks and local utilities.
- Within 30 days, the secretary of the **Treasury**, in consultation with the national cyber director and the directors of the National Security Agency (NSA) and CISA, are directed to form an "AI cybersecurity clearinghouse" in voluntary collaboration with the AI industry and critical infrastructure operators. The clearinghouse will coordinate scanning for software vulnerabilities, validate discoveries, and prioritize remediation and patch distribution.
- The director of the **Office of Management and Budget** must identify whether any federal grant programs have funding available for applicants developing advanced AI vulnerability detection.
- The **Office of Personnel Management** must expand hiring pathways for cybersecurity specialists through the U.S. Tech Force within 60 days.

Secure Frontier Model Deployment

The EO directs multiple departments and agencies to take a number of significant actions to secure private sector AI development on an accelerated 60-day timeline.

First, they must develop and maintain a classified benchmarking process to assess the advanced cyber capabilities of AI models and determine the threshold at which a model should be designated a "covered frontier model." The director of the NSA will make such determinations in consultation with the national cyber director, the assistant to the president and director of the White House Office of Science and Technology Policy, the CISA director and other representatives of the Department of War.

Second, when an AI model is designated a "covered frontier model" under the forthcoming classified benchmarking process, the model's developer may provide the government with access to the model — subject to confidentiality, cybersecurity, insider-risk and intellectual property (IP) protections — for up to 30 days before releasing it more broadly.

[1] Congress has not yet acted on the administration's renaming of the Department of Defense.

New AI Executive Order Calls for Frontier Model Security, Early Government Access and AI-Enabled Cyber Defense

Following the access period, the EO contemplates a narrower release to "trusted partners" selected in collaboration with the government, rather than immediate broad public release. Covered frontier models may also be made available for federal agencies, state and local authorities, and critical infrastructure operators (such as rural hospitals, community banks and local utilities).

Critically, the EO expressly provides that nothing in it "shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models."

Protect Against Criminal Actors

The attorney general is directed to prioritize enforcement of federal criminal statutes — including 18 U.S.C. §§ 1028, 1030, and 1343 — against anyone who uses AI to illegally access or damage a computer without authorization, or who uses AI while engaged in such illegal access to further any other crime. This includes breaching public or private information technology (IT) systems and employing AI agents to unlawfully access data that is subsequently used for a criminal or unlawful purpose.

The EO in Global Context

The U.S. approach comes amid a global race to develop appropriate regulatory and oversight models that achieve national objectives. Other jurisdictions have moved toward more formalized control of advanced AI.

The European Union's AI Act establishes a binding, risk-based regulatory framework, imposing mandatory obligations on providers of "general-purpose" AI systems — such as large language models — and "high-risk" AI systems such as those used for employee recruitment or credit scoring purposes. It sets significant penalties for noncompliance.

In the EU and U.K., data protection authorities may expect prior engagement or consultation where frontier AI model deployments present heightened risk to individuals, for example, where data protection impact assessments identify high residual risks.

In addition, the **U.K.'s AI Security Institute** conducts pre-deployment testing and evaluation of frontier models for safety and security risks, working with leading developers on a basis that, while currently voluntary, reflects a more institutionalized government role in model evaluation than the U.S. framework.

Against this backdrop, the EO's voluntary, access-based approach — coupled with its express disclaimer of any licensing or preclearance requirement — positions the U.S. as comparatively light-touch.

Practical Takeaways

- **Frontier AI model developers should assess whether and how to participate in the proposed voluntary framework.** Although the EO emphasizes that participation in the frontier model framework is voluntary and expressly disclaims any licensing or preclearance requirement, companies developing models that could be designated as "covered frontier models" should expect significant government interest in engagement.

  Although the EO does not contemplate the imposition of penalties for nonparticipation, companies that choose not to participate may find themselves at a disadvantage in securing government contracts, gaining early access to federal cybersecurity resources or being selected as "trusted partners" for early model access.
- **Prepare for the classified benchmarking process.** The EO directs agencies to develop a classified process for assessing whether models meet the "covered frontier model" threshold. AI developers should begin internal assessments of their models' cyber capabilities and consider what personnel and processes they will need in place to engage with classified government evaluations — including obtaining or maintaining appropriate security clearances.
- **The 30-day access window requires advance planning.** Participating frontier AI model developers may need to account for a potential government access period of up to 30 days before releasing these models more broadly. Companies should begin planning internal workflows to accommodate this window, including protocols for protecting IP and confidential information during government review. Customers awaiting new frontier models should correspondingly prepare for possible delays in public availability, as the pre-release access window may extend development-to-release timelines.
- **Criminal enforcement signals heightened scrutiny.** The direction to the attorney general to prioritize criminal enforcement against AI-enabled cyberattacks signals that the Department of Justice (DOJ) is likely to bring cases in this space. Companies should consider reviewing their internal controls to ensure that their AI systems and AI-powered agents cannot be used — whether by internal actors or external threat actors — to access data or systems without authorization.
- **Monitor the cybersecurity clearinghouse.** The AI cybersecurity clearinghouse represents a new public-private coordination mechanism for vulnerability scanning and patch distribution. AI developers and critical infrastructure operators should consider monitoring the formation of this body as well as early engagement to shape its processes and benefit from coordinated vulnerability remediation.

New AI Executive Order Calls for Frontier Model Security, Early Government Access and AI-Enabled Cyber Defense

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Aleksander J. Aleksiev
Associate / London
44.20.7519.7212
aleksander.aleksiev@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

William Chandler
Associate / Washington, D.C.
202.371.7341
william.chandler@skadden.com

Summer Associate **Ryan Penney** contributed to this article.