JENNER & BLOCK

Two New Executive Orders on Quantum Computing: Key Takeaways for Companies Operating in Quantum Information Science and Critical Infrastructure

Client Alerts

June 26, 2026
By: Aaron R. Cooper, Philip J. Chertoff, Steven J. Arango, Katie Garcia

On June 22, 2026, President Trump signed two Executive Orders establishing an updated comprehensive federal framework for quantum information science and technology. The first order focuses on security—requiring federal agencies and government contractors to upgrade their encryption systems to withstand attacks from future quantum computers, before those computers arrive. The second focuses on innovation—accelerating research, commercialization, and workforce development in quantum computing and related technologies.

Together, the two orders reshape the federal government's relationship with quantum technology on two fronts simultaneously: racing to deploy it while hardening defenses against it. For quantum technology companies, the orders represent significant near-term opportunity, with a major new government quantum computing initiative, advance-purchase commitments for commercial quantum systems, and a sensor-fielding mandate together signaling that the federal government intends to start making significant procurements from the domestic quantum industry. However, export restrictions on specialized quantum components are also likely to tighten, and companies conducting quantum R&D should prepare for increased engagement from federal counterintelligence. And while the transition to post-quantum cryptography (PQC) has been pushed on contractors for a few years now, government contractors now face a hard December 31, 2030 deadline to upgrade to quantum-resistant encryption, and critical infrastructure companies should expect mounting regulatory pressure even without a direct mandate.

Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks

The first executive order, on "Securing the Nation Against Advanced Cryptographic Attacks," addresses the "harvest now, decrypt later" threat: the concern that foreign adversaries are already collecting encrypted US data today, intending to decrypt it once they have a sufficiently powerful quantum computer.

The National Institute of Standards and Technology (NIST), within the Department of Commerce, has spent years developing new encryption standards specifically designed to resist quantum attacks and completed the first iteration of those standards in 2024. The June 22 orders now direct the government to actually use those standards.

The order accelerates the government's encryption upgrade timeline from a prior target of around 2035 to December 31, 2031, reflecting growing concern that quantum computing is advancing faster than earlier estimates suggested. Its key provisions include:

- **Federal agency upgrade deadlines.** Agencies must upgrade their most critical systems to quantum-resistant encryption by the end of 2030 (for data transmission) and 2031 (for digital signatures), though it appears the government will first run a pilot on its own systems, to be completed by the end of 2027.

- **Critical infrastructure.** Sector regulators must help critical infrastructure operators—in energy, financial services, healthcare, transportation, and communications—develop their own upgrade plans. Within nine months, federal agencies must release guidance on a standardized inventory framework to help organizations identify where vulnerable encryption exists in their systems.

- **Government contractor requirements.** Proposed rules will require government contractors to complete encryption upgrades by December 31, 2030, and to maintain formal programs for disclosing encryption vulnerabilities. Both rules will go through public comment before taking effect.

- **International PQC coordination.** The order directs the Secretary of State to engage foreign governments and industry groups to encourage adoption of NIST-standardized PQC algorithms. For multinational companies, this signals that US PQC standards may increasingly become the basis for allied nations' requirements, which could help simplify PQC compliance across jurisdictions over time.

Executive Order 14413: Ushering in the Next Frontier of Quantum Innovation

The second executive order, on "Ushering in the Next Frontier of Quantum Innovation," directs a government-wide push to cement US leadership in quantum technology across research, commercial deployment, supply chains, and workforce.

This executive order builds on a foundation laid by the first Trump administration. In 2018, President Trump signed the National Quantum Initiative Act, which for the first time organized federal quantum research across agencies and created the government coordinating bodies that still drive quantum policy today. That law's core research funding authorities quietly lapsed in 2023 despite bipartisan support for renewal, a gap this order may help push Congress to close.

Its key provisions include:

- **An updated national quantum strategy.** The Assistant to the President for Science and Technology must update the government's national quantum strategy within six months, with each relevant agency submitting an alignment plan within 30 days of its release.

- **NQIAC reconstitution.** The order directs the reconstitution of the National Quantum Initiative Advisory Committee (NQIAC) within 210 days, tasking it with developing recommendations to stimulate quantum-enabling technology development in the United States.

- **A major new quantum computing initiative.** The order launches an effort to build at least one large-scale quantum computer at a Department of Energy facility, available to the scientific community for breakthroughs beyond the reach of classical computers. The Energy and Commerce Departments must develop partnership and procurement models with private companies within six months.

