



The clock has started

What the White House quantum executive orders mean for your organization

KPMG QUANTUM SECURITY PRACTICE



"Quantum technologies, like a quantum computer or a quantum sensor, will provide transformational capabilities in manufacturing, drug discovery, energy, agriculture, and more. These breakthroughs will drive American innovation, power economic growth, generate high-paying jobs in existing and entirely new industries, and bolster national security."—The White House, Fact Sheet on EO 14413, June 22, 2026¹

On June 22, 2026, President Trump signed two executive orders that together represent the most consequential quantum security policy action in US history.^{2,3} The first—**"Ushering in the Next Frontier of Quantum Innovation" (EO 14413)**⁴—launches a national program to build and deploy an advanced quantum computer for scientific research by 2028. The second—**"Securing the Nation Against Advanced Cryptographic Attacks" (EO 14412)**⁵—sets binding deadlines for federal agencies and covered contractors to migrate to post-quantum cryptography (PQC), with key establishment systems required to meet quantum-safe standards by **December 31, 2030** and digital signatures by **December 31, 2031**.^{6,7}

For every organization that touches federal systems, operates critical infrastructure, or holds contracts with the US government, these orders are not background policy—they are a compliance starting gun. The organizations that act now will migrate on their own terms. The ones that wait will find themselves managing a crisis at the worst possible moment.

What the orders require

Order 1: "Ushering in the Next Frontier of Quantum Innovation" (EO 14413)

This order establishes the **Quantum Computer for Application Development and Discovery Science (QC-ADDS) Effort**—a whole-of-government program to deliver at least one advanced quantum computer to a Department of Energy facility, with a target date of 2028.⁸ The Department of Energy and Department of War⁹ are tasked with building and hosting the system.^{10,11} The Secretary of Commerce is directed to develop a plan—

¹ "Fact Sheet: President Donald J. Trump Ushers in the Next Frontier of Quantum Innovation," The White House, June 22, 2026

² Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation," 91 Fed. Reg. 38487, June 25, 2026

³ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

⁴ Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation," 91 Fed. Reg. 38487, June 25, 2026

⁵ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

⁶ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

⁷ "Fact Sheet: President Donald J. Trump Secures the Nation Against Advanced Cryptographic Attacks," The White House, June 22, 2026

⁸ Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation," 91 Fed. Reg. 38487, June 25, 2026

⁹ Executive Order 14347, "Restoring the United States Department of War," 91 Fed. Reg. 43893, September 5, 2025

¹⁰ Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation," 91 Fed. Reg. 38487, June 25, 2026

¹¹ "Energy Department Announces Initiative to Create and Deploy the World's First Scientifically Relevant, Fault-Tolerant Quantum Computers," U.S. Department of Energy, Office of Science, June 23, 2026

potentially including advance market commitments—to encourage contributions to the QC-ADDs Effort from commercial quantum computing companies.¹²

Beyond the hardware push, the order directs the Departments of Commerce, War, and Energy, and National Aeronautics and Space Administration to each draft five-year plans for quantum sensing and networking. The order notably expands the Quantum Counterintelligence Protection Team, tasking the intelligence apparatus to study adversarial threats to the domestic quantum ecosystem—including foreign acquisition of US research and intellectual property (IP). The Secretary of War is directed to identify at least three next-generation quantum sensor projects to field by September 30, 2028.^{13,14}

Order 2: “Securing the Nation Against Advanced Cryptographic Attacks” (EO 14412)

The second order contains immediate compliance implications for the private sector. It tasks the Office of Management and Budget (OMB), National Cyber Director, Department of Commerce, National Security Agency, and Department of Homeland Security with overhauling federal cryptography to a quantum-resilient standard—and extends that mandate to covered contractors.^{15,16} Crucially, the order accelerates the existing 2035 federal migration deadline: Civilian networks must now adopt quantum-resistant encryption on the new 2030–2031 schedule.^{17,18} Agencies that miss the new deadline must report to OMB explaining why.¹⁹

Figure 1: Requirements and deadlines for Quantum Executive Orders*

Requirement	Deadline	Applies to
Migrate key establishment systems to PQC standard	December 31, 2030	Federal agencies (high-value assets and high-impact systems); covered contractors
Migrate digital signatures to PQC standard	December 31, 2031	Federal agencies (high-value assets and high-impact systems); covered contractors
Federal Acquisition Regulatory (FAR) Council publish proposed rule requiring PQC for contractors	Within 180 days of signing (approximately December 19, 2026)	FAR Council
Contractor compliance with National Institute of Standards and Technology (NIST) PQC standards (ML-KEM, ML-DSA)	December 31, 2030	Covered contractors working with federal agencies
Agencies designate a PQC migration lead	Near-term agency action	All federal agencies
Commerce Department PQC migration pilot project completed	December 31, 2030	Department of Commerce

