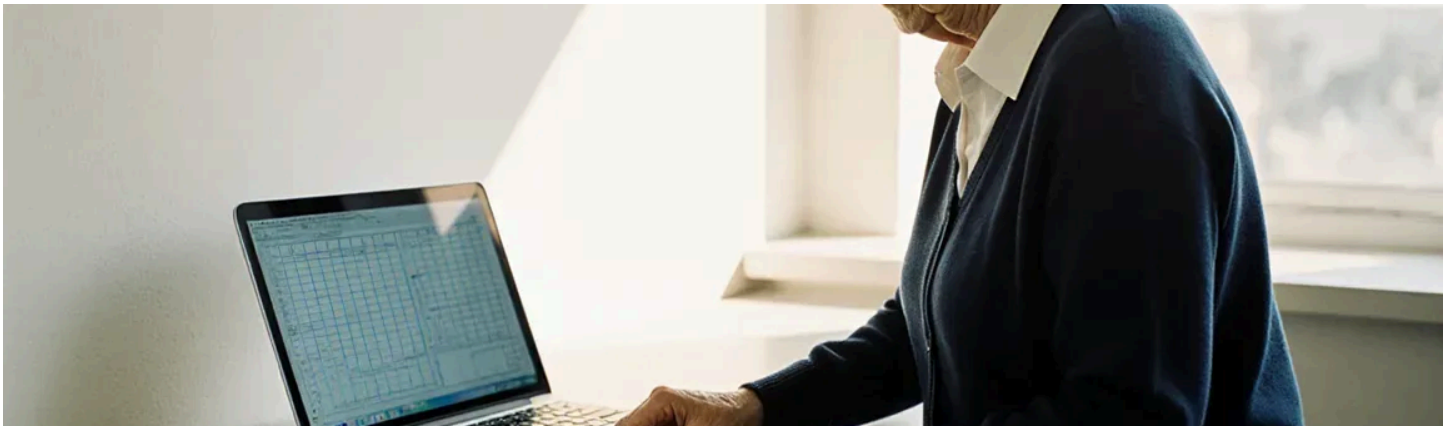


Post Quantum Starts With an Inventory You Do Not Have

Every post quantum cryptography plan starts with one question: where do we use cryptography today? Most organizations, federal agencies included, cannot yet answer it.

Dave Hoon
Chief Technology Officer, Norseman Defense Technologies · October 2026

Every post quantum cryptography plan starts with one question: where do we use cryptography today? Most organizations, federal agencies included, cannot yet answer it.

In 2026 that question gained deadlines. The fastest way to fall behind is to treat post quantum as an algorithm problem when it is first a cryptographic inventory problem.

What Changed in 2026

Federal deadlines became firm. On June 22, 2026, the President signed Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks." It requires agencies to move high value assets and high impact systems to post quantum cryptography for key establishment by December 31, 2030, and for digital signatures by December 31, 2031. Each agency had to name a migration lead within 30 days.

OMB set the playbook. Two days later, OMB issued Memorandum M-26-15, "Execution of the Migration to Post-Quantum Cryptography." It lays out a five phase schedule running from 2026 to 2035, starting with inventory and governance. It also required each civilian agency to submit a migration plan within 120 days, which meant by October 22, 2026.

Defense moved in parallel. The Department of War (DoW) released a post quantum cryptography strategy in June 2026. Published summaries say it requires DoW systems to support post quantum cryptography by the end of 2030, and it

signals that requirements will extend to the defense industrial base. For National Security Systems, the NSA's CNSA 2.0 suite requires new acquisitions to be compliant starting January 1, 2027.

GAO measured the gap. On October 6, 2026, GAO released GAO-27-108740, "Quantum Computing: Federal Actions Needed to Prepare for Emerging Cyber Threat." None of the 24 Chief Financial Officers Act agencies had fully addressed three key practices: a prioritized inventory of systems that use vulnerable cryptography, a funding estimate for replacing it, and testing of quantum resistant algorithms. Eighteen agencies reported lacking cryptography expertise. GAO's report also states that only "five agencies used automated tools to identify and verify data in their inventories," which leaves 19 of the 24 without them. The underlying audit work ran through September 2025, so agencies may have made progress since then. Even so, it shows how hard the first step is.

The standards are ready. NIST published FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) in August 2024. The algorithms are no longer the obstacle. Finding every place they need to go is.

Why This Matters Now: Harvest Now, Decrypt Later

An adversary does not need a quantum computer today to cause damage later. Encrypted traffic and files captured now can be stored and decrypted once a capable machine exists. If your data must stay confidential for ten years or more (personnel records, health data, financial records, intellectual property, mission data), it is already at risk.

