

June 30, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

New Executive Orders and Government Strategy Advance US Quantum Innovation and Mandate Post-Quantum Cryptography Transition

Executive Summary

- **What's new:** On June 22, 2026, President Trump signed two executive orders to expand the use and development of quantum technology. Executive Order 14412 accelerates the adoption of post-quantum cryptography in critical federal and private sector systems to address emerging post-quantum threats. Executive Order 14413 seeks to accelerate U.S. quantum innovation in computing, sensing, networking, supply chains and workforce development.
- **Why it matters:** The executive orders establish timelines and enforceable obligations for federal agencies and government contractors to implement NIST-approved post-quantum cryptography standards and related implementation, validation and procurement requirements.
- **What to do next:** Federal contractors and subcontractors, critical infrastructure companies, software and cloud providers, and companies developing or deploying quantum-related technologies should prepare for an accelerating timeline to transition to post-quantum cryptography and consider assessing long-standing sensitive data, vendor post-quantum cryptography road maps and cryptographic bill of materials readiness.

On June 22, 2026, President Donald Trump signed two executive orders (“EOs” or the “Orders”) addressing quantum technology:

- EO 14412, “Securing the Nation Against Advanced Cryptographic Attacks” (Cryptographic Order).
- EO 14413, “Ushering in the Next Frontier of Quantum Innovation” (Quantum Innovation Order).

The Orders direct the government to prepare for and facilitate the emergence of quantum technologies, which have the potential to revolutionize computation, communication and sensing capabilities by manipulating the properties of subatomic particles (*i.e.*, quantum mechanics).

Foremost among the expected risks of quantum computing is the power to make existing cryptographic systems obsolete, including those that keep global financial systems, government defense and intelligence systems, and other highly sensitive digital operations secure.

New Executive Orders and Government Strategy Advance US Quantum Innovation and Mandate Post-Quantum Cryptography Transition

The Cryptographic Order accelerates the development of National Institute of Standards and Technology (NIST)-approved Federal Information Processing Standards (FIPS) for post-quantum cryptography (PQC) and requires FIPS compliance from federal agencies and government contractors. (See also our June 29, 2026, client alert [“Big Changes Coming for Government Contractors: Proposed FAR CUI and DoW FOCI Rules, New Quantum Cryptography Order and Ongoing CMMC Rollout.”](#))

The Quantum Innovation Order directs a coordinated, whole-of-government approach to accelerate the development, deployment and commercialization of quantum computing, sensing and networking technologies.

The Orders build on prior executive and legislative actions related to the emerging technology:

- In December 2018, the National Quantum Initiative Act surged federal funding for research and development of quantum technology.
- In May 2022, President Joe Biden issued National Security Memorandum 10, which ordered sensitive federal government systems to migrate to PQC by 2035.
- President Biden also signed the Quantum Computing Cybersecurity Preparedness Act in December 2022, which further supported the transition to PQC across the federal government.

The Orders establish the Trump administration’s quantum technology agenda and reflect the view that these technologies represent a transformative opportunity and an urgent national security challenge requiring immediate action.

Key Provisions

EO 14412 – Securing the Nation Against Advanced Cryptographic Attacks

The Cryptographic Order addresses the risk that adversaries may harvest highly sensitive but encrypted material, which is currently unreadable, and store it until large-scale quantum computing makes today’s state-of-the-art cryptography obsolete. As a result, sensitive encrypted data related to intelligence assets, personal health and trade secrets is at risk even before the quantum technology to decrypt it exists.

The Cryptographic Order accelerates the previous 2035 PQC migration deadline to 2030 for key compliance requirements.

PQC coordination. The Cryptographic Order assigns coordination and oversight of national PQC migration policy to the director of the Office of Management and Budget (OMB) and the national cyber director (together, the “Coordinating Authorities”). Technical support and guidance will be provided by the secretary of Commerce, through the director of NIST, and in consultation with the director of the National Security Agency (NSA) and the secretary of Homeland Security through the director of the Cybersecurity and Infrastructure Security Agency (CISA). Within 30 days, each agency head must designate a PQC migration lead responsible for overseeing agencywide cryptographic inventory management, developing a prioritized PQC migration plan and coordinating cross-agency efforts in PQC.

PQC transition. Within 90 days, the Coordinating Authorities, in consultation with the secretary of Homeland Security through the director of CISA, must issue guidance requiring agencies to review their inventory of designated “high value assets” (HVAs) and “high impact systems” and transition both to PQC — by December 31, 2030, for cryptographic key establishment and by December 31, 2031, for digital signatures. Also within 90 days, each agency must submit a plan to the Coordinating Authorities to accomplish the Cryptographic Order’s directives. NIST is directed to initiate a PQC migration pilot project on its own systems within 180 days, which must be completed by December 31, 2027.

