June 3, 2026

Trump's AI Cybersecurity Order: A Voluntary Framework with Mandatory Implications

Authors: Regina Sam Penti, Edward R. McNicholas, Sabrina Kim

On June 2, 2026, President Trump signed an executive order titled "Promoting Advanced Artificial Intelligence Innovation and Security" (the "Order"), which establishes a new framework for government collaboration with the AI industry on cybersecurity and the secure deployment of advanced AI models.[1] While voluntary in form, the Order builds significant institutional architecture, including classified benchmarks administered by the National Security Agency (NSA) and a government-managed pre-release review window, that marks the administration's first direct engagement with pre-deployment evaluation of frontier AI capabilities.

This alert examines the Order's key provisions and their implications for AI developers, critical infrastructure operators, enterprises deploying AI tools, and investors in AI-driven companies.

Key Takeaways

- The Order creates a *classified* benchmarking process, administered by the NSA, to identify "covered frontier models," a significant institutional choice that places an intelligence agency in the lead role for evaluating commercial AI capabilities.
- Although the Order is explicitly voluntary and disclaims any licensing or pre-clearance authority, it builds institutional infrastructure (including pre-release review windows, a "trusted partners" tier, and a vulnerability-sharing clearinghouse) that could harden into de facto compliance expectations.

- The Order's pre-release access framework and cybersecurity clearinghouse each carry intellectual property, competitive, and information-sharing implications that warrant careful evaluation before participation.

- DOJ enforcement of existing criminal statutes against AI-enabled cyberattacks, including by autonomous AI agents, signals heightened attention to enterprise AI deployments that interact with external systems.

Background

The Order is the latest in a series of AI-related executive actions. In January 2025, President Trump revoked the Biden-era AI executive order and directed development of an "AI Action Plan."[2] Subsequent executive orders addressed AI education (April 2025),[3] national cybersecurity (June 2025),[4] and promotion of AI technology exports (July 2025).[5] On July 4, 2025, President Trump signed the "One Big Beautiful Bill Act," which enacted sweeping new requirements for AI and technology companies, including stringent restrictions on foreign influence in the AI supply chain, broad extraterritorial rules targeting "prohibited foreign entities," enhanced domestic sourcing mandates, and rigorous supply chain integrity requirements.[6] In December 2025, President Trump signed an executive order establishing a national AI policy framework and directing federal agencies to challenge state-level AI regulations.[7] In March 2026, the White House issued legislative recommendations proposing a single national standard for AI governance.[8] The new Order builds on those deregulatory and export-promotion efforts while pivoting toward a cybersecurity-focused posture, and, notably, toward pre-deployment evaluation of advanced AI capabilities.[9]

Key Provisions

1. Upgrading American Systems for Advanced AI

Section 2 directs a series of actions within 30 to 60 days to strengthen the nation's cyber defenses. Key directives include prioritizing the cyber defense of National Security Systems and Department of War information systems. CISA is directed to

release Binding Operational Directives to expedite cybersecurity for civilian federal systems, expand AI-enabled defensive tools, and facilitate access to cybersecurity services, including “covered frontier models,” for agencies, state, and local authorities,[10] and critical infrastructure operators such as rural hospitals, community banks, and local utilities. Additional measures include forming an AI cybersecurity clearinghouse in voluntary collaboration with industry to coordinate vulnerability scanning, validation, and remediation, identifying federal grant funding for advanced AI vulnerability detection, and expanding cybersecurity specialist hiring pathways.[11]

2. Secure Frontier Model Deployment

Section 3 is the Order's most consequential provision for AI developers. A consortium of agencies led by the NSA must within 60 days develop a “classified benchmarking process to assess the advanced cyber capabilities of AI models” and determine the threshold at which a model should be designated a “covered frontier model.”[12] Notably, the final determination will be made by the Director of the NSA, an intelligence agency, not a civilian regulatory body like the National Institute of Standards and Technology, in consultation with the National Cyber Director, the Assistant to the President for Science and Technology, and the Director of CISA.

