Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 9, 2026

Controlling Advanced Artificial Intelligence: Executive Order 14409 Explained

On June 2, 2026, President Donald Trump signed Executive Order 14409 (E.O. 14409), *Promoting Advanced Artificial Intelligence Innovation and Security*. The E.O. directs agencies to harden federal government infrastructure against artificial intelligence (AI)-enabled risks and work with the private sector to strengthen AI security. It is the latest in a series of E.O.s addressing AI and cybersecurity. E.O. 14409 frames AI as both a strategic asset and an emerging attack vector. The order creates a policy for directing the federal government to work with the private sector to modernize federal and private information systems, protect American intellectual property from adversary exploitation, and accelerate AI-enabled defensive capabilities.

E.O. Summary

The E.O. has dual goals of accelerating AI innovation and improving security. It directs federal agencies to coordinate on assessing how advanced AI models might be used for both defensive and offensive cyber operations. The order calls for a classified benchmarking process to determine whether an AI system qualifies as a *covered frontier model* (to be defined within 60 days (August 1, 2026)) based on its cyber capabilities.

Companies developing advanced AI models are asked to participate in a voluntary review process that gives the government a window of 30 days to examine new systems before such models are released to "other trusted partners" (e.g., critical infrastructure companies). The order instructs specified agencies to create an *AI cybersecurity clearinghouse* to centralize information on AI-related vulnerabilities and threats, and to modernize government networks using advanced AI tools. It links this security posture to broader economic and strategic goals, emphasizing protection of U.S. intellectual property and maintaining American leadership in AI.

Tasks

The order directs various federal entities to complete certain tasks. The list below shows each task and, in parentheses, the relevant entity or entities (beginning with the lead agency) and due date:

- Prioritize cybersecurity of National Security Systems (Committee on National Security Systems). Due within 30 days (July 2, 2026).
- Prioritize cybersecurity of Department of Defense (DOD; currently using "Department of War" as a secondary designation under E.O. 14347 dated September 5, 2025) information systems. Due within 30 days (July 2, 2026).
- Issue Binding Operational Directives for civilian federal systems; expand AI-enabled defensive tools; extend cyber tools and services to states, local authorities, and critical infrastructure (Cybersecurity and Infrastructure Security Agency [CISA], Office of Management and Budget [OMB], the National Security Council [NSC], the Assistant to the President for National Security Affairs [APNSA], and the National Cyber Director [NCD]). Due within 30 days (July 2, 2026).
- Form an AI cybersecurity clearinghouse (Department of the Treasury [Treasury], NCD, the National Security Agency [NSA], and CISA). Due within 30 days (July 2, 2026).
- Identify federal grant funding for AI vulnerability detection research and development (OMB, CISA, and NCD). Due within 30 days (July 2, 2026).
- Develop a classified AI benchmarking process and establish a voluntary framework for covered frontier model pre-release access (NSA, NCD, Assistant to the President for Science and Technology [APST], CISA, and DOD). Due within 60 days (August 1, 2026).
- Develop a voluntary framework for AI companies to disclose their models (Treasury, NSA, CISA, National Institute of Standards and Technology [NIST], APST, and DOD). Due within 60 days (August 1, 2026).
- Expand U.S. Tech Force cybersecurity specialist hiring pathways (Office of Personnel Management [OPM]). Due within 60 days (August 1, 2026).
- Prioritize AI-facilitated cybercrime prosecutions under 18 U.S.C. §§1028, 1030, 1343 (Department of Justice [DOJ]). Ongoing and without stated due date.

Certain tasks in the E.O. are similar to those in E.O. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* signed on October 30, 2023, and rescinded by E.O. 14148, *Initial Rescissions of Harmful Executive Orders and Actions*, signed on January 20, 2025.

Cybersecurity Implications

The E.O.'s cybersecurity provisions aim to expand voluntary national security oversight of advanced AI models while stopping short of formal licensing or requiring preclearance. By creating a category of *covered frontier models,* the order treats advanced AI systems as potential *dual-use* tools over which early government oversight is desirable—similar to technologies with potentially dual civilian and military applications (e.g., sensors, lasers, avionics), as covered by the Wassenaar Arrangement. A voluntary notification and review window

aims to give agencies time to probe models for offensive and defensive cyber applications before public release. Such a process may increase the potential for earlier detection of vulnerabilities or potential abuse pathways.

