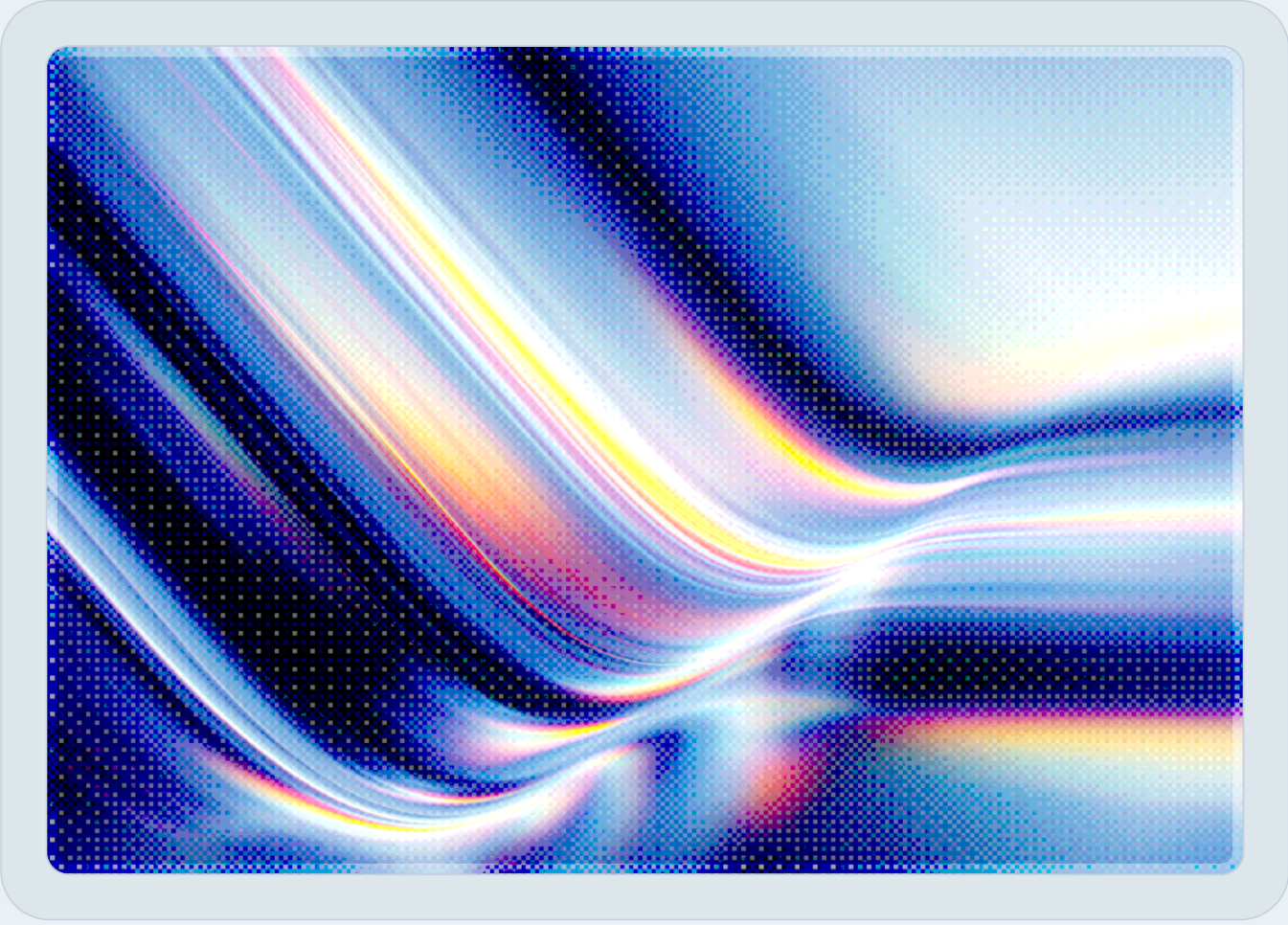
CSAI Foundation | Cloud Security Alliance

