POLSINELLI

Publications

July 23, 2026 • Updates

Technological Shifts Compel New Executive Orders for AI and Quantum Computing

Key Takeaways

- New capabilities from existing technologies are outpacing data governance considerations and guardrails necessary for appropriate accountability.
- Acknowledging the AI shift in cyber risk, the U.S. and its allies released a statement saying cybersecurity is a core business strategy, with a focus on leaders getting the basics right.
- "Reasonable security" in the Age of AI requires reconsidering the speed, scale and sophistication of expanding risks, as shown by recent unprecedented cyber incidents.
- An AI risk register, along with existing cybersecurity practices such as an incident response plan, are must-haves for companies developing, deploying or using AI.

"We must act now." That was the clarion call last week by thousands of economists and researchers that signed a statement warning that AI systems could reshape the economy at unprecedented speed and on a vastly shorter timeline. "We must act swiftly to remain ahead." That was the call-to-action last month as a follow-up to guidance issued in May.

These statements arrive on the heels of unprecedented events in June and July, when frontier models publicized the cybersecurity capabilities of new models, pre-released them to a select few and were forced to withdraw them for national security reasons based on an Executive Order signaling federal priorities and foreshadowing potential new legal duties.

For an administration that had previously taken a hands-off approach to regulating AI, its current approach has been a sudden shift. Given the way AI has accelerated the speed, scale and sophistication of cyber threats, we explain below how recent federal actions on AI and quantum computing and AI-driven cyber incidents are reshaping what "reasonable security" means.

Executive Orders Signal a Secure Deployment Framework for AI and Quantum Computing

Related People

- Romaine C. Marshall
- Matt A. Todd
- Bryce H. Bailey
- Ashleigh Bickford

Related Capabilities

- Artificial Intelligence & Machine Learning
- Privacy & Cybersecurity
- Technology
- Executive Orders

On June 2, the White House released an Executive Order titled *Promoting Advanced Artificial Intelligence Innovation and Security*. The most notable section of the order is the requirement by frontier models to provide the federal government with access "for a period of up to 30 days before they plan to release such models to other trusted partners."

Last month's AI order, under the subheading "Secure Frontier Model Deployment," also outlined the establishment of a classified benchmarking and voluntary framework process for determining "select trusted partners" that will have early access to covered frontier models. The order expressly points out that this process is not a permitting requirement.

A few days after the order, the White House released a fact sheet titled *AI in the National Security Enterprise*, aimed at accelerating AI adoption for national security. As an extension of the order and fact sheet, the Gold Eagle Initiative was announced last Tuesday to leverage frontier AI for public and private sector collaboration of actionable threat and remediation information.

Also in June, two executive orders relating to quantum computing were released, each signaling an overlap with national security concerns like those with AI and cybersecurity:

- *Ushering in the Next Frontier of Quantum Innovation* frames quantum science and technology as a driver of American innovation and national security and directs the federal government to update the "National Quantum Strategy," accelerate commercialization and deployment and support quantum computing, supply chains and workforce development.
- *Securing the Nation Against Advanced Cryptographic Attacks* addresses the other side of the same technological shift. It recognizes that large-scale quantum computers could threaten widely used cryptographic systems and directs a transition of federal information systems toward NIST-approved post-quantum cryptography, including specific timelines. It also calls for a cryptographic bill of materials and procurement-related changes that would push quantum-resistant security expectations beyond the federal government.

Both orders reflect a familiar framing: quantum is a powerful tool and a major area for commercial growth, and the United States should seek to develop it before other world powers. Just as AI systems become more autonomous and integrated into critical workflows, the security supporting quantum computing systems also becomes more consequential.[1]

In the AI and quantum computing contexts, policymakers are not rejecting the underlying technology; they are recognizing that the same tools that create commercial and strategic advantage can also compress risk timelines, lower barriers for adversaries and require organizations to revisit assumptions that previously seemed sufficient.

AI-Driven Incidents Show How Quickly Cyber Risk is Changing

Unprecedented cybersecurity incidents have also happened this month. Three weeks ago, an agentic AI threat actor exploited several software vulnerabilities, made decisions on how to string them together and executed a ransomware attack and demand note. The identity of the victim company has not been disclosed, but the attack details have.

In a separate incident a day later, a global cyber-readiness and incident response firm released a report detailing how a lone threat actor used AI to extort a well-known global enterprise through agentic AI workflows combining multiple attack techniques. The result, and how "[a]n attack that would have taken weeks to execute all happened under 72

hours," are outlined in the report.

These and other recent incidents highlight the order of magnitude at which frontier models' cybersecurity capabilities are not only expanding the risk surface by enabling autonomous agents to perform thousands of logged-actions, but also compressing timelines for AI developers, deployers and users to refine data governance programs.

Cybersecurity Basics Remain the Foundation for AI Governance

This is why the United States and its allies are emphasizing getting the basics right as a core business strategy. Unlike their initial guidance issued in May, which included 122 best practices and 18 prerequisites, the recent follow-up statement focuses on five practical action areas for leaders to address. These include:

1. Reducing the attack surface;[2]
2. Accelerating patching processes;
3. Addressing legacy systems;
4. Reviewing and strengthening identity and access control; and
5. Preparing for incidents before they happen.

Asset inventorying has been described by one expert as the first meaningful AI governance intervention because it could be the first time members of an organization have to sit down and agree, out loud, on what AI is really running and why.[3] Asset inventorying has long been a cybersecurity requirement, including by the National Institute of Standards and Technology.[4]

NIST's AI RMF Playbook is instructive, describing an AI inventory as an organized database of artifacts relating to an AI system or model "that enables a holistic view of organizational AI assets."[5] The Playbook points out that an individual or team should be responsible for maintaining the inventory.

To this end, Australia — one of the United States' main allies for AI and cybersecurity — has created an AI register template that can be downloaded in a document or spreadsheet format. The register template provides a format for users to list key characteristics, use cases and accountable people, and it encourages organizations to have informed conversations about AI use.

The structure mirrors the cybersecurity risk register, which is created and used to identify, evaluate and track potential threats, vulns and their business impacts. As an addition to an organization's incident response plans, an AI risk register is just one other way teams can focus on fast containment and recovery.

For more information on AI-driven cybersecurity risks and evolving legal expectations, contact the authors or your regular Polsinelli attorney.

[1] For a more in-depth analysis of risk management and governance requirements for quantum computing see Guest Post – Looking Ahead: 'The Best Time to Prep for Quantum Was 20 Years Ago …' in Quantum Insider by Matt Todd and Bryce Bailey (dated June 23, 2026).

[2] Defined variously as "multiple entry points" including "every device, link, or software that connects to a network" that can be exploited. *See, e.g.,* https://www.sentinelone.com/cybersecurity-101/cybersecurity/attack-surface-reduction/ (describing Attack Surface Reduction Guide: Steps & Benefits).

[3] https://governance.aicareer.pro/blog/building-ai-inventory-first-governance-intervention

[4] *See, e.g.,* https://www.polsinelli.com/bruce-a-radke/publications/cybersecurity-compliance-in-2025-know-your-technology-assets (describing various government agencies emphases on asset inventorying).

[5] https://airc.nist.gov/airmf-resources/playbook/ (at 12-13).