¹² Executive Order 14413, “Ushering in the Next Frontier of Quantum Innovation,” 91 Fed. Reg. 38487, June 25, 2026

¹³ Executive Order 14413, “Ushering in the Next Frontier of Quantum Innovation,” 91 Fed. Reg. 38487, June 25, 2026

¹⁴ Executive Order 14413, “Ushering in the Next Frontier of Quantum Innovation,” 91 Fed. Reg. 38487, June 25, 2026

¹⁵ Executive Order 14412, “Securing the Nation Against Advanced Cryptographic Attacks,” 91 Fed. Reg. 38483, June 25, 2026

¹⁶ “Fact Sheet: President Donald J. Trump Secures the Nation Against Advanced Cryptographic Attacks,” The White House, June 22, 2026

¹⁷ Executive Order 14412, “Securing the Nation Against Advanced Cryptographic Attacks,” 91 Fed. Reg. 38483, June 25, 2026

¹⁸ Justin Doubleday, “White House PQC order ‘lights a fire’ under post-quantum transition,” Federal News Network, June 23, 2026

¹⁹ Executive Order 14412, “Securing the Nation Against Advanced Cryptographic Attacks,” 91 Fed. Reg. 38483, June 25, 2026

Requirement	Deadline	Applies to
State Department: assist critical infrastructure and allied partners	Ongoing	Critical infrastructure operators, allied governments
Intelligence assessment of commercial quantum threat to cryptography	Near-term (classified)	Intelligence community

**Refer to sources 1, 2, 3, and 7.*

The direction to intelligence officials to assess the national security implications of commercially available quantum computers is the most underappreciated provision of these orders. It signals that the US government no longer regards Q-Day as a purely classified, state-capacity risk. The harvest-now, decrypt-later (HNDL) threat is operational today—sophisticated adversaries are already collecting encrypted data in anticipation of a quantum decryption capability that may arrive through the commercial market, not just through state programs.

Why this matters beyond the federal government

These orders are written for federal agencies, but their reach extends materially into the private sector through three mechanisms—and organizations in every industry should be reading them accordingly.

1. The contractor mandate is binding and time-limited

The FAR Council has 180 days from signing to publish a proposed rule embedding PQC compliance into federal contract law, with contractor compliance required by December 31, 2030.^{20,21} Any organization that holds or pursues federal contracts—defense contractors, healthcare providers working with Centers for Medicare & Medicaid Services (CMS) or the Veterans Administration (VA), technology vendors, financial institutions serving federal programs, research universities on federal grants—must now treat PQC migration as a contract compliance requirement, not merely a security best practice. The FAR rule will require contractors to meet NIST PQC standards, including the ML-KEM (FIPS 203) and ML-DSA (FIPS 204) algorithms. Organizations that have not started a cryptographic inventory have no basis on which to plan a compliant migration.

2. Critical infrastructure is explicitly framed

The order specifically frames the protection of power grids, water systems, and transportation networks as a motivation for the PQC migration mandate, and directs the State Department to assist critical infrastructure operators in making the same transition as federal systems.^{22,23} For organizations in energy, utilities, healthcare, and transportation—particularly those already subject to sector-specific cybersecurity regulations (North American Electric Reliability Corporation Critical Infrastructure Protection [NERC CIP], Health Insurance Portability and Accountability Act of 1996 [HIPAA], Transportation Security Administration directives)—this order establishes the directional signal that quantum security will become a regulatory compliance requirement, not just a risk-management choice.

3. The commercial quantum intelligence assessment changes the threat calculus

The direction to intelligence agencies to assess the national security implications of commercially available quantum computers reflects a significant evolution in policy thinking. It confirms that the US government regards Q-Day as a near-term operational risk, not a distant theoretical one. The HNDL model is active: adversaries are already archiving today's encrypted federal and contractor communications, waiting for the quantum capability to arrive. Organizations that treat 2030 as the start of their quantum security program are, by definition, already behind.

²⁰ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

²¹ "Fact Sheet: President Donald J. Trump Secures the Nation Against Advanced Cryptographic Attacks," The White House, June 22, 2026

²² Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

²³ "Fact Sheet: President Donald J. Trump Secures the Nation Against Advanced Cryptographic Attacks," The White House, June 22, 2026

"[The executive order] really lights a fire under everyone to say, 'Hey, this is something that the government's taking seriously.' It drops it right in the CIO's lap to say, 'I've got to get this ready. This is not for somebody else's tenure 10 years from now. It's my tenure now that I have to get this done.'"—Garfield Jones, former Associate Chief of Strategic Technology, CISA; Executive Vice President for Strategy and Research, QuSecure, quoted in Federal News Network, June 23, 2026²⁴

What organizations should do now: The KPMG Q-PREP response

These executive orders confirm what KPMG has been advising clients: The PQC migration is not a future information technology (IT) project—it is a present-tense governance and compliance program. With 2030 now an accelerated federal deadline, organizations have fewer than four years to complete what is, for most, the largest cryptographic infrastructure change they will ever undertake. The KPMG Q-PREP methodology provides a structured, seven-phase pathway that begins with three actions every organization should take immediately.

