LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Trump EOs Pair Quantum Push With Cyber Defense Overhaul

By **Olivia Radin, Ana Daily and Ryan Jones** (July 2, 2026, 3:30 PM EDT)


Olivia Radin


Ana Daily


Ryan Jones

On June 22, President Donald Trump signed two companion executive orders addressing quantum technology.

Executive Order No. 14409 directs a governmentwide shift to new encryption standards designed to withstand cryptographic attacks by quantum computers.[1] Executive Order No. 14411 launches a coordinated federal effort to develop and commercialize quantum computing, sensing and networking.[2]

Together, the two orders form a unified strategy: One accelerates the buildout of quantum capability, while the other defends against the security risks that same technology creates.

The cryptography order responds to what national security officials call the harvest now, decrypt later threat — the risk that adversaries are collecting encrypted U.S. data today with plans to unlock it once quantum computers become powerful enough to break current encryption.[3]

The order warns that large-scale quantum computers "in the hands of adversaries ... will pose a significant threat to widely used cryptographic security systems," and directs the government to adopt new, quantum-resistant encryption standards developed by the U.S. Department of Commerce's National Institute of Standards and Technology, the agency responsible for developing federal technology standards and guidance.

The order assigns the Office of Management and Budget and the Office of the National Cyber Director significant roles in coordinating the government's encryption upgrade. The Department of Commerce, through NIST and in coordination with the National Security Agency and the Cybersecurity and Infrastructure Security Agency, will provide agencies with technical guidance.

The order directs the OMB to require that agencies identify their most critical systems and migrate them to quantum-resistant encryption by Dec. 31, 2030 (for key establishment), and Dec. 31, 2031 (for digital signatures).

The order also directs changes to federal contracting rules. The order directs the Federal Acquisition Regulatory Council to propose a rule requiring covered contractors to comply with NIST's quantum-

resistant encryption standards by Dec. 31, 2030.

A second proposed rule would require contractors to maintain vulnerability disclosure policies, including the reporting of encryption weaknesses such as the use of outdated algorithms.

These requirements may be especially relevant for artificial intelligence companies that contract with the federal government or provide systems, software or services used in federal environments.

Model weights and training data are highly valuable, and AI systems may rely on the encryption that threat actors try to defeat using quantum technology. For AI developers, upgrading to quantum-resistant encryption is not just a compliance exercise but could also protect core intellectual property.

The innovation order takes the offensive side of the strategy. It declares the administration's policy to maintain "a strategic technical advantage" in quantum technology and to lead "a robust and trusted quantum ecosystem" spanning research, manufacturing, commercialization and practical applications.

The order directs the assistant to the president for science and technology to update the national quantum strategy within 180 days, with an emphasis on commercialization, the quantum-components supply chain and partnerships with U.S. industry.

The order's centerpiece is the Quantum Computer for Application Development and Discovery Science, or QC-ADDS, Effort, a national initiative to build a quantum computer powerful enough to "initiate the era of quantum-enabled scientific discovery." The order provides that at least one such machine will be installed at a U.S. Department of Energy facility and made available to the scientific community.

To attract commercial partners, the order directs the secretary of commerce to develop a plan, "potentially including advance market commitments," to encourage contributions from private quantum-computing companies.

The order also directs five-year plans for deploying quantum sensors and networks, measures to strengthen domestic supply chains and manufacturing, a governmentwide quantum workforce strategy, an expansion of a counterintelligence team focused on protecting the quantum ecosystem, and coordinated engagement with international partners on market access, export controls and research security.

The QC-ADDS Effort's goal of standing up a science-enabling computer parallels the administration's broader federal efforts to leverage AI for scientific discovery.

Read together, the two initiatives suggest a converging federal strategy in which AI and quantum systems are positioned as complementary engines of scientific and economic advantage.

Potential Downstream Implications

Described below is a preliminary overview of the potential downstream legal and regulatory issues that may arise as the executive orders are implemented, and areas where agencies, Congress, regulators or private litigants may seek to build on the orders' policy direction over time.

Export Controls and Foreign Investment

The innovation order's references to export controls, research security and coordinated engagement with international partners signal that quantum technology may face heightened scrutiny under the Export Administration Regulations.

Companies developing quantum hardware, software or components should monitor whether the order leads to new or expanded export licensing.

The order's emphasis on counterintelligence protection and guarding against adversarial threats to the quantum ecosystem also suggests that foreign investment in U.S. quantum companies may face closer review by the Committee on Foreign Investment in the United States, potentially as a critical technology where the relevant technology is export-controlled and the transaction otherwise meets the mandatory-filing criteria.

Government Contractor Compliance and Enforcement Risk

The FAR amendments required by the cryptography order are expected to create new compliance obligations and potentially new enforcement exposure.

Contractors who misrepresent their cryptographic compliance status, fail to maintain the required vulnerability disclosure policies or continue using outdated encryption algorithms while certifying compliance could face False Claims Act exposure, depending on the final rule and certification structure.

Given the hard Dec. 31, 2030, deadline, contractors should begin assessing their current cryptographic posture and planning their migration now.

Congressional Action and Funding

The orders build on the National Quantum Initiative Act, but their implementation, particularly large-scale initiatives like the QC-ADDS, will depend on future congressional appropriations and any reauthorization or expansion of the act's framework.

The reauthorization debate will provide signals about long-term federal investment.

State Privacy Law Implications

As NIST's post-quantum cryptographic standards become the federal baseline, they may also reshape what constitutes reasonable security under state privacy, cybersecurity and data breach laws.

Regulators and private plaintiffs could increasingly look to NIST's post-quantum standards as a benchmark for "reasonable security," particularly for long-lived sensitive data. Over time, continued reliance on quantum-vulnerable encryption — after federal standards and migration timelines are established — may face greater scrutiny.

Standard Essential Patents

To the extent NIST's post-quantum cryptographic standards require implementation of patented technology, mandatory adoption through federal procurement rules could raise licensing and cost issues for contractors and technology providers.

Any disputes would likely turn on whether relevant patents are actually essential to the standards, whether licensing commitments apply, and whether terms are reasonable and nondiscriminatory.

These issues could become more significant as agencies and covered contractors move toward the 2030 migration deadline, particularly for smaller vendors that must update products or services to remain eligible for federal work.

Conclusion

These two executive orders represent a significant federal commitment to both advancing and defending against quantum technology. For companies in the quantum, AI and technology sectors — and for government contractors across industries — the orders establish concrete federal migration deadlines and point toward future contractor compliance obligations.

The 2030 and 2031 cryptographic migration deadlines are not distant; organizations may benefit from starting to assess their systems, supply chains and contracting relationships now. At the same time, the innovation order creates potential opportunities for companies positioned to contribute to the QC-ADDS Effort or grow with the federal investment in quantum infrastructure.

Olivia Radin is a partner, Ana B. Daily is a senior associate and Ryan Jones is an associate at King & Spalding LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Exec. Order, Securing the Nation Against Advanced Cryptographic Attacks (June 22, 2026), https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/.

[2] Exec. Order, Ushering in the Next Frontier of Quantum Innovation (June 22, 2026), https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/.

[3] What Is Post-Quantum Cryptography?, Nat'l Inst. of Standards & Tech., https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography (last visited June 25, 2026).