QUANTUM READINESS IS A BOARDROOM ISSUE: A POST-QUANTUM CRYPTOGRAPHY MIGRATION ROADMAP FOR INDUSTRY

Date: 24 November 2026

US Policy and Regulatory Alert

By: Sanjeev Bhasker, Guillermo S. Christensen, Corey Bieber, Ragae Ghabrial, David S. Easwaran

Data protection is already a board-level concern. Recent cybersecurity incidents involving financial institutions, payment networks, and their third-party vendors show how quickly sensitive information can move beyond an organization's control. Quantum computing adds a new dimension to that risk: information encrypted today may be collected by adversaries now and decrypted once sufficiently powerful quantum computers exist. This is not a theoretical issue. The data at risk could be collected today, not in the future.

On 22 June 2026, the White House issued Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, directing federal agencies to accelerate the transition to post-quantum cryptography (PQC). On 27 October 2026, the US Department of Commerce's National Institute of Standards and Technology (NIST) published its migration roadmap for moving away from quantum-vulnerable algorithms. Together, these developments signal that PQC migration is moving from long-term planning toward implementation. Federal deadlines do not automatically apply to every private-sector organization, but they will increasingly shape technology providers, government contractors, critical infrastructure operators, and the wider commercial ecosystem. Organizations that delay planning risk compressed timelines, higher vendor costs, contractual complications, and exposure of sensitive information. This alert examines the threat, the regulatory developments, and the practical steps boards, general counsel, and chief information security officers (CISOs) should take now.

WHAT IS Q-DAY?

Quantum Day, or "Q-Day," is the point at which a sufficiently powerful quantum computer can break the public-key encryption that protects much of today's digital infrastructure, including secure websites, payments, and software updates. Its timing is uncertain. Some industry leaders including Google say it could arrive as early as 2029, while many experts place it in the 2030s. Because the date is uncertain, the practical question is how long your organization needs to find and replace its encryption. For organizations with legacy systems and many vendors, that work can take years, so it is important to prioritize the inventory and migration of your data now.

HARVEST NOW, DECRYPT LATER

The risk is compounded by the "harvest now, decrypt later" threat. Adversaries may collect encrypted information today, store it, and decrypt it once sufficiently powerful quantum computers become available. This creates a present-day concern for information that must remain confidential for ten, twenty, or more years. That describes many companies, including those with trade secrets, intellectual property, financial records, healthcare

©2005-2026 K&L Gates LLP. All Rights Reserved.

information, and sensitive customer data. For trade secret owners, a risk-based PQC migration plan can form part of the reasonable measures required to maintain secrecy under US law (18 U.S.C. § 1839(3)).

WHY NOW: FEDERAL POLICY IS ACCELERATING PQC ADOPTION

Federal policy is moving PQC migration from long-term planning toward implementation. Recent developments are particularly important for industry.

Executive Order 14412

The President directs federal agencies to accelerate PQC adoption, prioritize high-value assets and high-impact systems, and coordinate migration efforts. It establishes federal migration milestones, including 31 December 2030, for key establishment and 31 December 2031, for digital signatures in high-value assets and high-impact systems.

NIST Standards and Guidance

NIST has finalized three principal PQC standards: FIPS 203 (ML-KEM) for key establishment, and FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures. Its 27 October 2026, report, Transition to Post-Quantum Cryptography Standards (NIST IR 8547), provides additional direction for transitioning away from quantum-vulnerable algorithms, with those algorithms deprecated after 2030 and disallowed after 2035. The Office of Management and Budget's Memorandum M-26-15, issued 24 June 2026, requires agencies to align their migration plans with NIST IR 8547 and sets 2035 as the target for completing the broader federal migration.

Federal Procurement

The executive order also directs the Federal Acquisition Regulatory (FAR) Council to publish, by mid-December 2026, a proposed rule requiring "covered contractors" to comply with NIST's Federal Information Processing Standards (FIPS), including the PQC standards. For the PQC signature standards, compliance would be due 31 December 2030, one year ahead of the 31 December 2031 federal deadline for digital signatures. A second proposed rule, due in March 2027, would require covered contractors to maintain vulnerability disclosure programs that capture cryptographic weaknesses, including the use of algorithms not approved under FIPS. The order does not define "covered contractor"; the rulemaking will. Government contractors and technology suppliers should monitor these developments and assess their vendors' and products' migration readiness.