Immediate actions—Q3/Q4 2026

- **Designate a quantum champion.** The order requires federal agencies to designate a PQC migration lead.^{25,26} Every organization with federal contractor exposure, critical infrastructure obligations, or regulated data environments should do the same—with cross-functional authority spanning IT, security, legal, procurement, and compliance.
- **Conduct a cryptographic asset inventory.** The 2030 deadline applies to high-value assets and high-impact systems.²⁷ You cannot sequence a migration until you know what you have. A Cryptographic Bill of Materials (CBOM)—mapping every asset, protocol, algorithm, and key length across the enterprise, including third-party and supply chain connections—is the non-negotiable first step.
- **Classify assets by HNDL exposure, not just algorithm strength.** The compliance deadline is a floor, not a ceiling. Assets transmitting long-lived sensitive data—IP, regulated health information, defense-relevant research—must be prioritized based on how long that data retains its value. The adversary is already collecting.

2027–2030: Migrate, validate, and demonstrate compliance

- **Pilot hybrid PQC configurations** in 2027 for external-facing and inter-agency/contractor communication channels, using ML-KEM (FIPS 203) and ML-DSA (FIPS 204).
- **Engage your supply chain.** The FAR contractor requirement will cascade downstream. Audit third-party cryptographic readiness now and embed PQC requirements in contract renewals and RFPs.
- **Build the compliance evidence trail.** FAR compliance will need to be demonstrated, not just claimed. Automated cryptographic monitoring and continuous CBOM maintenance are the infrastructure for that evidence.
- **Track the Commerce Department pilot (due December 31, 2027^{28,29}).** KPMG is actively monitoring regulatory output and will translate guidance into client-ready frameworks as it is released.

²⁴ Justin Doubleday, "White House PQC order 'lights a fire' under post-quantum transition," Federal News Network, June 23, 2026

²⁵ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

²⁶ Justin Doubleday, "White House PQC order 'lights a fire' under post-quantum transition," Federal News Network, June 23, 2026

²⁷ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

²⁸ Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," 91 Fed. Reg. 38483, June 25, 2026

²⁹ "Fact Sheet: President Donald J. Trump Secures the Nation Against Advanced Cryptographic Attacks," The White House, June 22, 2026

Sector-specific implications at-a-glance

Sector	Key exposure	Priority actions
Defense and government contractors	Direct FAR mandate by 2030; existing CMMC and cybersecurity contract requirements	Immediate CBOM; designate PQC lead; build FAR compliance attestation capability
Healthcare and life sciences	Federal program exposure (CMS, VA, NIH); HIPAA-regulated data with long retention; validated GxP systems	CBOM across OT/lab systems; HNDL risk assessment of long-lived IP; GxP-aware migration planning
Financial services	DORA (EU); potential federal program exposure; long-lived customer and transaction data	Cryptographic inventory; PKI/TLS migration roadmap; third-party vendor PQC assessments
Energy and utilities	Critical infrastructure explicitly named; NERC CIP framework; OT/ICS with 15- to 20-year lifespans	OT asset discovery; network-layer protection for legacy systems; regulatory engagement
Higher education and research	Federal research grant obligations; quantum counterintelligence protection mandate; sensitive research IP	Research data HNDL classification; supply-chain review; engage updated quantum CI guidance
Technology and software-as-a-service	Federal contractor pipeline; products serving regulated industries	Product PQC roadmap; CBOM disclosure capability; customer-facing PQC readiness communications

The bottom line

President Trump's quantum executive orders signal that the US government has moved from planning to mandate. The 2030 and 2031 deadlines are real. The FAR contractor requirements are binding. The critical infrastructure framing reaches across sectors. And the direction to assess the threat from commercially available quantum computers confirms that the US intelligence community regards Q-Day as a near-term operational risk, not a distant theoretical one.

The KPMG Q-PREP methodology is designed precisely for this moment: a structured, risk-prioritized, governance-grounded approach to quantum security that meets organizations where they are and builds the program they will need to meet both the 2030 compliance deadline and the underlying threat it was designed to address.

Contact us



Dr. Aaron Kemp

US Quantum Leader
KPMG LLP

aaronkemp@kpmg.com



Dr. Lekshmy Sankar

Head of Quantum Security
KPMG LLP

lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



[kpmg.com](https://www.kpmg.com)

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043489-2A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.