Now & Next

Technology Alert

June 10, 2026

Executive Order on AI and security: Fortifying American AI systems against new cyber threats

By Jason Hirsch and Elijah Rockhold

The order focuses on improving cyber-readiness across all levels of government and enhancing public-private collaboration through voluntary, pre-release review of frontier AI models.

What's the impact?

- AI developers will have a standardized framework for pre-release government review of a frontier model's cybersecurity defenses. Developers should evaluate the terms of participation, including the reviewing entities, IP protections, and confidentiality.
- Government contractors, cybersecurity firms, and critical infrastructure operators should monitor the order's reach. Benchmarking guidelines could become procurement standards. Prioritization of cyber-readiness and new grant opportunities should drive demand for cyber services. New federal guidance will expand access to improved cyber tools and services.
- The order marks a notable shift in the administration's AI policy to a much more active federal role at the intersection of AI and cybersecurity.

On June 2, President Trump signed an Executive Order, "Promoting Advanced Artificial Intelligence Innovation and Security." The order outlines the administration's plan "to promote AI innovation and security by working collaboratively with the private sector to modernize government and private sector information systems and harden them against external threats." The plan is designed to leverage increased public-private coordination to bolster the cybersecurity of American "artificial intelligence" systems used across government and the private sector, without restricting growth and innovation.

The order addresses three areas, with a focus on the first two. The most notable development is the administration's establishment of a "voluntary framework" through which AI developers can confidentially share a "covered frontier model" for review of the model's cybersecurity defenses and vulnerabilities before it is made available to the public. The framework builds off recent voluntary agreements between some prominent AI developers and the Commerce Department's Center for AI Standards and Innovation to facilitate similar assessments.

Second, the order calls for upgrades to critical elements of America's cybersecurity infrastructure. Finally, the order prioritizes federal enforcement of cyber-related crimes aided by the use of AI.

The order represents a meaningful shift in the administration's AI policy. Although its central feature is a "voluntary framework," the order sets out a much more active role for the federal government at the intersection of AI and cybersecurity than the "light-touch" regulatory approach reflected in the administration's prior AI pronouncements. The order arrives amid increased concern about the capabilities, and potential for misuse by bad actors, of the most recent frontier models, which can reportedly identify cyber vulnerabilities at unparalleled speed and precision.

Upgrading US cyber defenses

The order directs multiple federal agencies to take expedited action—within 30 days—to prioritize the cyber defense of critical American AI systems. Specifically, the order requires:

- The Secretary of the Treasury, in collaboration with other federal agencies, the AI industry, and operators of critical infrastructure, to form a voluntary "AI cybersecurity clearinghouse" that will coordinate and facilitate evaluation and (where necessary) remediation of AI models' security vulnerabilities.
- The Secretary of War and the Committee on National Security Systems to prioritize any necessary improvements to the nation's cyber defense.
- The Secretary of Homeland Security, in consultation with other agencies, to release "Binding Operational Directives" designed to:
    - Prioritize and accelerate the cyber-readiness of civilian federal government information systems

    - Establish or expand federal programs to enhance AI-enabled cybersecurity tools
    - Facilitate access to cybersecurity tools, including frontier models, for federal agencies, state and local authorities, and operators of critical infrastructure like hospitals, banks, and utilities
- The Director of the Office of Management and Budget to determine whether any federal grant funding can be directed toward applicants "developing advanced AI vulnerability detection," and the US Tech Force (within 60 days) to prioritize hiring additional cybersecurity specialists.

Pre-Deployment review of frontier models

The order tasks a group of federal agencies, particularly those focused on national or cyber security, with establishing a classified benchmarking process to assess the cyber capabilities of advanced AI models within 60 days. The process will have two main components: determining which AI systems constitute "covered frontier model[s]" and evaluation of the cyber-readiness of those models, all toward a goal of collaboratively strengthening the cyber protections of covered frontier models. This model-evaluation process likely flows from voluntary collaborations between the Commerce Department's Center for AI Standards and Innovation and a handful of prominent AI developers, which similarly facilitated pre-deployment evaluation of security risks for significant models. Each of those collaborations was reportedly subject to its own bespoke negotiation and terms. The order outlines a more formalized, consistent approach that should be more efficient for participating entities.