Post-Quantum Cryptography: From Guidance to Mandate

2026-07-10

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Post-quantum cryptography has moved from a research-and-planning exercise into an enforceable compliance obligation in the span of a few weeks. France's national cybersecurity agency, ANSSI, announced it will stop certifying non-quantum-safe security products starting in 2027 and expects businesses to buy exclusively quantum-safe products by 2030 [1]. In the United States, Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," signed June 22, 2026 alongside a companion order on broader quantum research, and the accompanying OMB Memorandum M-26-15, impose binding migration deadlines on federal agencies, with key-establishment cryptography required to be quantum-safe by the end of 2030 and digital signatures by the end of 2031 for high-value assets [2][6]. Forrester has characterized inaction in the face of this convergence of national mandates as "quantum negligence," arguing that boards which fail to match the federal government's posture will struggle to justify a lower standard of care if litigation follows a future breach of long-lived encrypted data [4]. For CISOs, the practical effect is that post-quantum migration is no longer an optional roadmap item to be revisited when NIST's algorithms mature; it is a procurement gate, a certification requirement, and, increasingly, a contractual and legal exposure that demands board-level accountability now.

Background

The cryptographic transition away from RSA, Diffie-Hellman, and elliptic-curve algorithms has been anticipated for years, driven by the eventual arrival of cryptographically relevant quantum computers capable of running Shor's algorithm against public-key systems. What changed in mid-2026 is not the underlying technical threat but the regulatory posture toward it. NIST finalized its first three post-quantum cryptography standards in August 2024 after an eight-year, multi-round evaluation process: FIPS 203 (ML-KEM, a lattice-based key encapsulation mechanism derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, a lattice-based signature scheme), and FIPS 205 (SLH-DSA, a hash-based signature scheme offered as a structurally distinct backup) [5]. Those standards gave regulators and standards bodies around the world a concrete technical baseline to point to, and over the following two years more than a dozen major economies — including the United States, the European Union, the United Kingdom, Germany, France, Australia, Canada, Japan, South Korea, India, Singapore, and the UAE — published their own post-quantum guidance or roadmaps [3].

Through 2024 and 2025, most of that guidance remained aspirational: recommended timelines, best-practice frameworks, and voluntary readiness assessments. The European Commission's April 2024 Recommendation on a Coordinated Implementation Roadmap, formalized with EU member states in June 2025, set targets asking member states to begin transitioning by the end of 2026 and to protect critical infrastructure with post-quantum cryptography no later than 2030, with as many systems as practically feasible converted by 2035 [7]. The U.S. National Security Agency's CNSA 2.0 suite, first published in 2022, laid out a similarly phased expectation: software and firmware signing, browsers, and cloud services were to support and prefer CNSA 2.0 by 2025, with full exclusive enforcement across National Security Systems reached in stages between 2030 and 2033, aligning with the broader 2035 quantum-resistance target set by National Security Memorandum 10 [8].

What distinguishes the summer of 2026 is the shift from roadmap to rule. ANSSI's announcement that it will stop certifying non-quantum-safe products from 2027 converts what had been a voluntary best practice into a binding gate for any vendor selling into the French government or regulated critical-infrastructure market, since ANSSI certification is a prerequisite for those sales [1]. Days apart, the White House's June 22, 2026 Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks" — issued alongside a companion order addressing broader quantum computing research and workforce development — and OMB's June 24, 2026 implementing memorandum, M-26-15, did the analogous thing for the U.S. federal government: they replaced general encouragement with a five-phase migration schedule that runs from 2026 through 2035 across the federal estate, with concrete 2030 and 2031 deadlines for high-value assets, a longer 2035 horizon for the remaining, lower-priority systems, and a hard requirement that every federal agency submit a post-quantum migration plan to OMB within 120 days — a deadline that falls around October 22, 2026 [2][6]. Together, these actions mean that organizations selling into, contracting with, or operating alongside these governments no longer have the option of treating post-quantum readiness as a multi-year strategic aspiration; it is now a near-term procurement and certification condition.