The same officials must also design a voluntary framework through which AI developers would be able to (i) engage the federal government to determine whether model(s) under development meet the “covered frontier model” designation; (ii) provide the federal government with access to covered frontier models for up to 30 days before release to other trusted partners, “subject to appropriate confidentiality, cybersecurity, insider-risk, and intellectual property protection, use, and nondisclosure requirements”;[13] and (iii) collaborate with the government to select “trusted partners” that will have early access to covered frontier models to promote secure innovation and strengthen critical infrastructure cybersecurity.

Critically, Section 3(c) states: “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."[14] This disclaimer reinforces the administration's stated commitment to a voluntary, industry-collaborative approach rather than a prescriptive regulatory regime.

3. Enforcement against Criminal Use of AI

The Order directs the Attorney General to prioritize enforcement of existing federal criminal statutes, including 18 U.S.C. § 1028 (identification fraud), § 1030 (computer fraud and abuse), and § 1343 (wire fraud), against anyone who "utilizes AI to illegally access or damage a computer without authorization, or who utilizes AI while engaged in such illegal access to further any other crime."[15] The express reference to "employing AI agents to unlawfully access data or information that is subsequently used for a criminal or unlawful purpose"[16] is noteworthy. As autonomous AI agents become more prevalent in enterprise environments, the scope of potential liability under the Computer Fraud and Abuse Act for agent behavior without authorization or in excess of authorized access is an area of increasing focus, despite the potential complications created by the Supreme's Court narrow reading of that statute in *Van Buren*.[17]

Takeaways for AI Companies and Stakeholders

Several aspects of the Order warrant close attention from AI developers and companies operating in or adjacent to the frontier AI space:

- *Classified benchmarking and the NSA's gatekeeper role.* The Order introduces a new term of art: "covered frontier model," to be defined through a classified benchmarking process administered by the NSA. The classified nature of the criteria means developers may not know ex ante whether their models meet the threshold, and the criteria will not be subject to the public notice-and-comment dynamics that typically accompany federal standard-setting. For non-U.S. developers, submitting models to an American signals intelligence agency for

classified evaluation may raise data sovereignty and national security concerns in their home jurisdictions, potentially driving a wedge between U.S. and non-U.S. AI ecosystems.

- *Voluntary today, baseline tomorrow.* The Order explicitly disclaims any mandatory licensing or pre-clearance authority.[18] But voluntary frameworks that attract broad industry participation have a tendency to harden into de facto standards of care. Companies that sit out may face informal pressure or reputational risk, particularly as peers engage. California's recent AI procurement certification framework, though limited to state vendors, illustrates the dynamic: standards adopted for one purpose can quickly set broader market expectations.[19]

- *IP and competitive risk in the 30-day pre-release window.* The requirement that developers provide government access to covered frontier models up to 30 days before release to trusted partners raises significant intellectual property and competitive concerns. The Order references confidentiality, cybersecurity, insider-risk, and IP protections, but the details remain to be negotiated. Developers will want to scrutinize those terms carefully before opting in.

- *"Trusted partners" selection.* The Order contemplates that the government and developers will collaborate to select "trusted partners" for early access to covered frontier models. Who qualifies as a trusted partner, and what access they receive, could have significant competitive implications. The framework may effectively create a tiered system in which certain companies receive preferential early access to the most capable models.

- *Cybersecurity clearinghouse: benefits and risks.* The AI cybersecurity clearinghouse could offer valuable vulnerability intelligence to participants. However, participation in a government-coordinated vulnerability-sharing program raises considerations including discovery exposure if vulnerability data is later subpoenaed, and the interplay with existing vulnerability disclosure frameworks. While the Cybersecurity Information Sharing Act of 2015 may

provide antitrust and liability protections for qualifying cybersecurity information sharing, participants in the clearinghouse will want to confirm that the scope of information exchanged remains within the statute's safe harbor. Companies considering participation will want to weigh these factors against the operational benefits.

