wiley

ALERT

New AI Executive Order Addresses Frontier Models and Cybersecurity Vulnerabilities

June 3, 2026

On June 2, 2026, President Trump signed an Executive Order (EO), *Promoting Advanced Artificial Intelligence Innovation and Security*, that provides a framework for assessing and addressing cybersecurity vulnerabilities that may be identified by new frontier AI models. The EO directs a range of federal agencies to establish processes for information sharing around new frontier AI models with heightened vulnerability identification and exploitation capabilities, and efforts to remediate identified vulnerabilities. For the private sector, the EO establishes a voluntary process for AI model developers to submit AI models for federal review prior to broader release, and provide critical infrastructure entities with early access to these models in order to strengthen cybersecurity protections.

Below, we summarize the key directives of the EO, as well as what industry can expect next.

Directives for Updating Systems for Advanced AI

Section 2 of the EO, *Upgrading American Systems for Advanced AI*, requires various federal agencies to take action to prepare federal government and private-sector systems for advanced AI tools within 30 days of the EO – that is, by July 2, 2026. In particular:

- Cyber Defense for Key Federal Systems: The Committee on National Security Systems must prioritize the cyber defense of National Security Systems, as defined in 44 U.S.C. 3552(b)(6)(A); and the Secretary of War must prioritize the cyber defense of Department of War (DoW) information systems.
- Cyber Defense Directives and Guidance for Civilian Federal Government Systems and Critical Infrastructure: The Secretary

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

AI Executive Order
Artificial Intelligence (AI)
Cyber and Privacy Investigations, Incidents & Enforcement
Cybersecurity
Emerging Technologies
Government Contracts
Government Contracts
Privacy, Cyber & Data Governance
Trump Administration Resource Center

of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA), must consult with the Office of Management and Budget (OMB), the Assistant to the President for National Security Affairs, and the National Cyber Director, to release Binding Operational Directives and other guidance that (1) promotes cyber defense of civilian information systems in the federal government; (2) expands federal programs that enhance AI-enabled defensive tools; and (3) gives federal and state agencies and operators of critical infrastructure access to advanced cybersecurity tools including, where appropriate, covered frontier models.

- AI Cybersecurity Clearinghouse: The Secretary of the Treasury, in partnership with other agencies, must form an AI cybersecurity clearinghouse to coordinate identification, validation, and remediation of software vulnerabilities. The AI industry and operators of critical infrastructure may voluntarily collaborate in the clearinghouse.
- Federal Grants: The Director of OMB, in coordination with other agencies, must identify federal grant programs that have funding that can be directed to applicants to develop advanced AI vulnerability detection.

Finally, within 60 days of the EO (by August 1, 2026), the Director of the Office of Personnel Management must expand the United States Tech Force Information Cybersecurity Specialist hiring and placement pathways.

Directives for Benchmarking and Voluntary Early Access for Frontier Models

Section 3 of the EO, *Secure Frontier Model Deployment,* requires a new classified benchmarking process to assess the advanced cyber capabilities of AI models. The Secretaries of the Treasury, War (through the National Security Agency, or NSA), and Homeland Security (through CISA) are charged with developing and maintaining the benchmarking process, in consultation with the National Cyber Director (NCD), the Assistant to the President for Science and Technology (APST), and the National Institute of Standards and Technology (NIST). The EO anticipates sharing these assessments generated from this benchmarking process with AI developers and researchers.

The same departments and agencies will also establish a threshold for when an AI model should be designated as a "covered frontier model." The Director of NSA, in consultation with the NCD, the APST, the Director of CISA, and other representatives of the DoW, will be responsible for the designations of covered frontier models.

Finally, the above-identified agencies and departments are required to "design a voluntary framework with AI developers" through which developers may:

- Work with the federal government to determine whether a model meets the threshold for a covered frontier model.
- Provide the federal government with "access to covered frontier models, subject to confidentiality, cybersecurity, insider-risk, and intellectual property protection, use, and nondisclosure requirements," for 30 days prior to release of the models.

- Collaborate with the federal government to "select trusted partners that will have early access to covered frontier models to promote secure innovation and strengthen the cybersecurity of critical infrastructure."

The EO includes a disclaimer that nothing under Section 3 authorizes or establishes a "mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models."

The new benchmarking process and voluntary framework for early access to covered frontier models has a 60-day timeline, with deliverables required by August 1, 2026.

Directive to Prioritize Enforcement Against Criminal Actors

Section 4 of the EO, *Protection Against Criminal Actors*, addresses the use of AI to perpetrate digital crimes, including illegally accessing computers and information technology systems, identity fraud, and wire fraud. Specifically, the EO requires the Attorney General to prioritize enforcement of federal criminal laws related to fraud and related activity against anyone who uses AI to illegally access or damage a computer or uses AI while engaged in illegal access while committing another crime. The EO specifically identifies 18 USC § 1028, which is the primary federal statute for prosecuting identity fraud; 18 USC § 1030, commonly known as the Computer Fraud and Abuse Act, which is used to prosecute computer crimes; and 18 USC § 1343, the federal wire fraud statute. Criminal activities identified by the EO include breaching a public or private IT system or using AI agents to access protected data later used in a crime.

What to Expect Next

Given the EO's short timelines – with directives for actions to be taken this summer – stakeholders should monitor the various agencies and departments tasked with deliverables, including new CISA Binding Operational Directives and other guidance from CISA, a new AI Cybersecurity Clearinghouse, and the new benchmarking process and opportunity for early access for frontier models.

***

Wiley's Artificial Intelligence and Government Contracts practices counsel clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly moving area. Please reach out to the authors with any questions.