Cooley

AI Executive Order Creates Voluntary Framework for Frontier Models, Advances Critical Infrastructure Cybersecurity

June 8, 2026

On June 2, 2026, President Donald Trump signed a new executive order (EO) addressing the intersection of artificial intelligence and cybersecurity. This EO has direct implications for AI developers, critical infrastructure companies, and any business operating at the intersection of AI and cybersecurity. The EO directs federal agencies to take a series of actions (many within 30 to 60 days) with the purposes of upgrading the cyber defenses of government information systems, establishing a voluntary framework for the deployment of advanced AI models and reinforcing criminal enforcement against the misuse of AI. Below, we summarize the key provisions of the EO and highlight potential implications for AI developers, critical infrastructure operators and other stakeholders.

Importantly, the EO does not impose mandatory licensing or pre-clearance; the EO's voluntary framework for frontier model deployment creates a structured pathway for engagement with the federal government, but participation is not mandatory. **The EO also does not create new civil liability, and it does not address AI governance beyond the cybersecurity context**.

Background

The EO frames the United States' continued leadership in AI as a product of private-sector innovation and a regulatory environment that avoids overly burdensome restrictions. At the same time, the EO acknowledges that advanced AI capabilities introduce new national security considerations requiring coordinated federal action.

Key issues for developers

The most significant provision for AI developers is the direction to the secretary of the Treasury, the secretary of Defense (through the director of the National Security Agency (NSA)) and the secretary of Homeland Security (through the director of the Cybersecurity and Infrastructure Security Agency (CISA)), in consultation with other senior officials, to develop within 60 days:

- **A classified benchmarking process**. This classified benchmarking process will assess the advanced cyber capabilities of AI models and determine the threshold at which a model should be designated a "covered frontier model" for purposes of the EO. The director of NSA will make such designations in consultation with the National Cyber Director, the assistant to the president for Science and Technology, the director of CISA and other Department of Defense representatives. The benchmarking will be classified, and the process is to be "developed and maintained," presumably to reflect the changing "frontier" of development, in contrast with the EU AI Act's publicly available risk-tier classification criteria.
- **A voluntary developer framework**. The EO provides for a voluntary framework through which AI developers would be able to:
    - Engage the federal government to determine whether models under development meet the "covered frontier model" designation.
    - Provide the government with access to covered frontier models for up to 30 days before releasing them to trusted partners (subject to confidentiality, cybersecurity, insider risk and intellectual property protections).
    - Collaborate with the government to select trusted partners for early access to promote secure innovation and strengthen critical infrastructure cybersecurity.

Notably, the EO expressly provides that nothing in that portion of the EO 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. This voluntary framing is consistent with the administration's broader deregulatory posture.

Additional elements of the EO

In addition to the benchmarking process and voluntary developer framework, the EO imposes additional instructions to other government agencies regarding AI.

Upgrading federal cyber defenses

The EO imposes aggressive 30-day deadlines on federal agencies to prioritize and enhance the cybersecurity of government information systems. The Committee on National Security Systems and the secretary of Defense are each directed to prioritize the cyber defense of National Security Systems and Department of Defense information systems, respectively. The secretary of Homeland Security, acting through the director of CISA, is directed to release Binding Operational Directives and other guidance to:

- Expedite the cyber defense of civilian federal information systems.
- Establish or expand federal programs that enhance AI-enabled defensive tools.
- Facilitate access to cybersecurity tools and services – including, where appropriate, covered frontier models – for agencies, state and local authorities, and critical infrastructure operators, such as rural hospitals, community banks and local utilities.

AI cybersecurity clearinghouse

The secretary of the Treasury, in consultation with the National Cyber Director, the secretary of Defense(through the director of the NSA) and the secretary of Homeland Security (through the director of CISA), is directed to establish an AI cybersecurity clearinghouse. This clearinghouse would operate in voluntary collaboration with the AI industry and critical infrastructure operators to coordinate and deconflict vulnerability scanning, discover and validate such vulnerabilities, and coordinate and prioritize remediation and distribution of vulnerability patches.

Grant funding and workforce

The director of the Office of Management and Budget, in coordination with the National Cyber Director and the director of CISA, is directed to identify federal grant programs with available funding that can be directed toward advanced AI vulnerability detection. Separately, within 60 days, the director of the Office of Personnel Management must expand the US Tech Force information cybersecurity specialist hiring and placement pathways.

Deadline	Agency/actor	Required action
30 days	CISA	Release Binding Operational Directives on cyber defense of civilian federal systems
30 days	Committee on National Security Systems/ secretary of Defense	Prioritize cyber defense of National Security Systems
60 days	Treasury, NSA, CISA	Develop classified benchmarking process and voluntary developer framework
60 days	Office of Personnel Management	Expand US Tech Force cybersecurity hiring pathways
Ongoing	Attorney general	Prioritize enforcement against AI-facilitated cyber crimes

The EO also directs the attorney general to prioritize enforcement of 18 USC §§ 1028 (identity fraud), 1030 (computer fraud and abuse) and 1343 (wire fraud), and all other applicable federal criminal laws, against anyone who utilizes AI to illegally access or damage a computer without authorization, or who utilizes AI in furtherance of such illegal access to commit other crimes. This includes breaching any public or private information technology system or employing AI agents to unlawfully access data or information that is subsequently used for a criminal or unlawful purpose. While these statutes already apply to AI-facilitated conduct, the EO signals the administration's intent to make such prosecutions a priority.

Key next steps

The EO's voluntary framework for frontier model deployment creates a structured pathway for engagement with the federal government, but participation is not mandatory.

For AI developers

- Monitor the forthcoming classified benchmarking process and assess whether models may meet the "covered frontier model" threshold.
- Establish an internal working group to evaluate the costs and benefits of voluntary framework participation before the 60-day window closes.
- Ensure IP, confidentiality and cybersecurity protocols can accommodate government pre-release access if you choose to participate.

For critical infrastructure operators (healthcare, financial services, utilities)

- Monitor CISA for Binding Operational Directives expected within 30 days.
- Evaluate participation in the AI cybersecurity clearinghouse.
- Assess eligibility for federal grant funding for AI vulnerability detection.

For all companies

- Review cyber incident response plans in light of the heightened federal enforcement priority.
- Assess whether your AI deployments introduce any potential liability exposure under the prioritized statutes.

Importantly, the EO does not impose mandatory licensing; it does not create new civil liability; and it does not address AI governance beyond the cybersecurity context.

How Cooley can help

Cooley's AI and cyber/data/privacy teams are available to advise on voluntary framework participation, IP and confidentiality protections, and incident response planning.

Key Contacts

Travis LeBlanc **Washington, DC**	**tleblanc@cooley.com** **+1 202 728 7018**
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Sean Quinn New York	squinn@cooley.com +1 202 728 7075