June 12, 2026

What the New AI Executive Order Means for Businesses That Use AI

By: David L. Hayes , Melanie Jolson , Adine Mitrani , Jason Raylesberg

What You Need To Know

- In a significant shift from the current administration's previous innovation-first approach, the White House has established a *voluntary* framework that gives it up to 30 days to review frontier models before public release.
- A new AI cybersecurity clearinghouse, to be set up by July 2, 2026, will coordinate AI-assisted vulnerability scanning, validate findings, and manage patch distribution across critical infrastructure sectors including healthcare, banking, and utilities.

Related Professionals

David L. Hayes
Partner · Intelle

Melanie Jolson
Counsel · Priva
Cybersecurity

Adine Mitrani
Associate · Inte
Property

- Companies that rely on frontier AI models but don't build them face a new dependency risk: the 30-day review window could delay access to new capabilities, with some real competitive consequences for businesses whose differentiation depends on early adoption.
- An emerging "trusted partners" framework could grant select organizations early access to frontier AI models ahead of general release, making the criteria for that designation a significant and still-undefined competitive consideration.
- Although framed as voluntary, the order formalizes government presence in the AI development cycle.

The federal government has taken its most significant step yet toward oversight of AI, with President Donald Trump issuing a new executive order (EO) that establishes a voluntary review framework under which developers give the government access to frontier large language models for up to 30 days before releasing them to their trusted partners, and then the general public. It also creates an “AI cybersecurity clearinghouse” to review vulnerabilities. While the order is aimed squarely at frontier labs, its effects will ripple through every sector of the economy that has come to rely on those labs’ models.

Background

For most of the past two years, the administration’s posture toward AI development leaned toward permissiveness. Their stated view was that a government

Related Practices

→ Corporate

→ Corporate Governance

→ Privacy & Cybersecurity

Related Industries

→ AI & Machine Learning

Share

→ Subscribe

minimal-intervention approach would keep American AI competitive globally. That stance appears to have changed as it became clear that the newest generation of AI models possess capabilities that introduce new risks including the ability to discover software vulnerabilities at a scale and speed never before anticipated. Government officials and operators of critical infrastructure grew concerned that such capabilities, in the wrong hands, could be used to identify and exploit systemic weaknesses across the economy before defenders even knew the threat existed.

The EO signed on June 2, 2026, is Washington's response. "Advanced AI capabilities make our Nation stronger," it states, "but also introduce new national security considerations that require coordinated action."

What the Order Does

The order establishes two new mechanisms for AI oversight.

1. **Pre-Release Window:** The first mechanism is a voluntary pre-release review window for frontier AI models. Companies that develop systems the government designates as "covered frontier models" (a threshold to be determined through a classified benchmarking process) can allow the government up to 30 days to assess a new model before the company shares it with their trusted partners; broader public release typically follows that partner phase, so the practical delay to the open market can run longer than 30 days. The review period was originally proposed to last 90

days but was trimmed to 30 in the version that was ultimately signed.

Importantly, the order explicitly bars the government from turning this into a mandatory licensing or preclearance requirement; participation is framed as voluntary, though with the federal government representing a significant customer for many of these systems, "voluntary" may carry considerable weight in practice. As written, the order contains no enforcement mechanism for non-participants, no penalty for a developer that opts out, and no authority to delay or block a release; any developer that declines faces commercial and reputational consequences, not legal ones.

2. **AI Cybersecurity Clearinghouse:** The second mechanism is an AI cybersecurity clearinghouse, to be set up by the Treasury Department by July 2, 2026. The clearinghouse will coordinate the AI-assisted scanning of systems for software vulnerabilities, validate findings, and manage the disclosure and distribution of patches. The goal is to close the window between when a vulnerability is discovered and when it can be exploited.

What It Means If You Build *With* AI, Not Just *On* It

Most companies are users of this frontier technology, not creators of it. They build on top of frontier models; integrating them into functionality such as customer service platforms, software development pipelines, fraud detection systems, and clinical decision-support tools. For these businesses,

the order introduces a new kind of dependency risk.