- *Criminal enforcement and AI agent exposure.* DOJ's prioritization of existing criminal statutes against AI-enabled unauthorized access has implications beyond deterring malicious actors. Companies deploying autonomous AI agents that interact with external systems or third-party data may wish to assess whether their agent architectures and access controls are designed to mitigate the risk that agent behavior could be characterized as exceeding authorized access under the Computer Fraud and Abuse Act.

- *Regulatory divergence across jurisdictions.* Unlike the December 2025 executive order, this Order does not address state AI regulation directly, but viewed alongside the March 2026 legislative recommendations, it further consolidates the federal government's posture as the primary regulator of frontier AI. For multinational companies, the Order's voluntary, cybersecurity-focused approach stands in notable contrast to the EU AI Act's mandatory risk-classification regime, adding compliance complexity for organizations operating across jurisdictions.[20]

Looking Forward

The most consequential details of this Order will emerge in the coming weeks as agencies implement the 30- and 60-day action items. The classified benchmarking criteria, the terms of the voluntary pre-release framework, and the operational rules governing the cybersecurity clearinghouse will determine whether this Order remains a collaborative exercise or begins to establish de facto compliance expectations for the frontier AI industry. Companies developing or deploying advanced AI models, operators of critical infrastructure, and investors in AI-driven businesses may wish to

monitor these developments closely, assess their models' potential exposure to the "covered frontier model" designation, and evaluate the costs and benefits of early engagement with the emerging frameworks.

---

1. Exec. Order, *Promoting Advanced Artificial Intelligence Innovation and Security* (June 2, 2026), https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/.
2. Exec. Order, *Removing Barriers to American Leadership in Artificial Intelligence* (January 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.
3. Exec. Order, *Advancing Artificial Intelligence Education for American Youth* (April 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/.
4. Exec. Order, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity* (June 6, 2025), https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694.
5. Exec. Order, *Promoting the Export of the American AI Technology Stack*, (July 23, 2025) https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/.
6. Ropes & Gray LLP, *AI and Tech Under the One Big Beautiful Bill Act: Key Restrictions, Risks and Opportunities* (July 23, 2025), https://today.westlaw.com/Document/I78a3623c67cf11f099aadf2a8d10cf74/View/FullText.html.
7. Exec. Order, *Ensuring a National Policy Framework for Artificial Intelligence* (Dec. 11, 2025), https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
8. The White House, *Legislative Recommendations: National Policy Framework for Artificial Intelligence* (Mar. 2026); *see also* Ropes & Gray LLP, *The White House Legislative Recommendations: National Policy Framework for Artificial Intelligence and Federal Preemption of State AI Laws* (Mar. 30, 2026), https://www.ropesgray.com/en/insights/alerts/2026/03/the-white-house-legislative-recommendations-national-policy-framework-for-artificial-intelligence-an.
9. Supra note 1, at § 1.
10. Supra note 1, at §§ 2(a)-(c).
11. Id. at § 2(d)-(f).
12. Id. at § 3(a).
13. Id. at § 3(b)(ii).
14. Id. at § 3(c).
15. Id. at § 4.
16. Id.
17. *Van Buren v. United States*, 593 US 374 (2021) (limiting the scope of the CFAA when applied to authorized users).
18. Id. at § 3(c).
19. Ropes & Gray LLP, *Newsom Signs Executive Order Establishing AI Vendor Certification and Procurement Framework* (Apr. 2026), https://www.ropesgray.com/en/insights/alerts/2026/04/newsom-signs-executive-order-establishing-ai-vendor-certification-and-procurement-framework.
20. *Supra* notes 7-8; *see also* Ropes & Gray LLP, *Trump Attempts to Preempt State AI Regulation Through Executive Order* (Dec. 12, 2025), https://www.ropesgray.com/en/insights/alerts/2025/12/trump-attempts-to-preempt-state-ai-regulation-through-executive-order.