- **Fielding quantum sensors.** The Department of War must identify at least three next-generation quantum sensor projects to deploy by September 30, 2028, that address the vulnerability of GPS systems to jamming and spoofing by providing precise location and timing data that does not rely on GPS signals. Other agencies must each develop five-year sensing and networking roadmaps.

- **Counterintelligence protections for quantum R&D.** The order directs the FBI to propose an expansion of the Quantum Information Science and Technology Counterintelligence Protection Team (QCPT), with a mandate covering cybersecurity threats, coordinated public outreach, and threat information sharing with federal agencies, industry, and academia. All relevant agencies are directed to coordinate with the QCPT on quantum-specific security guidance.

- **International framework alignment (Pax Silica).** The order specifically directs the Secretary of State to align existing bilateral and multilateral engagements, including "Pax Silica"—a US-led strategic international initiative aimed at securing supply chains for semiconductors, artificial intelligence computing power, critical minerals, and digital infrastructure among allied nations—with the order's quantum priorities.

What Comes Next

The orders set a fast-moving implementation schedule, with the first round of agency actions due in 30 to 90 days. That said, much of what the orders direct is planning—strategies, roadmaps, and proposed rules—rather than funded programs. The real test will be whether agencies follow through quickly and effectively. The contractor encryption rules will go through public notice and comment, giving industry a formal opportunity to weigh in, but companies that wait for final rules before acting will have little runway to meet the 2030 deadline. Whether Congress uses this moment to finally reauthorize the lapsed National Quantum Initiative research funding will be an important indicator of whether the executive push is matched by sustainable legislative backing.

What These Executive Orders Mean for Businesses

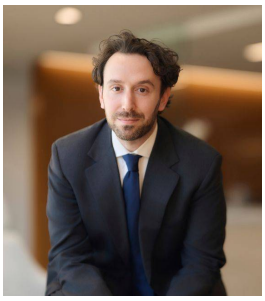
The two orders raise a range of immediate and near-term considerations across several business areas:

- **Government contractors face a hard encryption deadline.** Forthcoming rules will require companies that contract with the federal government to upgrade to quantum-resistant encryption by December 31, 2030, and to maintain formal vulnerability disclosure programs. Contractors should begin inventorying their encryption dependencies now and plan to engage during the public comment period.
- **Critical infrastructure companies will face mounting pressure to act, even without a mandate.** While the order does not require the broader private sector to upgrade its encryption, companies in regulated industries should expect sector-specific guidance from their regulators and treat the forthcoming inventory framework as a practical planning tool to start using now.
- **Quantum technology companies have significant new government contracting opportunities.** The new quantum computing initiative, advance-purchase commitments for commercial quantum systems, and the Department of War's sensor-fielding mandate represent concrete near-term opportunities. These orders signal that the federal government intends to be a significant early customer for the domestic quantum industry.
- **NQIAC engagement.** The NQIAC will be an important venue for private sector input into federal quantum policy. Companies in the quantum ecosystem should monitor its membership and emerging recommendations.
- **Prepare for QCPT engagement.** Companies conducting quantum research and development—whether as contractors, grantees, or independent technology developers—should expect increased engagement from the QCPT and should review their internal research security programs accordingly.
- **Export restrictions on quantum components are likely to tighten.** Companies that manufacture or sell specialized quantum components—precision lasers, cryogenic equipment, photonic devices, and advanced materials—should review their export classifications and foreign customer relationships in anticipation of stricter controls.
- **The "harvest now, decrypt later" threat calls for action today, not just compliance planning**. For companies that hold sensitive long-lived data—trade secrets, health records, financial information, or confidential communications—upgrading encryption is a present risk management decision. The new quantum-resistant standards published in 2024 are available to use now, and companies should evaluate where to prioritize adoption based on the sensitivity and longevity of the data they hold.

Jenner & Block's Critical and Emerging Technologies Practice will continue to track key developments as the Administration's quantum policy takes shape, including regulatory processes, comment periods, and guidance.

Related Attorneys

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333



Philip J. Chertoff
Associate
pchertoff@jenner.com
+1 202 637 6346

Steven J. Arango
Associate
sarango@jenner.com
+1 202 637 6348

Katie Garcia
Associate
katharine.garcia@jenner.com
+1 212 407 1793

Related Capabilities

Communications, Internet, and Technology

Critical and Emerging Technologies

National Security and Crisis

Stay Informed →