BALANCING INNOVATION AND RISK—PRESIDENT TRUMP'S EXECUTIVE ORDER AIMS TO REVIEW SECURITY IMPLICATIONS OF HIGH-RISK AI MODELS

Date: 4 June 2026

US Policy and Regulatory Alert

By: Marne Marotta, Scott J. Gelbman, Guillermo S. Christensen, Jake Bernstein, Finch Fulton, Varun M. Jain, Andrew H. Tabler, Liam J. Row, Abby Dinegar

OVERVIEW

On 2 June 2026, President Donald Trump signed an Executive Order entitled Promoting Advanced Artificial Intelligence Innovation and Security (the EO). The EO represents a significant development as the first action by the Trump Administration to directly confront the national security implications of advanced artificial intelligence (AI) models, while maintaining the Administration's firmly pro-innovation posture. The EO is notable for four key reasons: (1) an explicit prohibition on mandatory AI licensing, preclearance, or permitting requirements for AI model development or distribution; (2) the creation of a new classified "covered frontier model" designation controlled by the Director of the National Security Agency (NSA), (3) a directive to the Attorney General to prioritize criminal enforcement against actors who weaponize AI to illegally access or damage computer systems; and (4) aggressive whole-of-government cybersecurity timelines, with most provisions requiring action within just 30 days. After internal disagreements over the timing of certain provisions, the White House appears to have struck a balance on high-risk AI standards, notably including an amended voluntary framework and benchmark standards against which future AI models will be evaluated.

With the release of recent high-risk generative AI models, the threats posed by AI have become increasingly prominent, as have the threats posed to AI systems. Although the White House has released its AI Policy Framework and Executive Orders to halt state AI regulation, it had not yet addressed the national security implications of high-risk frontier models—until now. This EO balances the Administration's pro-innovation and deregulatory posture with a collaborative framework for private companies to work with the federal government on cybersecurity infrastructure for high-risk AI models.

CYBERSECURITY

The EO prioritizes cyber defense and security through the Committee on National Security Systems, the Department of War, and the Department of Homeland Security—all of which are subject to an aggressive 30-day action timeline. The Cybersecurity and Infrastructure Security Agency (CISA) is tasked with creating "Binding Operational Directives and other guidance" related to national security across the federal government. CISA is also tasked with facilitating access to cybersecurity resources for agencies, state and local authorities, and operators of critical infrastructure. The EO directs the Secretary of Treasury to form an AI cybersecurity clearinghouse, in voluntary collaboration with the AI industry and operators of critical infrastructure, to coordinate vulnerability scanning, discovery, and remediation. The cybersecurity provisions within the EO aim to create a more consolidated effort to address AI risks across the federal government.

FRONTIER MODELS

The focal point of the Administration's risk-mitigation efforts lies in the third section of the EO, related to Secure Frontier Model Deployment. “Frontier model” refers to the most advanced, cutting-edge AI models—those whose cyber capabilities, such as automated hacking and sophisticated system-control tactics, meet a threshold to be determined through a classified benchmarking process. Given the threats these models could present to networks and internet infrastructure, if left unregulated, the White House issued the EO as a regulatory middle ground—a voluntary framework that promotes engagement with and access to such models.

The EO mandates the development of a classified benchmarking process to assess the cyber capabilities of AI models, including the creation of a “covered frontier model” designation. This process will include a voluntary framework that allows AI developers to engage and collaborate with the federal government through protected agreements.

Critically, the EO expressly prohibits construing any of its provisions as authorizing mandatory governmental licensing, preclearance, or permitting requirements for the development, publication, release, or distribution of AI models. This provision explicitly frames the order as a rejection of the prior administration's regulatory approach, positioning deregulation as a national security and economic competitiveness strategy. Consistent with the “America First” posture throughout the EO, the Administration resolves the ongoing tension in AI governance—innovation against security—decidedly in favor of voluntary frameworks and industry collaboration, reserving enforcement authority for bad actors rather than imposing compliance burdens on developers.

