VENABLE LLP

New EO on AI, Innovation, and Security

June 04, 2026

Jennifer Daskal and Caitlin Clarke

On June 2, the White House issued its previously delayed executive order (EO), *Promoting Advanced Artificial Intelligence Innovation and Security*. Slightly modified from a previously leaked draft, the EO does three key things:

1. Directs federal agencies to take new actions to protect federal and other critical infrastructure from cyber-related threats
2. Directs the creation of a new "AI cybersecurity clearinghouse" to identify vulnerabilities and distribute applicable patches and
3. Directs the creation of a voluntary information-sharing system, pursuant to which AI developers are encouraged—but are not required—to share "covered frontier models" with the federal government 30 days prior to broader release. (An earlier leaked draft would have made this advance notice provision 90 versus 30 days.)

Overall, the EO reflects a recognition of the evolving threat environment, the importance of coordinated action across both the public and private sectors to defend against cybersecurity threats, and the importance of increased coordination with critical infrastructure operators. The following delves into each in more detail.

Protection of Federal and Other Critical Infrastructure

The EO gives the Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA), 30 days to issue Binding Operational Directives designed to strengthen cybersecurity across federal civilian systems and to support access to advanced, AI-enabled cybersecurity tools by state and local authorities and operators of critical infrastructure, such as hospitals, community banks, and local utilities. Once issued, Binding Operational Directives operate as a mandate to other federal agencies that they must follow.

The EO also directs the secretary of war to take action, also within 30 days, to prioritize the cyber defense of Department of War information systems.

In addition, the Office of Personnel Management is directed to expand federal cybersecurity hiring pathways, reflecting the administration's effort to increase technical cybersecurity expertise across government.

New AI Cybersecurity Clearinghouse

Within 30 days, the secretary of the treasury, working in coordination with the national cyber director, the director of the National Security Agency, and the secretary of homeland security, is required to create a new AI cybersecurity clearinghouse. Per the EO, the clearinghouse should involve the "voluntary collaboration" of the AI industry and critical infrastructure operators. The stated goals: To coordinate and deconflict vulnerability scanning; identify and validate software vulnerabilities; and coordinate remediation and distribution of security patches.

Relatedly, the director of the Office of Management and Budget is directed to determine whether there are available federal grant program dollars that can be directed toward applicants developing advanced AI vulnerability detection.

Advance Access to Covered Frontier Models

The EO defines a new category of "covered frontier models" and implements a voluntary advance sharing system between frontier labs and the federal government.

Several federal entities, including Treasury, the National Security Agency (NSA), and CISA, are directed to develop a classified benchmarking process to assess the cyber capabilities of advanced AI systems and to designate certain AI models as "covered frontier models." The designation itself will be made by the director of the NSA, in coordination with other federal entities.

The EO also directs federal agencies to establish a voluntary framework with AI developers pursuant to which developers would be able to engage with the federal government to determine whether a model under development qualifies as a covered frontier model. Under this same voluntary framework, AI developers would share the model with the federal government for up to 30 days before broader release and would coordinate with the federal government to select other trusted partners that would have early access to the models in order to "promote secure innovation and strengthen the cybersecurity of critical infrastructure."

The EO doubles down on the voluntary nature of this arrangement: "Nothing in this section shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models."

Although voluntary, these provisions will set standards and expectations that frontier AI companies will be expected to, and likely will, follow. As agencies develop benchmarking standards and operational procedures, participation in the framework may increasingly become a market expectation for AI developers, particularly those seeking to demonstrate alignment with evolving federal cybersecurity priorities and best practices.

Implications and Looking Ahead

The short timelines reflects a sense of urgency, as the White House works through ways fortify federal systems, as well as those at the state and local level. The commitment to getting key defensive tools in the hand of critical infrastructure is a critical element of this strategy. As is the focus on identifying vulnerabilities and patch sharing.

That said, key details are still being developed. The EO directs multiple federal agencies to develop the rules, technical standards, guidance, and implementation measures in the coming days. We will be watching those developments closely.

For further information on evolving laws, regulations, and policy developments relating to artificial intelligence and cybersecurity, please contact Jennifer Daskal and Caitlin Clarke.