

Quantum Computing EOs Create Immediate Compliance Deadlines, New Federal Partnership Opportunities

July 29, 2026

On June 22, 2026, President Donald Trump signed two executive orders (EOs) that make quantum computing a concrete compliance and business reality for critical infrastructure operators, federal agencies, federal contractors and quantum technology companies. The first order focuses on the threats posed by a quantum future and sets hard deadlines for migrating federal systems and contractor operations to post-quantum cryptography (PQC), with initial agency steps due by late July 2026. The second order launches a coordinated federal push to develop the most advanced quantum technologies in the world, creating significant partnership opportunities for the private sector.

This alert summarizes the key provisions, deadlines and action items arising from these orders. In light of the growing importance of quantum computing to organizations' cybersecurity, privacy and data regulatory concerns, Cooley's cyber/data/privacy practice will be publishing an ongoing series of alerts to keep you informed about what's to come.

Overview: Two orders, two missions

Executive Order 14412, titled "Securing the Nation Against Advanced Cryptographic Attacks" (Defensive Order), focuses on US defense and preparedness against the threats posed by quantum computing. It responds to a threat that the Trump administration understands to already be materializing: Adversaries are collecting sensitive encrypted data today with the intention of decrypting it later, once large-scale quantum computers are operational. This "harvest now, decrypt later" strategy means the window for action is defined not by when quantum computers arrive, but by when organizations complete their migrations to quantum-resilient safeguards. Experts have been aware of this attack strategy for some time, since the algorithms underlying the widespread distribution of public key cryptography (such as RSA and elliptic curve) produce output using mathematical computations that make that output feasible to decryption in a reasonable period of time with quantum technology. To counter this, the Defensive Order mandates a government-wide transition to post-quantum cryptography (PQC), meaning encryption algorithms specifically designed to withstand attacks by both quantum computers and the classical computers in use today. Federal contractors and critical infrastructure operators, as defined under the USA PATRIOT Act, are squarely in scope.

Executive Order 14413, titled "Ushering In the Next Frontier of Quantum Innovation" (Innovation Order), focuses on US innovation and achieving primacy in the quantum technology space. It directs a whole-of-government effort to:

- Develop a quantum computer capable of scientific discoveries beyond anything currently possible on a classical computer.
- Accelerate quantum sensing and networking capabilities.
- Strengthen domestic supply chains for quantum hardware and components.
- Grow a trained US quantum workforce.
- Entrench US global leadership in quantum technology.

The Innovation Order also serves as a call to the private sector, signaling the federal government actively seeks industry partners.

Immediate deadlines for federal agencies

For federal agencies, the deadlines in the Defensive Order begin almost immediately. Within 30 days of its

release, or by July 22, 2026, every agency head must designate a PQC migration lead, meaning an employee who will be responsible for overseeing the agency's cryptographic inventory, developing a prioritized migration plan and coordinating across the government, and will report to the agency's chief information officer. Within 90 days, or by September 20, 2026, the Office of Management and Budget must issue guidance requiring agencies to review their inventories of their high- value assets and high-impact systems and submit plans to transition them, with firm completion targets:

- All high-value assets and high-impact systems must use PQC for key establishment purposes (i.e., the creation of a shared encryption key for communication between different systems) by **December 31, 2030**.
- All high-value assets and high-impact systems must use PQC for digital signature purposes (i.e., for verifying the authenticity and integrity of data) by **December 31, 2031**.

A NIST-led pilot migration on a subset of its own systems must begin within 180 days and be complete by December 31, 2027, providing a model for agencies to follow.

Implications for federal contractors

Federal contractors are not exempt. The Defensive Order requires the Federal Acquisition Regulatory Council, within 180 days, to publish a proposed rule requiring federal contractors to comply with post-quantum cryptography standards by December 31, 2030. A separate proposed rule, due within 270 days, would require federal contractors to maintain vulnerability disclosure programs and incorporate reports of cryptographic vulnerabilities into such programs, including the use of encryption methods that do not meet federal standards.

These proposed rules are not yet final but will be soon. Federal contractors that begin cryptographic inventories now – cataloging what systems they run, what encryption they rely on and where their gaps are – will be far better positioned than those who wait for the rules to be proposed and finalized.

Implications for critical infrastructure operators

The Defensive Order extends to operators of critical infrastructure across sectors including energy, water, transportation, healthcare and financial services. The federal agencies that oversee each of these sectors are required to assist operators in developing PQC migration plans. If you operate critical infrastructure, expect outreach from your sector's federal oversight agency. Engaging proactively now will put you ahead of that process.

Implications for quantum technology companies

For companies in the quantum technology space, the Innovation Order signals substantial federal investment and partnership opportunities. The Innovation Order directs agencies to explore advance market commitments and use prize challenges to encourage private-sector participation in building next-generation quantum computers, quantum sensors and quantum networks, as well as in developing domestic supply chains for quantum-enabling components. Companies should monitor the National Quantum Strategy update due within 180 days of the Innovation Order, which will define the specific areas of federal focus and map where the partnership opportunities will be.

The Innovation Order also carries a cautionary note for quantum technology companies. The federal government intends to work with international allies to tighten restrictions on the export of quantum-enabling technologies to countries of concern and harmonize research security policies across allied nations to prevent adversarial actors from gaining access to critical quantum technology through research partnerships or other channels. For quantum technology companies, this signals that export control compliance in this space is likely to become more demanding, and that existing research collaborations with foreign universities, institutions or individuals may warrant a closer look.

Looking ahead

These EOs mark a turning point: Quantum computing is no longer a future concern but a present compliance

and strategic priority. Whether your organization faces new migration obligations or stands to benefit from federal quantum investment, prompt attention to these orders is essential. Watch for the next installment in our quantum computing series, which will break down key quantum computing concepts, contextualize these orders and help enterprises and their leaders prepare for what comes next. If you have questions about either of these orders or any other quantum computing issues, please contact the Cooley cyber/data/privacy practice.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140
Emma Plankey Boston	eplankey@cooley.com +1 617 937 1349
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.