ALERT

White House Executive Order Signals Federal Focus on Frontier AI Cybersecurity

By Shruti Bhutani Arora, Anne M. Voigts, Brian E. Finch, Mark L. Krotoski, Ya'ara Z. Barnoon, Nathan D. Banks

TAKEAWAYS

- The EO does **not impose mandatory licensing or preclearance requirements** for AI development. Instead, it builds a **voluntary, but operationally consequential framework** for collaboration between government and industry on cyber defense, vulnerability sharing and secure deployment of advanced "frontier" AI models.
- The EO directs federal agencies to **prioritize cybersecurity risks associated with advanced AI systems** and **establish a voluntary framework for federal engagement with developers of certain "covered frontier models**."
- The EO comes amid **broader federal-state policy tension over AI regulation**. States continue to legislate in this area, with states like New York and California passing a series of laws regulating frontier models. A bipartisan discussion draft released earlier this week would create a federal AI governance framework and temporarily preempt certain state AI laws, and, following the White House's earlier EO, Ensuring A National Policy Framework For Artificial Intelligence, the Department of Justice intervened in xAI's lawsuit challenging Colorado's algorithmic discrimination law.

06.10.26

On June 2, 2026, the White House issued an executive order (EO) titled Promoting Advanced Artificial Intelligence Innovation and Security, establishing a federal policy framework that prioritizes AI-driven cybersecurity while preserving an innovation-first, voluntary regulatory model. The EO was reportedly edited to respond to industry concerns and is framed as a pro-innovation measure. The EO expressly states that it does not create a mandatory licensing, preclearance or permitting requirement for the development, release or distribution of AI models. At the same time, it strengthens cybersecurity across

federal and critical infrastructure systems using AI-enabled tools, seeks to protect intellectual property and technology from adversarial exploitation, and directs closer coordination with the private sector on AI security risks and mitigation strategies. Notably, the federal government is increasingly treating advanced AI capabilities as a cybersecurity and national security issue, particularly where frontier models may be capable of discovering, validating or exploiting software vulnerabilities at scale.

The EO also follows a growing trend at the state level, where states such as California and New York have begun imposing frontier AI-specific governance, transparency and incident-reporting obligations on frontier developers, including requirements aimed at assessing and mitigating risks of catastrophic or "critical harm."

Key provisions of the EO include:

- **Federal cyber defense priorities.** Within 30 days, federal officials are tasked with taking measures in line with the purpose of the memo to prioritize the cyber defense of National Security Systems, Department of War information systems and civilian Federal Government information systems. The EO directs CISA, in consultation with OMB and other White House officials, to issue Binding Operational Directives and other guidance to expedite cyber defense measures, expand AI-enabled defensive tools, and facilitate access to cybersecurity tools and services for federal agencies, state and local authorities, and operators of critical infrastructure.
- **AI cybersecurity clearinghouse.** The EO also directs the Treasury Department, in consultation with the National Cyber Director, NSA and CISA, to form an AI cybersecurity clearinghouse within 30 days. The clearinghouse is intended to coordinate and deconflict software vulnerability scanning, validate vulnerabilities, and prioritize remediation and patch distribution in voluntary collaboration with AI companies and critical infrastructure operators.
- **Classified benchmarking for covered frontier models.** Within 60 days, Treasury, NSA, CISA, NIST and other federal officials must develop and maintain a classified benchmarking process to assess the advanced cyber capabilities of AI models and determine when a model should be designated a "covered frontier model." The NSA Director, in consultation with other federal officials, will determine whether a model meets that threshold.
- **Voluntary pre-release access framework.** The EO directs federal officials to design a voluntary framework through which AI developers may engage with the federal government to determine whether models under development qualify as covered frontier models. Developers would also be able to provide the federal government with access to covered frontier models, subject to confidentiality, cybersecurity, insider-risk and intellectual property protections, for up to 30 days before releasing those models to other trusted partners. This 30-day period has drawn notable attention: Earlier reporting suggested that draft versions of the order contemplated a longer review window, including up to 90 days.
- **Enforcement focus on AI-enabled cybercrime.** The EO directs the Attorney General to prioritize enforcement of existing federal criminal laws against actors who use AI to illegally access or damage computers, or who use AI in connection with unauthorized access to further other crimes. The order

specifically references: computer fraud and abuse (18 U.S.C. § 1030); identity fraud (18 U.S.C. § 1028); and wire fraud (18 U.S.C. § 1343), including circumstances where AI is used to facilitate unauthorized access, data exfiltration or cyber-enabled crimes. This underscores increasing DOJ attention to AI-assisted cyber intrusion and autonomous agent misuse.

