ISSUE 6

THIS WEEK IN QUANTUM CRYPTOGRAPHY

June 26, 2026

By
Joel Van Dyk
Quantum Security Advisor and Strategist

One thing stood out this week.

The conversation around post-quantum cryptography is moving from planning into enforcement.

For the past year, much of the discussion has focused on standards, roadmaps, and awareness. This week felt different. The United States issued a new executive order. Europe continued building its coordinated transition roadmap. France sent a clear certification signal. Singapore clarified its national position on quantum-safe migration. The UAE is already building sovereign cryptographic discovery capability.

The common thread is becoming hard to miss:

Post-quantum migration is no longer just a technical upgrade.

It is becoming policy, procurement, compliance, and national infrastructure.

What's Trending

1 The U.S. Has Put a Federal Clock on PQC Migration

On June 22, the White House published Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks. The order explicitly recognises harvest now, decrypt later risk and directs the transition of federal information systems to NIST-approved post-quantum cryptography standards.

Cloudflare's analysis points to a 2030 deadline for federal agencies to transition their most sensitive systems to post-quantum encryption, with post-quantum authentication following in 2031. The order also brings federal contractors more directly into scope.

Once federal agencies and contractors have deadlines, vendors, cloud providers, software companies, and critical infrastructure operators have to respond.

2 Europe Is Turning PQC Into a Coordinated Transition

The European Commission and the NIS Cooperation Group have set out a coordinated implementation roadmap for the transition to post-quantum cryptography. EU Member States should begin transitioning to PQC by the end of 2026, with critical infrastructure expected to transition as soon as possible and no later than 2030.

PQC is becoming part of the broader European cybersecurity and resilience stack, sitting alongside NIS2, DORA, critical infrastructure protection, digital sovereignty, and financial-sector operational resilience.

Europe is not waiting for a single dramatic quantum breakthrough. It is building the regulatory and resilience framework before the threat fully materialises.

3 France Is Turning Quantum-Safe Encryption Into a Certification Issue

ANSSI has indicated that, beginning in 2027, it will stop certifying security products that do not include quantum-safe encryption.

This moves post-quantum cryptography out of the realm of advisory guidance and into product trust, compliance, and procurement. Vendors selling into sensitive environments will need to demonstrate quantum-safe capability, not simply talk about it.

France is effectively saying: if you want trust, you need a migration path.

4 Singapore Is Taking a Risk-Oriented, Practical Approach

The Cyber Security Agency of Singapore has stated that post-quantum cryptography is expected to be the mainstream solution for quantum-safe migration. Singapore is taking NIST standards as a baseline while treating quantum key distribution as complementary and more appropriate for niche, high-assurance use cases.

The CSA has released a Quantum-Safe Handbook and Quantum Readiness Index to help organisations, particularly Critical Information Infrastructure owners and government agencies, assess readiness, prioritise actions, and begin executive-level conversations.

Singapore's message is clear: readiness starts with awareness, but it has to move quickly into assessment, planning, and capability building.

5 The UAE Is Moving From Policy to National Crypto Discovery

I did not find a Dubai-specific announcement this week, but the UAE signal is strong.

The UAE Cyber Security Council has partnered with QuantumGate to launch a national Crypto Discovery Tool, built in Abu Dhabi and customised to requirements set by the UAE National Cryptography Center.

Discovery is the hardest first step in PQC migration. You cannot migrate cryptography you cannot see. The UAE tool is designed to give organisations visibility into cryptographic assets, support inventory management, enable continuous monitoring, and feed into a national PQC readiness view.

6 The Market Is Converging Around Crypto-Agility

Across all of these developments, the same theme keeps appearing: cryptographic agility.

The ability to change cryptography safely, repeatedly, and without rebuilding entire systems from scratch may become one of the defining security capabilities of the next decade.

The technical standards matter. But the operational capability may matter more.

Why It Matters

A year ago, many organisations were still asking whether quantum risk was real enough to plan around.

That question is fading.

The better question now is: Can institutions move fast enough to understand their cryptographic exposure before deadlines, regulators, and procurement requirements force the issue?

The U.S. is now using executive authority. Europe is building a coordinated transition roadmap. France is using certification. Singapore is using readiness frameworks and practical guidance. The UAE is building national discovery infrastructure.

Different approaches. Same direction.

The transition to post-quantum cryptography is becoming real through policy, procurement, and operational controls.

The organisations that move early will not simply be better protected.

They will be easier to regulate, easier to audit, easier to insure, and easier to trust.

That is where this is heading.

ONE NUMBER TO WATCH

2030

Europe expects critical infrastructure to transition as soon as possible and no later than 2030. Cloudflare's reading of the new U.S. executive order points to a 2030 deadline for the most sensitive federal systems. Different jurisdictions, same practical horizon.

What I'm Reading

- **White House: Executive Order 14412 - Securing the Nation Against Advanced Cryptographic Attacks**
  https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
- **Cloudflare: The White House's Post-Quantum Executive Order Is an Important Milestone**
  https://blog.cloudflare.com/post-quantum-eo-2026/
- **European Commission: Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography**
  https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- **European Commission: EU Reinforces Its Cybersecurity with Post-Quantum Cryptography**
  https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography
- **ENISA: Post-Quantum Cryptography - Current State and Quantum Mitigation**
  https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
- **Europol: Urgent Plan Needed to Transition to Post-Quantum Cryptography Together**
  https://www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together
- **Reuters: France to Stop Certifying Products Without Quantum-Safe Encryption**
  https://www.reuters.com/legal/litigation/france-stop-certifying-products-without-quantum-safe-encryption-2026-06-16/
- **Cyber Security Agency of Singapore: Quantum-Safe Handbook and Quantum Readiness Index**
  https://www.csa.gov.sg/news-events/press-releases/csa-releases-a-quantum-safe-handbook-and-quantum-readiness-index/
- **Cyber Security Agency of Singapore: Committee of Supply 2026 Speech on Quantum-Safe Migration**
  https://www.csa.gov.sg/news-events/speeches/senior-minister-of-state-tan-kiat-how-committee-of-supply-2026-speech/

- **Abu Dhabi Media Office: UAE Cybersecurity Council Partners with QuantumGate to Launch Crypto Discovery Tool**
https://www.mediaoffice.abudhabi/en/security/uae-cybersecurity-council-partners-with-quantumgate-to-launch-crypto-discovery-tool/
- **NIST NCCoE: Migration to Post-Quantum Cryptography**
https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc
- **GSA: 2026 Post-Quantum Cryptography Summit**
https://www.gsa.gov/events/2026-postquantum-cryptography-summit-in-person-91626

- Joel Van Dyk