Who is Subject

The order binds federal agencies, not private companies. Private-sector organizations fall into three groups. Federal contractors, and the subcontractors and technology suppliers that support them, should expect the requirements to reach them through contract clauses and flow-down provisions once the FAR rule is final. Critical infrastructure owners and operators do not face a new mandate under the order, but it directs Sector Risk Management Agencies (the federal agencies responsible for security in each critical infrastructure area) and the Cybersecurity and Infrastructure Security Agency (CISA) to help them develop migration plans, which will shape expectations in those sectors. All other organizations have no direct obligation, but will encounter these requirements through vendors, customers, and contract negotiations as federal standards become the commercial baseline.

©2005-2026 K&L Gates LLP. All Rights Reserved.

WHAT RECENT CYBERSECURITY BREACHES TELL US ABOUT THIRD-PARTY RISK

Breaches of consumer data have become routine, and many start with a vendor. In November 2026, a leading US bank warned customers that attackers had reached marketing data held by third-party vendors. Two well-known card networks reported exposures at outside providers the following week, though neither reported that payment card numbers were compromised. The lesson is that a company's security depends on every vendor that holds its data. The same is true of cryptography. An organization that cannot list its third-party systems and the encryption they use will not know which ones depend on algorithms that quantum computers could break.

The broader lesson is that an organization's cybersecurity posture depends on more than the systems it owns and operates. Vendors, cloud providers, software developers, and managed service providers may have access to sensitive information or support critical business functions. PQC migration should therefore be treated as an enterprise-wide supply-chain security initiative. Organizations need visibility into internal systems and external technology dependencies, including cloud services, software, hardware, connected devices, operational technology, and vendor-managed infrastructure.

THE PQC MIGRATION ROADMAP: FIVE STEPS FOR INDUSTRY

PQC migration is not simply a matter of installing new encryption software. It requires organizations to understand where cryptography is used, identify vulnerable dependencies, assess business priorities, and coordinate technology changes across the enterprise.
Organizations should consider the following five-step approach:

Inventory: Identify Cryptographic Assets and Dependencies

Develop a comprehensive inventory of cryptographic assets, including algorithms, libraries, certificates, public-key infrastructure (PKI), hardware security modules, applications, cloud services, databases, connected devices, and third-party technology. Identify where sensitive information resides, how it is protected, and which vendors have access to it. A cryptographic bill of materials (CBOM) can help improve visibility into cryptographic components embedded in software and hardware. The executive order directs CISA and NIST to publish guidance on the minimum elements of a CBOM by March 2027.

Prioritize: Assess Risk Based on Data Sensitivity and Business Criticality

Prioritize systems based on the sensitivity and expected useful life of the information they protect, the consequences of compromise, external exposure, and migration complexity. Information requiring long-term confidentiality, critical infrastructure, intellectual property, financial records, and sensitive customer data deserve particular attention. Systems requiring significant redesign may need to enter the migration pipeline earlier than applications that can be updated through routine software releases.

Assess Vendors: Address Third-Party Readiness

Engage critical vendors to understand their PQC roadmaps, implementation plans, and product timelines. Evaluate whether contracts adequately address cryptographic modernization, security standards, vulnerability disclosure, incident notification, and vendor cooperation during migration. Organizations should seek specific

©2005-2026 K&L Gates LLP. All Rights Reserved.

information about supported standards and upgrade commitments rather than assuming general cybersecurity certifications establish PQC readiness. Compliance with NIST standards does not itself establish patent freedom to operate. Organizations should also assess third-party patent rights, software licensing obligations, upgrade rights, and IP infringement indemnities.

Pilot: Test PQC Implementations and Hybrid Configurations

Conduct controlled pilots to evaluate performance, interoperability, operational impacts, and security considerations. Hybrid configurations that combine conventional and post-quantum algorithms may provide a useful transition strategy in appropriate environments. Testing should address network performance, latency, bandwidth, hardware requirements, certificate sizes, authentication processes, and compatibility with existing applications and vendors. Where migration involves developing new technology, address ownership of resulting IP and evaluate patent protection for potentially patentable improvements before public disclosure.