Government procurement and rulemaking.

The Cryptographic Order’s procurement mandate requires that within 180 days, the Federal Acquisition Regulatory (FAR) Council, in consultation with the secretary of Homeland Security through the CISA and NIST directors, publish a proposed rule requiring covered contractors to comply with NIST’s FIPS, including all those that incorporate PQC-compliant algorithms, by December 31, 2030. Within 270 days, the FAR Council must publish a separate proposed rule requiring covered contractors to implement vulnerability disclosure policies (VDPs) that incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS-approved algorithms. Given the weight of federal procurement requirements throughout the private sector, this requirement is expected to flow through the government supplier ecosystem and spur PQC adoption across a broader swath of the U.S. economy by 2030.

New Executive Orders and Government Strategy Advance US Quantum Innovation and Mandate Post-Quantum Cryptography Transition

Department of War (DoW)¹ PQC Strategy and implications for the defense industrial base. On June 23, 2026, the DoW released its Post Quantum Cryptography Strategy (the Strategy), which provides a concrete example of how PQC migration is likely to reshape the U.S. federal contractor ecosystem. The Strategy adopts deadlines aligned with the Cryptographic Order: It requires that all DoW systems “support” PQC or be phased out no later than December 31, 2030, and that all DoW systems “use” PQC no later than December 31, 2031. The Strategy is expansive, noting that “nearly every deployed military asset will be affected in some way.” It calls for a rapid, enterprisewide transition spanning DoW networks, weapon systems, satellite and space systems, secure tactical radios and telephony, edge devices, and related IT infrastructure.

Echoing the Cryptographic Order’s procurement focus, the Strategy directs the DoW to update its acquisition processes and integrate PQC-compliant commercial products into contract requirements; to accelerate the intake, testing and deployment of commercial PQC-supporting technologies through streamlined NSA certification and evaluation; and to extend cryptographic requirements across the Defense Industrial Base, including updates to the Cybersecurity Maturity Model Certification (CMMC) to incorporate PQC. Notably, the Strategy underscores that PQC readiness is not solely an information technology (IT) enterprise undertaking; it includes implementation in product design, public key infrastructure and certificate modernization, secure software and firmware signing, and other mission-supporting technologies across the cryptographic life cycle.

Critical infrastructure and international engagement.

The Cryptographic Order requires all designated Sector Risk Management Agencies to work with the Department of Homeland Security through the director of CISA “to assist critical infrastructure owners and operators in developing their PQC migration plans.” The order also requires several executive branch officials to coordinate engagement with foreign governments and industry groups to encourage their transition to NIST-standardized PQC algorithms.

Cryptographic bill of materials. Within 270 days, the secretary of Homeland Security, through the director of CISA and in coordination with NIST, must release public guidance describing the minimum elements for a cryptographic bill of materials (CBOM) that enables automated assessment of the cryptographic assets utilized by a hardware or software element. This element represents an important step in the broader PQC migration, as an

effective CBOM would facilitate programmatic audits of an entity’s cryptographic posture and could become as critical to supply chain security initiatives as software bills of materials (SBOMs) are today.

EO 14413 – Ushering in the Next Frontier of Quantum Innovation

The Quantum Innovation Order seeks to accelerate the development of American quantum information science and technology (QIST) by driving innovation in quantum computing, sensing and networking. This component of the Trump administration’s quantum strategy aims to establish a U.S.-based ecosystem of quantum technologies spanning research, manufacturing and commercial applications. The Quantum Innovation Order directs federal agencies to take actions to spur U.S. quantum capabilities while hindering the development of adversarial capabilities through export controls and investment restrictions.

Quantum-enabled scientific discovery. The Quantum Innovation Order establishes the Quantum Computer for Application Development and Discovery Science (QC-ADDs) Effort, an initiative to develop a quantum computer capable of pursuing scientific discoveries. The Effort’s goal is to deliver such a quantum computer to a Department of Energy facility and make it available to the scientific community. The Quantum Innovation Order directs several cabinet secretaries and executive agencies to collaborate to provide the relevant expertise, capabilities and manufacturing infrastructure for the Effort, and to explore the deployment of these resources for commercial, government and national security applications. Within 90 days of issuance, the secretary of Energy, in coordination with relevant agencies, must identify the required technical specifications for QC-ADDs performance and publish identified economically significant applications for the Effort beyond the capabilities of current computing.

Private sector engagement and the quantum supply chain.

The Quantum Innovation Order contains several mechanisms to spur private sector development of quantum technologies. It requires that within 120 days, the secretaries of War, Commerce and Energy, as well as the director of the National Science Foundation (NSF), develop a plan to partner with the private sector, including via prize challenges or advance market commitments, to develop quantum-enabling component technologies domestically. It also orders the director of NSF to pursue grants to establish quantum “user facilities” and directs that steps be taken to increase private sector access to DoW-sponsored quantum-relevant foundry resources. It also includes workforce development provisions such as the expansion of

¹ Congress has not yet acted on the administration’s renaming of the Department of Defense.