At the same time, the voluntary structure in this E.O. potentially creates coverage gaps if major developers decline to participate, criteria for covered models are narrowly tailored, or the length of review is insufficient to identify potential risks. The order's plan for an AI-focused cybersecurity clearinghouse and expanded information sharing could strengthen defenses for critical infrastructure operators if implemented with timely, actionable threat intelligence. The concentration of possibly sensitive model details and cyber-threat data in federal systems also creates a potential risk for targeting by malicious actors.

For companies that choose to participate, the framework may provide closer security collaboration with defense and civilian agencies, but also potential exposure to more probing questions about model architecture, training data, and red-teaming results.

Implications for Broader AI Policy

A central tension in U.S. policy debates about AI technologies has been balancing support for AI innovation and competitiveness with efforts to minimize safety and security risks. E.O. 14409 broadly appears to continue the federal government's approach on AI governance and regulation, which has focused largely on voluntary benchmarks and evaluations of AI systems, public-private partnerships for AI innovation, and leveraging of federal agencies' existing authorities. The E.O. also focuses primarily on implications of AI technologies in the cybersecurity and critical infrastructure contexts, continuing an apparent shift in focus from AI safety (e.g., encoding alignment with human values) under the rescinded E.O. 14110 to AI security concerns (e.g., protecting AI from external threats such as cyberattacks).

E.O. 14409 directs Treasury, with DOD and DHS, to carry out activities to secure frontier model deployment, in consultation with NIST, among other agencies. Previous agreements between the NIST and AI companies Anthropic and OpenAI established a framework for NIST to "receive access to major new models from each company prior to and following their public release." Such agreements neither provided for public transparency on AI testing and evaluation nor included all frontier AI companies. Proposed legislation would mandate pre-deployment evaluation of certain AI models (e.g., the Artificial Intelligence Civil Rights Act of 2025, H.R. 6356). A draft bill would outline transparency and assessment frameworks, and security testing of frontier AI models (e.g., the discussion draft of the Great American Artificial Intelligence Act of 2026).

National Security Presidential Memorandum-11

On June 5, 2026, President Trump issued National Security Presidential Memorandum-11 (NSPM-11), a related document that provides guidance for "[accelerating] the development and use of AI for national security applications." NSPM-11 directs the national security enterprise to work with industry to "make the most advanced frontier models broadly available to national security professionals.... " The directive additionally notes that the national security enterprise is to ensure that any adopted AI systems "are designed to be reliable, robust, steerable, and controllable, and that they operate, in accordance with applicable laws, government policies, and guidance." In support of the objectives of E.O. 14409, NSPM-11 also directs the Secretary of Defense, the Secretary of Energy, the Director of National Intelligence, and the Director of the NSA, through the AI Security Center, in consultation with the APST, to work with industry to enhance the security of data centers and advanced AI technologies. This could include information sharing; joint testing, research, and development; and the provision of technical support. Congress may conduct oversight of these activities and, if necessary, "establish plans to mitigate potential concerns" in consultation with industry, as recommended by the March 2026 National Policy Framework for AI.

Considerations for Congress

Congress might consider the extent to which certain implementation details of E.O. 14409 are not specified by the order itself. The order does not define *covered frontier model*. The order relies on existing appropriations, leaving it unclear as to how new requirements, such as the AI cybersecurity clearinghouse (for which Treasury did not specifically request FY2027 funding), and expanded cybersecurity tools and services for states and local authorities may be funded. Left unclear are the scope of resources and the appropriate roles for organizations to carry out certain technical activities, such as developing an AI benchmarking process.

Congress might consider whether to maintain the overarching approach of voluntary industry engagement in AI or whether safety and security concerns of AI models warrant the establishment of federal requirements for testing and evaluation of certain AI models prior to release.

Congress may choose to consider the E.O.'s proposed assessment of AI models as a tool to address national security concerns, especially in contrast to stronger government direction or regulation. It may also choose to consider the Administration's other approaches, such as requiring Anthropic to suspend access to a frontier AI model showing advanced cyber capabilities, in the context of the E.O.'s broader policy and its effects on industry compliance and future policymaking.

Chris Jaikaran, Specialist in Cybersecurity Policy
Laurie Harris, Analyst in Science and Technology Policy
Kelley M. Sayler, Specialist in Advanced Technology and Global Security

IF13268

Disclaimer