Migrate and Monitor: Build for Cryptographic Agility

Implement migration in phases, beginning with the highest-risk systems. Establish measurable milestones, assign executive accountability, and report progress regularly to management and the board. Organizations should also build cryptographic agility, meaning the ability to replace or update algorithms and cryptographic implementations without requiring a complete technology overhaul. PQC migration should be treated as an ongoing governance responsibility, not a one-time compliance exercise.

QUESTIONS BOARDS AND EXECUTIVE LEADERSHIP SHOULD BE ASKING

Quantum readiness should become a regular component of enterprise cybersecurity and risk-management discussions. Directors and senior executives do not need to understand the mathematics of quantum computing, but they should understand their organization's exposure, migration strategy, resource requirements, and accountability structure.

Boards and executive leadership should consider whether management can answer five fundamental questions:

1. Visibility: Does the organization have a comprehensive inventory of cryptographic assets, including third-party vendors and cloud service providers?
2. Data exposure: Which categories of information must remain confidential for ten, twenty, or more years, and could that information be vulnerable to harvest-now, decrypt-later attacks?
3. Accountability: Has an executive been designated to coordinate PQC migration across cybersecurity, information technology, legal, compliance, and procurement functions?
4. Investment: Has management developed a funded migration strategy that accounts for legacy infrastructure, vendor dependencies, and system replacement costs?
5. Vendor readiness: Are critical suppliers developing PQC migration plans, and do existing contracts adequately address cryptographic modernization?

A board does not need to manage the technical migration. It should, however, ensure that management has a documented strategy, appropriate resources, and a process for evaluating and addressing quantum-related risks.

©2005-2026 K&L Gates LLP. All Rights Reserved.

QUANTUM GOVERNANCE PLAN

A quantum governance plan turns an uncertain, long-term risk into a managed business responsibility. Without one, the issue tends to drift between teams: security assumes IT owns it, IT assumes legal owns it, and nobody owns the budget. A written plan names an accountable executive, sets out who handles each part, and gives the board a regular way to check progress.

The plan also protects the company later. If regulators, customers, or business partners ask what the company did and when, a dated plan with funding and milestones shows that leadership took the risk seriously and acted on it. That record is far easier to produce than one reconstructed after a dispute begins.

Acting early costs less than acting under pressure. Spending spread over several years fits normal budget cycles and planned system upgrades. Waiting until a regulator, a major customer, or a government contract forces the issue usually means paying for rush work, emergency hiring, and changes made without time to test. Companies that start now also have more room to negotiate with their technology vendors before everyone else is asking for the same upgrades.

HOW THE FIRM CAN HELP

The fim's multidisciplinary team advises clients on the legal, regulatory, cybersecurity, procurement, and national-security dimensions of emerging quantum technologies. Our lawyers include former government officials with experience in the White House, the intelligence community, and the US Department of Justice.

We help clients evaluate quantum-related cybersecurity risks, develop enterprise quantum governance frameworks, assess regulatory and contractual exposure, review vendor commitments, prepare for evolving federal procurement requirements, and coordinate PQC migration planning with cybersecurity, privacy, and technology teams. Our team also advises on government contracting, critical infrastructure security, technology transactions, regulatory investigations, and intellectual property considerations involving quantum-resistant technologies.

Start This Quarter

One of the most useful first steps is a cryptographic inventory identifying where your organization relies on encryption, which vendors support those systems, what information must remain protected, and how long that protection must last. Organizations that begin this process now will be better positioned to manage migration costs, meet evolving expectations, and protect sensitive information as the quantum landscape develops.

Contact the firm to discuss how to develop a cryptographic inventory and enterprise quantum governance plan. For more on the federal executive order and what it means for your organization, read our earlier client alert: Preparing for Q-Day: New Executive Orders Address Quantum Innovation and Post-Quantum Cryptography.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



SANJEEV BHASKER
PARTNER

WASHINGTON, DC, MIAMI, CHARLOTTE
+1.202.778.9260
SANJEEV.BHASKER@KLGATES.COM



COREY BIEBER
PARTNER

CHICAGO
+1.312.807.4390
COREY.BIEBER@KLGATES.COM



DAVID S. EASWARAN
PARTNER

CHARLOTTE
+1.704.331.7455
DAVID.EASWARAN@KLGATES.COM



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



RAGAE GHABRIAL
PARTNER

PITTSBURGH
+1.412.355.8690
RAGAE.GHABRIAL@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.