Security Analysis

The core technical risk driving this shift predates the regulatory action: adversaries capable of intercepting and storing encrypted traffic today can decrypt it retroactively once a cryptographically relevant quantum computer becomes available, a pattern commonly described as "store now, decrypt later" or "harvest now, decrypt later." Because this attack does not require the adversary to act at the moment of interception, any data whose confidentiality or integrity must hold beyond the arrival of such a machine is exposed today, regardless of how far off that arrival date is. Estimates for when a cryptographically relevant quantum computer might exist still cluster around the early 2030s, but the risk calculus does not depend on precision in that estimate — it depends on whether the data being

protected will still matter by then. This is the framing CSA's Quantum-Safe Security Working Group has emphasized in its own guidance: the determining question for any given system is not "how vulnerable is this algorithm" but "will the data this algorithm protects still have value at Q-Day."

That framing matters because it clarifies which parts of the regulatory push are technically substantive and which are more about governance and accountability. Public-key algorithms — RSA, Diffie-Hellman, and elliptic-curve schemes — are the primary casualties of Shor's algorithm and require wholesale replacement with lattice-based or hash-based alternatives such as ML-KEM, ML-DSA, and SLH-DSA. Symmetric cryptography and hash functions are only weakened, not broken, by Grover's algorithm, which is why data encrypted at rest with 256-bit symmetric ciphers is not considered quantum-vulnerable in the same way [9]. This distinction meaningfully narrows the scope of what needs urgent replacement: session establishment protocols (TLS, SSH, IPsec/IKE), key management and hardware security module infrastructure that ultimately relies on public-key wrapping, X.509 certificates with expiration dates that extend past the early 2030s, and any non-repudiation function built on digital signatures are the highest-priority targets, while properly implemented AES-256 data-at-rest encryption is not.

The compliance dimension introduces risks that are organizational rather than cryptographic. Because ANSSI, CNSA 2.0, and OMB M-26-15 each define their own phased timelines, multinational organizations now face a patchwork of overlapping deadlines that differ by jurisdiction, sector, and system classification — a 2027 procurement gate in France, a 2027 CNSA 2.0 procurement gate for products bound for U.S. national security systems, and a 2030–2031 operational deadline for U.S. federal high-value assets, layered on top of the EU's 2026-start, 2030-critical-infrastructure, 2035-completion roadmap. Vendors selling security products into multiple regulated markets will need to track certification and procurement requirements separately, and enterprises relying on those vendors inherit whatever gaps exist in the vendor's own migration posture. Forrester's "quantum negligence" argument adds a second, less technical but increasingly material risk: as the U.S. federal government formalizes a structured migration timeline through statute-backed executive action, that timeline becomes a reference point for what a "reasonable" standard of care looks like, which plaintiffs' counsel and regulators can invoke after a future breach involving long-lived encrypted data that was never migrated [4]. Cyber insurance underwriters are likely to follow the same logic, incorporating PQC migration status into renewal terms and premium calculations well before any breach actually occurs.

A further risk worth naming directly: PQC tooling maturity has not caught up with the compliance timelines being imposed on it. Most PQC cryptographic libraries and hardware security module integrations remain in early production or pilot status, mainstream operating system and network equipment support is inconsistent across vendors and versions, and hybrid key-exchange modes (combining a classical algorithm like X25519 with ML-KEM) are still the most common production deployment pattern rather than pure post-quantum implementations. Organizations racing to meet

2027 procurement deadlines may find themselves selecting from an immature vendor ecosystem, which raises its own operational and interoperability risk that regulators have not yet fully addressed in their compliance frameworks.

Recommendations

Immediate Actions

Security leaders should treat the next two quarters as an inventory and accountability window rather than a migration-execution window. Organizations should identify which of their products, services, or contracts touch French government or critical-infrastructure procurement, U.S. federal contracting, or U.S. national security systems, since these are the channels where 2027 certification and procurement gates apply directly. In parallel, security teams should build or update a cryptographic inventory that classifies systems into the three categories AWS's CISO guidance recommends: components that vendors will upgrade automatically, components that require replacement, and internally built or managed systems that the organization must migrate itself [3]. Executive and board sponsorship should be secured now, framed explicitly around the compliance and liability exposure documented above rather than as a purely technical modernization project, since Forrester's negligence framing suggests that board-level visibility into migration status may itself become an audit and disclosure expectation [4].

