

# WHITE HOUSE EXECUTIVE ORDER ON ADVANCED AI INNOVATION AND SECURITY: IMPLICATIONS FOR THE TECHNOLOGY AND DEFENSE SECTORS

On June 2, 2026, President Trump issued an executive order (the Order) entitled *Promoting Advanced Artificial Intelligence Innovation and Security*, signaling the Administration’s continued focus on accelerating the development and deployment of advanced artificial intelligence (AI) capabilities for national security purposes while addressing the cybersecurity risks associated with increasingly sophisticated AI systems.

The Order directs the Secretaries of the Treasury, War, and Homeland Security to establish a classified benchmarking process designed to evaluate the advanced cyber capabilities of AI models. Through this process, federal agencies will assess whether a model possesses capabilities that warrant designation as a “covered frontier model,” a classification that may carry significant implications for government oversight, collaboration, and deployment opportunities.

To facilitate engagement between the public and private sectors, the Order also establishes a voluntary framework through which AI developers may work with the federal government to evaluate whether models under development meet the criteria for covered frontier model designation. As part of this framework, the federal government may obtain early access to certain advanced AI models, enabling agencies to assess potential national security, cyber defense, and operational applications before broader commercial deployment.

The Order further emphasizes enforcement against the malicious use of AI technologies. Specifically, it directs the U.S. Attorney General to prioritize the investigation and prosecution of criminal activity involving AI-enabled misconduct, including unauthorized access to computer systems, cyber intrusions, and the use of AI tools to facilitate other unlawful activities. This

## PEOPLE

Brian E. Kaveney

Stewart G. Mayo, CIPP/US

## SERVICES AND INDUSTRIES

Industrial Security and Security  
Clearance



directive reflects the Administration's growing concern regarding the use of advanced AI capabilities in offensive cyber operations and other emerging threat vectors.

The Order seeks to strengthen the federal government's cybersecurity posture and promote innovation in AI-driven security technologies. It instructs the Director of the Office of Management and Budget, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency (CISA), to evaluate the availability of federal grant funding for organizations developing advanced AI-based vulnerability detection and cybersecurity solutions. The Order also directs CISA to issue Binding Operational Directives (BODs) aimed at accelerating cybersecurity improvements across federal information systems and expanding agencies' access to AI-enabled cybersecurity tools and services.

Accordingly, the Order reflects a broader Administration strategy to leverage advanced AI capabilities as a national security asset while simultaneously addressing the cybersecurity risks posed by increasingly powerful AI systems. Technology companies, AI developers, defense contractors, cybersecurity providers, and other industry participants should closely monitor implementation of the Order, particularly the development of the covered frontier model framework, evolving government access and evaluation mechanisms, and potential funding opportunities related to AI-enabled cybersecurity technologies. These initiatives may create new avenues for public-private collaboration while also shaping future regulatory and operational expectations for organizations developing or deploying advanced AI systems.