Why This Matters for AI Governance

Although the EO stops short of creating a mandatory approval regime for frontier AI models, it makes clear that advanced AI capabilities are increasingly being viewed through the lens of cybersecurity and national security.

For developers of frontier AI models, the order puts particular emphasis on model capability, secure pre-release engagement with the federal government and governance over early access to covered frontier models. The EO directs federal agencies to develop a classified benchmarking process to assess advanced cyber capabilities and to design a voluntary framework through which developers may engage with the government about whether models under development qualify as covered frontier models. It also contemplates federal access to covered frontier models for up to 30 days before release to other trusted partners, subject to confidentiality, cybersecurity, insider-risk and IP protections.

The EO is also relevant to companies deploying AI-enabled cybersecurity tools or AI agents that interact with critical infrastructure. The EO directs federal agencies to expand access to AI-enabled cybersecurity tools for government agencies, state and local authorities, and critical infrastructure operators, and to establish an AI cybersecurity clearinghouse focused on vulnerability scanning, validation, remediation and patch distribution. It also directs the Attorney General to prioritize enforcement against actors who use AI, including AI agents, to unlawfully access computers, data or information.

Key Compliance Considerations

Companies developing or deploying covered frontier models, AI-enabled cybersecurity tools or AI agents that interact with sensitive systems should consider the following steps:

- **Assess model capability and release governance.** Evaluate whether any current or planned models could fall within the EO's concept of a covered frontier model, particularly where a model may have advanced cyber capabilities or could be used to identify, validate or exploit software vulnerabilities.
- **Document model evaluation and release decisions.** Maintain clear records of model capability assessments, security reviews, mitigation measures and release approvals. This documentation may be important for companies that choose to participate in the EO's voluntary federal engagement process or need to explain their AI governance practices to customers, regulators or business partners.
- **Updating AI risk governance frameworks**. Address cybersecurity misuse scenarios, AI-enabled unauthorized access risks, DOJ enforcement priorities and potential exposure from the deployment of AI agents or AI-enabled security tools.

- **Strengthen controls for unreleased models.** Evaluate who has access to unreleased models, how early-access partners are selected. And what technical and contractual safeguards apply. Companies that participate in a voluntary pre-release access framework should also assess confidentiality, insider-risk, cybersecurity and IP protections before sharing sensitive model information.
- **Coordinate privacy, cybersecurity and AI governance reviews.** Ensure that product, engineering, security, privacy and legal teams have a clear internal process for escalating higher-risk AI deployments before launch. Companies should also prepare for increased federal collaboration expectations where AI systems interact with critical infrastructure, sensitive systems or vulnerability detection programs.
- **Review vulnerability disclosure and incident response processes.** Evaluate whether vulnerability findings are validated, prioritized and remediated through documented processes, and whether information-sharing with government, vendors or critical infrastructure partners is subject to appropriate legal, confidentiality and security controls. Companies should also consider whether patch management programs should be updated in light of the EO's clearinghouse coordination.
- **Evaluating participation strategies.** Companies developing frontier models or AI-enabled cybersecurity tools should consider whether and how to participate in voluntary government engagement processes, including pre-release model sharing, clearinghouse initiatives or other public-private cybersecurity programs.
- **Aligning cybersecurity and AI teams.** Companies should ensure that cybersecurity, AI governance, engineering, legal and compliance teams are aligned on emerging federal collaboration expectations, particularly where AI systems may be used for vulnerability detection, cyber defense, model deployment or other security-sensitive functions.

Board-Level Questions

Boards should consider directing management to evaluate several key questions:

- **AI exposure.** Do any current or planned systems approach "frontier model" capabilities, or otherwise have advanced cyber capabilities that could implicate the EO's covered frontier model framework?
- **Cybersecurity posture**. Are vulnerability detection, disclosure, remediation and patching programs aligned with emerging federal expectations for AI-enabled cybersecurity?
- **Government engagement.** Should the company proactively participate in AI cybersecurity clearinghouse initiatives, frontier model review processes or other voluntary public-private collaboration programs?
- **Legal and compliance readiness.** Is the organization prepared for increased DOJ scrutiny of AI-enabled unauthorized access, data exfiltration or other cyber-enabled activity?
- **Intellectual property protection.** What safeguards are in place if the company engages with a government pre-release review framework, particularly where sensitive model information, proprietary architecture or unreleased capabilities may be shared?

Pillsbury helps clients navigate AI governance, data privacy, cybersecurity and regulatory compliance, including model risk assessments, cybersecurity and regulatory litigation, data-use governance, incident response, and engagement with emerging federal and state AI requirements.

pillsbury