Through this collaboration, the federal government plans to strengthen critical infrastructure cybersecurity, while companies designated as “trusted partners” will receive early access to covered frontier models to promote secure innovation.

BUILDING UPON THE CURRENT FRAMEWORK

Currently, the Center for AI Standards and Innovation within the National Institute of Standards and Technology (NIST) facilitates collaboration between the government and the private sector through voluntary guidelines and best practices. While not stated explicitly in the EO, the order appears to provide a similar voluntary standards framework through NIST oversight—only now with a primary focus on more sophisticated frontier models.

Notably, while NIST has traditionally been the home of AI related benchmarks and standards, the EO primarily designates [CJV1.1]the Secretaries of Treasury, War, Homeland Security through the Directors of NSA and CISA to take the lead with the Secretary of Commerce, through the Director of NIST, serving in a consultative role. These Secretaries are all jointly tasked with the rollout and enforcement of the benchmark and standards provisions of the EO. The Director of NSA is specifically designated as the authority to determine whether a model meets the “covered frontier model” threshold. The benchmarks themselves will be classified, so many questions around this order will remain publicly unanswered even after the 60-day development period.

TAKEAWAY

Although the EO's provisions are voluntary and the benchmark framework will be classified, this order signals the direction the Administration plans to take on future AI action: monitor high-risk AI systems while encouraging innovation. The explicit prohibition on mandatory AI licensing regimes reinforces the Administration's commitment to federal preemption and regulation. At the same time, the EO's criminal enforcement provisions direct the Attorney General to prioritize prosecution under 18 U.S.C. §§ 1028, 1030, and 1343, among other applicable statutes, against anyone who utilizes AI to illegally access or damage a computer without authorization, including through the deployment of AI agents. This signals that the Administration views AI-related threats as both a national security and law enforcement priority.

As the framework and benchmarks are developed over the next 30 to 60 days, the respective agencies will likely look to the private sector for guidance and collaboration. If your company is developing frontier models or working within the cybersecurity space, now is the time to engage in the process. While voluntary, these benchmarks will serve as the basis for categorizing future AI models and establishing national security standards. Just as NIST's AI Risk Management Framework was foundational to federal AI standards, this high-risk framework will be foundational to future cybersecurity standards for AI models.

Our team is tracking these developments in real time—from frontier AI oversight and federal preemption to state compliance obligations and emerging cybersecurity frameworks—and translating them into practical guidance. We are happy to discuss how these shifts may affect your AI model decisions, cyber practices, and federal partnerships, and what steps you can take now to prepare. Please feel free to reach out for a targeted readiness assessment, a legislative strategy briefing, or further analysis.

KEY CONTACTS

MARNE MAROTTA
PARTNER

WASHINGTON, DC
+1.202.778.9202
MARNE.MAROTTA@KLGATES.COM

SCOTT J. GELBMAN
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.9067
SCOTT.GELBMAN@KLGATES.COM

GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM

JAKE BERNSTEIN
GLOBAL AI AND INNOVATION PARTNER

SEATTLE
+1.206.370.7608
JAKE.BERNSTEIN@KLGATES.COM

FINCH FULTON
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.4565
FINCH.FULTON@KLGATES.COM

VARUN M. JAIN
OF COUNSEL

WASHINGTON, DC
+1.202.778.9030
VARUN.JAIN@KLGATES.COM

ANDREW H. TABLER
GOVERNMENT AFFAIRS ADVISOR

WASHINGTON, DC
+1.202.778.9041
ANDREW.TABLER@KLGATES.COM

LIAM J. ROW
GOVERNMENT AFFAIRS ANALYST

WASHINGTON, DC
+1.202.778.9250
LIAM.ROW@KLGATES.COM

ABBY DINEGAR
GOVERNMENT AFFAIRS ANALYST

WASHINGTON, DC
+1.202.778.4562
ABBY.DINEGAR@KLGATES.COM