Importantly, the order suggests that the pre-release review will not be limited to the government but will also include some set of "trusted partners"—private-sector entities selected by the federal government—that will receive pre-release access to the frontier models to help identify and remediate cyber vulnerabilities.

As part of the benchmarking process, the order directs the agencies to design a "voluntary framework" under which private-sector AI developers can engage with the government to determine whether their models qualify as "covered frontier model[s]." For those models that qualify, the framework will provide a path for developers to submit the models for review of their cyber protections, for a period of up to 30 days prior to a model's public release. The framework must cover key terms of the voluntary review process, including appropriate confidentiality, cybersecurity, insider-risk, and intellectual-property protections, and the government's eventual position on those terms—or at least the perception of their position across the AI industry—will likely have a significant impact on the success of the program. Before those processes kick off, AI developers should monitor how some of the order's important threshold issues are addressed, such as the evaluation criteria for a "covered frontier model" and the selection criteria for "trusted partners."

Critically for the AI industry, the order makes clear that no mandatory licensing regime will be imposed as part of the framework, nor will the government have a veto over the release of a model, or even when the model can launch (outside of the 30-day review period).

Prioritizing enforcement of AI-aided criminal activity

Finally, the order directs the attorney general to prioritize enforcement of existing federal criminal laws, including identity fraud and computer fraud and abuse, in cases where the alleged perpetrator(s) used AI to commit the crime. This prioritization represents a continued acknowledgement by the federal government, dating back to the last administration, that AI can be a force multiplier for criminal activity, and therefore its use for illegal means should be subject to a commensurately enhanced response from law enforcement.

Implications for businesses

The order's impact will be most acutely felt by developers of frontier models, who should begin evaluating whether engagement through the framework would be strategically advantageous, and, if so, under what terms they would (and would not) participate. Key considerations include:

- Who may review their model (including private-sector "trusted partners")
- How intellectual property rights will be protected
- How confidentiality will be maintained, and
- The duration of any review period.

Clients will benefit from preparing for these negotiations well in advance.

THE EFFECTS OF THE ORDER ARE NOT LIMITED TO AI DEVELOPERS

- Government contractors may eventually face more direct consequences from the order. While the order emphasizes voluntariness, and the substance of the benchmarking is confidential, that could evolve. The benchmarks could become procurement standards or contractual requirements for the federal government. The order's standards could also be included by the National Institute of Standards and Technology's Cybersecurity Framework or other similarly influential industry guidance.
- The cybersecurity industry should benefit from the order's prioritization of cyber defense. As the administration's prioritization migrates outward, to the broader AI-developer community and enterprises broadly deploying AI, it will generate increased demand for cyber services. More directly, the order points federal grant money toward the cybersecurity industry and opens new avenues for government partnerships. These shifts will benefit existing cyber

companies and could also create opportunities for new market entrants.

- State and local governments, as well as "operators of critical infrastructure," also stand to benefit from the order, which calls for federal agencies to provide those entities with access to new cyber tools and services, including frontier models, to significantly improve their cybersecurity capabilities.

Nixon Peabody's AI, Digital Platforms, and Emerging Technologies Team can counsel clients—from AI developers to cybersecurity companies to local governments—on how best to navigate the order and how it fits into the broader federal and state AI regulatory landscape. The team can help clients evaluate potential engagement with the "voluntary framework," including preparation for negotiations over the terms of participation in a cyber review. For clients outside of frontier-model development, the Team can advise on the range of risks and opportunities the order presents for your organization, and how you can mitigate the former while capitalizing on the latter.

For more information on the order, the broader regulatory landscape around AI, and how either may impact your organization, please contact your Nixon Peabody attorney or the authors of this alert.

Jason D. Hirsch
415.984.8308
jhirsch@nixonpeabody.com

Elijah T. Rockhold
617.345.6128
erockhold@nixonpeabody.com