JENNER & BLOCK

New AI Executive Order: Key Takeaways For Companies Developing Advanced AI Models

Client Alerts

June 8, 2026
By: Aaron R. Cooper, Caroline Cease, Will Weaver, Steven J. Arango, Justin Iannacone, Tashrima Hossain

On June 2, the Trump administration issued an Executive Order (EO) on artificial intelligence and cybersecurity—just weeks after abruptly pulling a prior version at the eleventh hour, with tech leaders already assembled at the White House for a signing ceremony. In the wake of reports on the new capabilities of frontier models to identify and exploit cybersecurity vulnerabilities at scale, the EO sets out the administration's framework for voluntary government pre-release review of "covered frontier models," along with orders to federal departments and agencies to strengthen cybersecurity defenses in light of advanced AI and a directive to DOJ to prioritize enforcement of AI-enabled hacking crimes.

The Administration has framed the EO as consistent with its broader posture of favoring a deregulatory approach to AI, while still addressing national security concerns about advanced AI capabilities. As such, the EO is interesting not just for what it says, but also how it has evolved, with the pre-release review period reduced from 90 days to just 30 days. This reflects the government's continued recognition of the national security value in voluntary pre-release testing, while also reacting to apparent concerns within the White House and industry of opening the door too far to federal government regulation of AI innovation. How the framework is implemented, and industry's interest in participating, will be the test for the administration's approach.

The Executive Order

The EO establishes three broad policy changes, aligned with a policy statement announced in Section 1 that emphasizes a spirit of public-private collaboration (rather than regulation) and a reminder that the federal government is also working quickly to understand and respond to these recent developments: "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."

First, the EO directs departments and agencies to take prompt steps to upgrade federal information systems with AI-enabled cyber defenses. Specifically, the EO directs the Cybersecurity and

Infrastructure Security Agency (CISA) to issue Binding Operational Directives (i.e., new security requirements applicable to certain federal information technology systems) within 30 days to prioritize cyber defense of civilian federal systems and enable access to cybersecurity tools and services for operators of critical infrastructure such as rural hospitals, community banks, and local utilities. It also directs the Treasury Department to establish a voluntary AI cybersecurity clearinghouse to coordinate vulnerability scanning and patching across government and critical infrastructure. This first policy initiative reflects the federal government's efforts to improve its own cybersecurity in light of model capabilities, and to make the benefits of its work more broadly available to critical infrastructure, including the financial sector, and critical infrastructure industry should closely track the creation of this clearinghouse. Funding resources and talent programs are also highlighted.

Second, the EO establishes a framework for AI developers to voluntarily submit "covered frontier models" for government review for a period of up to 30 days before planned release to trusted partners. Under the framework, developers may engage the federal government to determine whether a model under development meets the covered frontier model designation, a non-public benchmark that the federal government will develop and classify. The EO does not say how the benchmark will work, but it will involve an interagency process and could signal a different way to consider model capabilities other than the compute thresholds that the federal government has previously relied upon. The EO also directs the use of confidentiality, cybersecurity, insider-risk, and intellectual property protections for those models subject to the government's review, which will be critical to those developers who want to protect their models from further dissemination—either in response to public disclosure requests or through adversary espionage efforts. The EO also opens up collaboration with the government to identify trusted partners that will receive early access to covered frontier models to strengthen critical infrastructure cybersecurity. Here, the EO emphasizes that the pre-release testing program does not "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."

Third, the EO directs the Attorney General to prioritize criminal enforcement of existing statutes against anyone using AI to facilitate unauthorized computer access or related crimes.

What Comes Next

The June 2 EO reflects the administration's preference for relying on voluntary collaboration rather than regulation but also signals a recognition that some action may be necessary for the federal government to understand and prepare for the national security risks posed by advanced AI capabilities. But the EO will not be the end of the story, as the policy debates that shaped the order's turbulent path remain unresolved and will continue to shape the EO's implementation and any future policy action.

In some ways, the EO builds on existing voluntary frameworks—including the Center for Artificial Intelligence Standards and Innovation's (CAISI) recently expanded testing agreements—as a primary method to understand and address AI security. It remains to be seen, however, how strong the voluntary regime will be. With no binding commitments, companies can choose when and how to engage with the government's review process. At the same time, the EO opens the door to more extensive public-private collaboration on managing security risks going forward, providing a proof-of-concept for a more robust oversight model. Model developers that decline to engage in pre-release testing could face criticism should a released model later prove harmful to national security.

Implementation will be the next battleground: AI developers will face immediate decisions about whether to participate in the voluntary 30-day pre-release review framework. The June 2 EO is far from the final word on federal AI policy. If future AI models present unresolved cybersecurity risks, or if AI facilitates a major cybersecurity breach, the policy debate over mandatory review is likely to resurface.

What It Means for Your Company

The EO raises several immediate considerations for companies developing or deploying advanced AI:

- **The voluntary review framework is now in place, but its reach is limited by design.** The EO establishes a voluntary 30-day pre-release window for "covered frontier models" but explicitly prohibits mandatory licensing, preclearance, or permitting requirements. Companies developing AI models should assess whether to engage the federal government in determining whether their systems are likely to meet the "covered frontier model" threshold (to be defined through a classified benchmarking process) and consider engaging proactively with the voluntary framework. Before making models available, developers should insist on appropriate assurance that their information will be protected legally and technically from further dissemination.

- **State law risks remain elevated.** Even though the Trump administration previously ordered federal agencies to act to preempt state AI laws, states like California continue to adopt their own AI regulations, and the EO does not address state preemption. States have signaled that they are not waiting for federal policy to settle before acting. Companies operating across multiple states should continue monitoring and assessing any new compliance requirements imposed by state-level AI regulations.

- **The political calculus is shifting.** The EO reflects the current balance of power inside the administration, but that balance remains contested. Congress retains independent tools (i.e., subpoena power, oversight hearings, legislation), and with midterms approaching, members on both sides have strong electoral incentives to act on AI issues that generate public concern. Companies should factor congressional dynamics into their federal engagement strategies, not just the White House's posture.

Companies should assess now whether their AI models are likely to meet the “covered frontier model” threshold and what participation in the voluntary framework would mean for their development timelines. Jenner & Block’s AI practice is ready to advise clients on regulatory compliance and the latest developments in AI policy.

Related Attorneys

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333

Caroline Cease
Partner
ccease@jenner.com
+1 202 639 6056

Will Weaver
Partner
wweaver@jenner.com
+1 202 639 6870

Steven J. Arango
Associate
sarango@jenner.com
+1 202 637 6348

Justin Iannacone
Associate
jiannacone@jenner.com
+1 415 293 5949

Tashrima Hossain
Associate
thossain@jenner.com
+1 415 293 5944

Related Capabilities

AI Task Force

Critical and Emerging Technologies

Data Privacy and Cybersecurity

Government Controversies and Public Policy Litigation

Stay Informed →