If a frontier model is subject to a pre-release government review, that 30-day window (plus any subsequent trusted-partner phase) could delay when the model, and whatever new capabilities it carries, becomes accessible to the broader market. Because that delay generally lands on all market participants at once, it does not by itself reorder the competitive field for most companies; they are waiting together. The competitive stakes arise mainly in two situations: where a competitor obtains trusted-partner early access that others cannot, or where the delayed release carries a specific capability or fix a business is relying on in the near term.

Truster Partner Early Access

Under the EO, frontier model developers are encouraged to work with the government to identify "trusted partners" who can receive access ahead of general release. The criteria for trusted-partner status are not yet defined, but if that designation becomes a meaningful commercial advantage, granting early access to capabilities that competitors must wait for, the selection process may matter as much as the models themselves.

Early access tiers are already a reality in the market: ahead of this order, some developers opened advanced access to their newest models to small groups of partners before expanding to peers and leading Fortune 500 companies. For growing companies, the practical question is whether the company can get into a developer's early-access

program at all, and on what terms, well before the government's role is even settled.

Bug Fixes

Further, if a known bug or security flaw in the current model is slated to be fixed in the next release, a 30-day hold means many companies may have to live with that flaw a month longer, even though the patch already exists. Smaller companies, in particular, may have to divert engineering resources to build workarounds during the hold.

Relatedly, the cybersecurity clearinghouse carries its own downstream implications. Organizations that use AI-powered security tools, or whose infrastructure could be subject to AI-driven vulnerability scanning, are now operating in an environment the clearinghouse is designed to govern. The order specifically names rural hospitals, community banks, and local utilities as intended beneficiaries of expanded cybersecurity services. More broadly, the clearinghouse will shape what AI-assisted security tools can disclose, to whom, and when. Those are operational decisions that will affect risk management across industries.

Criminal Enforcement

The EO also directs the attorney general to prioritize enforcement of federal criminal statutes against anyone who uses AI to illegally access or damage computer systems. This includes prosecuting individuals who breach public or private IT systems using AI, or who deploy AI agents to unlawfully access data that is then used for criminal purposes. The relevant statutes are 18 U.S.C. 1028 (identity fraud), 18 U.S.C.

1030 (computer fraud and abuse), and 18 U.S.C. 1343 (wire fraud). They are not new, but the order's explicit focus on AI-enabled violations signals that the Justice Department views these tools as a growing vector for cybercrime and will treat their misuse as an enforcement priority.

For businesses, this provision is a reminder that much of the legal framework governing AI misuse is already in place. Organizations deploying AI agents or automated systems that interact with external networks or data sources should implement controls to ensure their use cases do not inadvertently cross into unauthorized access, particularly as AI systems and AI agents become more autonomous and capable of taking actions their operators may not fully anticipate.

The Larger Signal

The order's most consequential aspect may be what it signals, rather than what it requires. Even in its voluntary form, the pre-release review formalizes the government's presence in the AI development cycle, creating a more structured relationship between frontier model developers and federal agencies that could harden into binding requirements over time.

Some EO advocates are already pushing for exactly that, arguing that voluntary frameworks cannot keep pace with regulating advancing capabilities. Others flag a discretion concern: Because the framework puts the government in the room when developers decide who gets early access, policy analysts warn it could be wielded against companies that fall out of favor with the administration.

There is also the question of drift from voluntary into mandatory. Even without new legislation, "voluntary" terms have a way of migrating into procurement standards, sector cybersecurity guidance, and contract requirements; a development worth tracking for anyone in, or selling into, regulated industries or government contracting.

Companies working with AI models should take a few concrete steps in view of the EO:

- Know which frontier models your product depends on and avoid roadmap commitments that assume day-one availability of a not-yet-released model.
- If possible, seek out early-access relationships. A seat in a model developer's trusted-partner or early-access tier can become an asset.
- Build model portability into your systems' architecture. The ability to swap or fall back to an alternative model lessens the impact of any one provider's release delay.
- Check your customer contracts and procurement exposure. If you sell into regulated industries or to the government, watch for these voluntary norms surfacing as security or sourcing requirements; and make sure your commitments leave room to absorb them.

Related Insights

Publications

AI in the Boardroom: What Directors Need to Know Now

May 27, 2026

Publications

Building Responsible AI Agents: Design and Development Choices for Navigating Third-Party Platform Risks

May 04, 2026

View more related insights