Short-Term Mitigations

Over the next twelve to eighteen months, organizations should prioritize migrating session-establishment protocols and long-lived certificates using hybrid key-exchange modes that pair a classical algorithm with ML-KEM, which preserves interoperability with legacy systems while introducing quantum resistance. Certificates and non-repudiation functions with validity periods extending past the early 2030s should be flagged for early replacement, since these are the components most exposed to store-now-decrypt-later risk. Contractual language covering post-quantum readiness should be embedded into new and renewing vendor and supplier agreements, and procurement teams should begin requiring PQC roadmap disclosures from security product vendors as a standard due-diligence item. Organizations should also begin building the cryptographic telemetry AWS recommends – tracking which algorithms are in use where, and what percentage of the estate has moved to PQC – since this data will be needed both to demonstrate progress to regulators and to prioritize the highest-risk remaining gaps [3].

Strategic Considerations

Longer term, the objective should shift from a one-time migration project to durable cryptographic agility: the organizational and technical capacity to rotate algorithms and protocols on a recurring basis without a multi-year re-architecture effort each time. Historical precedent argues for starting early rather than waiting for tooling to mature — the deprecation of SHA-1 took nearly two decades industry-wide despite broad technical consensus that it was necessary [3]. Organizations should also monitor how cyber insurance carriers begin incorporating PQC migration status into underwriting, since this is likely to become a practical forcing function independent of any specific regulatory deadline. Finally, given the divergence between the EU's 2035 completion target, the U.S. federal government's 2030–2033 phased CNSA 2.0 enforcement, and France's 2027 certification cutoff, multinational organizations should build a single internal migration timeline calibrated to the earliest binding deadline they face in any jurisdiction, rather than managing separate regional workstreams that risk under-prioritizing the most urgent one.

CSA Resource Alignment

CSA's Quantum-Safe Security Working Group has published directly on-topic guidance that predates and anticipates this regulatory shift. The most specific and recent artifact is A Practitioner's Guide to Post-Quantum Cryptography (2025), which gives enterprises a structured, two-phase methodology — risk assessment followed by mitigation planning — for identifying at-risk data assets, mapping vulnerable cryptographic functions such as TLS, SSH, IPsec, and certificate infrastructure, and prioritizing migration using CSA's Cloud Controls Matrix as the governance backbone. Its central analytical device, evaluating risk according to whether a given piece of data will retain value by the time cryptographically relevant quantum computers arrive, is precisely the technical lens organizations need to cut through the compliance patchwork described above and distinguish genuinely urgent migration targets from lower-priority ones.

For organizations still building the program-management scaffolding around migration, CSA's earlier Practical Preparations for the Post-Quantum World (2021) remains the more comprehensive operational reference, laying out a five-phase implementation framework covering awareness building, project formation, data-protection inventory, risk analysis, and execution — the same sequence of work the ANSSI and OMB M-26-15 deadlines now compress into a hard timeline rather than a discretionary roadmap. Because the compliance obligations discussed in this note extend beyond pure cryptography into procurement, vendor management, and governance accountability, organizations should also anchor

their migration program to CSA's AI Controls Matrix (AICM) v1.1, CSA's current unified controls framework, to ensure post-quantum migration tracking is integrated into existing governance, risk, and compliance reporting rather than run as a parallel, disconnected initiative.

References

[1] Bruce Schneier. "France to Stop Certifying Non-Quantum-Safe Encryption." Schneier on Security, July 2026.

[2] The White House. "Securing the Nation Against Advanced Cryptographic Attacks." Executive Order 14412, June 22, 2026.

[3] AWS Security Blog. "The CISO's Guide to Post-Quantum Mandates and Migrations." Amazon Web Services, 2026.

[4] Forrester. "Quantum Negligence: On the Clock — The US Just Set the Egg Timer on Quantum Migration as an Enterprise Risk." Forrester Blogs, 2026.

[5] NIST. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, August 2024.

[6] Office of Management and Budget. "Execution of the Migration to Post-Quantum Cryptography (M-26-15)." Executive Office of the President, June 24, 2026.

[7] European Commission. "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography." Shaping Europe's Digital Future, 2025.

[8] National Security Agency. "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems (CNSA 2.0)." National Security Agency, September 2022.

[9] Cloud Security Alliance. "A Practitioner's Guide to Post-Quantum Cryptography." Quantum-Safe Security Working Group, 2025.