A Practical Framework: The Five Layer Crypto Inventory

Use this as a checklist. Each layer has different owners and different tools.

1. **Network and protocols.** VPNs, TLS endpoints, load balancers, SSH and wireless. Record versions and key exchange methods. OMB's guidance points to TLS 1.3 as the base for post quantum deployment at the network level.
2. **Certificates and PKI.** Every certificate authority, certificate, expiry date and signing algorithm. PKI is often the longest pole, because signatures carry the 2031 deadline and certificates are everywhere.
3. **Keys and hardware.** Hardware security modules, key management systems, smart cards and tokens. Check firmware support for the new algorithms.
4. **Applications and code.** Cryptographic libraries in custom and commercial software, found through software composition analysis and code scanning.
5. **Suppliers and services.** Cloud, SaaS and managed services. Ask vendors for their post quantum roadmaps and, as they become available, cryptographic bills of materials.

Then rank systems on two scores, data lifetime and difficulty to change, and migrate the long lived, hard to change systems first.

The Cost of Doing Nothing

- **Exposure grows silently.** Every month without a plan is another month of traffic that could be harvested.
- **Deadlines compress.** Discovery, funding, testing and rollout across a large enterprise take years. Starting in 2028 leaves little room before 2030.

- **Procurement locks in the past.** Buying equipment now that cannot support post quantum algorithms creates a second replacement cycle later.
- **Talent gets scarce.** GAO's finding on expertise suggests that demand for cryptography skills will outpace supply as the deadlines approach.

A simple way to frame it: (volume of long lived sensitive data in transit or storage) multiplied by (years it must stay secret), set against the cost of a planned migration compared with an emergency one.

How Norseman Helps

Norseman has protected systems for the Department of War, the Intelligence Community and federal civilian agencies since 1992, where the adversary is often a nation state with time and resources. We bring that same discipline to banks, health systems and other commercial organizations with long lived data.

- **Assess:** We combine discovery tools and interviews across all five layers, with vendor neutral tool selection from more than 300 technology vendors.
- **Integrate and test:** We test hybrid and post quantum configurations in our 13,000 square foot integration lab, on your own hardware and software, before anything reaches production.
- **Respond:** We deliver a phased, funded plan that sets out the cost of waiting.
- **Support:** We keep the inventory current as vendors ship updates.

Book a Post Quantum Inventory Workshop

You cannot migrate what you cannot see. In a focused engagement, our engineers will build your first cryptographic inventory, rank your highest risk systems and outline a plan you can fund.

Start my inventory

Frequently Asked Questions

What are the federal post quantum deadlines?

Executive Order 14412 requires agencies to move high value assets and high impact systems to post quantum key establishment by December 31, 2030, and to post quantum digital signatures by December 31, 2031. OMB M-26-15 sets a phased schedule through 2035. For National Security Systems, CNSA 2.0 requires new acquisitions to be compliant starting January 1, 2027.

What is a cryptographic inventory?

A record of where an organization uses cryptography: which algorithms, keys, certificates, libraries and vendors, on which systems, protecting which data. It is the first required step in every federal post quantum plan.

What is harvest now, decrypt later?

An attack in which adversaries collect encrypted data today and store it until a quantum computer can decrypt it. It makes post quantum migration urgent for any data that must stay secret for many years.

Related

- **Post Quantum Readiness: Cryptographic Inventory and Migration Plan**
- **Cyber Resilience and Zero Trust**
- **How we work**
- **Executive Briefing Center and integration lab**
- **Support**

Sources

- Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," June 22, 2026, 91 FR 38483
- OMB Memorandum M-26-15, "Execution of the Migration to Post-Quantum Cryptography," June 24, 2026
- **HSToday, "OMB Issues Federal Roadmap for Post-Quantum Cryptography Migration," June 29, 2026**
- GAO-27-108740, "Quantum Computing: Federal Actions Needed to Prepare for Emerging Cyber Threat," October 6, 2026
- **FedScoop, "Work needed to fortify systems against quantum threats, watchdog says," October 7, 2026**
- **eWeek, "GAO Finds Post-Quantum Security Gaps Across 24 Federal Agencies," October 12, 2026**
- NSA, CNSA 2.0 FAQ and CSA
- NIST, FIPS 203, 204 and 205, August 2024 (csrc.nist.gov)

Published at norseman.com/insights/cryptographic-inventory-post-quantum-cryptography. To talk with Norseman Defense Technologies, call 410.579.8600 or email sales@norseman.com.