New Executive Orders and Government Strategy Advance US Quantum Innovation and Mandate Post-Quantum Cryptography Transition

quantum-relevant apprenticeships and post-secondary training opportunities, as well as the establishment of a network of National QIST Workforce Development Institutes to further boost the nascent domestic quantum-industrial ecosystem.

The Quantum Innovation Order also calls on officials to identify “any changes to statutory or regulatory authorities” needed to address potential market hurdles and to “eliminate QIST manufacturing barriers,” suggesting that legislative or rulemaking initiatives to facilitate private sector activity may soon follow.

Quantum sensors and networks. The Quantum Innovation Order directs particular attention to the development of quantum-enabled sensors and networks, which are likely to have a significant geostrategic impact once the relevant technologies mature. It directs the secretary of War to identify at least three next-generation quantum sensor projects within 60 days of the order, to be fielded by September 30, 2028, and orders the secretaries of Commerce, Energy and the directors of NSF and National Aeronautics and Space Administration (NASA) to each develop five-year plans for advancing quantum sensing and networking applications in their respective domains.

National security restrictions. The Quantum Innovation Order instructs agencies to prevent “countries of concern” from acquiring critical quantum-enabling technologies by harmonizing investment restrictions and export control policies with international allies and partners. The Quantum Innovation Order also directs key figures in the U.S. national security establishment to expand the Quantum Information Science and Technology Counterintelligence Protection Team (QCPT) to coordinate actions against quantum-related threats, conduct messaging and outreach related to identified threats, and enhance sharing of threat information across government, industry and academic institutions. The QCPT will be responsible for coordinating and deconflicting all outreach to “industry and academia related to quantum-specific security guidance and threat information.”

International engagement. The Quantum Innovation Order calls for the secretaries of State and Commerce to align engagements to ensure U.S. quantum companies have access to strategic markets, maintain trusted supply chains, and promote quantum technology development and protection efforts with like-minded countries. It also directs the secretary of Commerce, in coordination with the U.S. trade representative, to identify and provide recommendations on foreign trade barriers, discriminatory treatment and other policies that “limit the competitiveness” of U.S. quantum companies. These provisions may signal that the U.S. wants to avoid the recent challenges

faced in the contest for secure access to rare earth minerals by developing the quantum supply chain among allied nations at the outset.

Looking Ahead

Together, the Orders outline a broad and multifaceted approach to a still-nascent technology, providing businesses time to strategically adapt before commercial or regulatory pressures mount. In particular, businesses should consider the following:

- **Map long-standing sensitive data and “harvest now, decrypt later” exposure.** Companies should identify sensitive data that must be kept confidential for years, including trade secrets and other intellectual property, health data, sensitive personal information, authentication information and national security-related information.
- **Build or update existing cryptographic inventories.** A meaningful PQC transition will require companies to know where vulnerable cryptography is used across applications, infrastructure, products, vendors, cloud services, software and firmware signing, identity systems and embedded devices.
- **Monitor FAR developments and customer flowdowns.** Federal contractors, subcontractors and suppliers should closely track forthcoming FAR proposals requiring covered contractors to comply with NIST FIPS, including applicable PQC FIPS, and implement vulnerability disclosure policies that address cryptographic vulnerabilities.
- **Prepare for CBOM expectations.** Forthcoming guidance from NIST and CISA on cryptographic bills of materials may create new expectations for automated assessment of cryptographic assets in hardware and software, similar to the growing role of SBOMs in software supply chain security.
- **Seek opportunities for collaboration and additional funding.** The Orders may present commercial opportunities to capitalize on government funding and developmental partnerships, warranting close attention to developments at the primary agencies listed in the Orders.
- **Prepare for heightened scrutiny of foreign quantum-related supply chains and personnel.** The Orders signal that the U.S. government intends to leverage economic national security authorities to limit adversaries’ access to significant quantum-enabling industrial components and technologies. Businesses involved in the quantum supply chain ecosystem should assess the extent to which investments, research and development, and partners are present in geographies that may enhance scrutiny from the U.S. government.

New Executive Orders and Government Strategy Advance US Quantum Innovation and Mandate Post-Quantum Cryptography Transition

Contacts

Brian J. Egan

Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

Michael E. Leiter

Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William E. Ridgway

Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon

Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Tatiana O. Sullivan

Partner / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Joshua Silverstein

Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Matthew Urfirer

Associate / Washington, D.C.
202.371.7039
matthew.urfirer@skadden.com

Summer associate **Jay Sheth** contributed to this client alert.