Post Quantum Readiness: Cryptographic Inventory and Migration Plan

A structured program that finds where and how your organization uses public key cryptography, ranks what to fix first, and builds a funded, testable plan to move to post quantum cryptography.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

A federal agency or contractor, or a regulated commercial enterprise such as a bank or health system, that holds long lived sensitive data and has no complete view of its cryptography.

Challenge

- Executive Order 14412 (June 22, 2026) requires federal 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.
- In October 2026, GAO reported that none of the 24 largest federal agencies had fully addressed three basic preparation practices: inventory, funding and testing.
- Cryptography is built into applications, network devices, certificates, firmware and third party services. Most organizations cannot say where it all is.
- Data stolen today can be stored and decrypted later, once a capable quantum computer exists. This is known as "harvest now, decrypt later."

Approach

- Combine automated discovery with interviews to inventory cryptography across networks, certificates, applications, code libraries and vendors.
- Rank systems by how long their data must stay secret and how hard they are to change.
- Assess the public key infrastructure (PKI), certificate lifecycles and hardware security modules for post quantum readiness.
- Check vendor roadmaps for support of NIST FIPS 203, 204 and 205.
- Test hybrid and post quantum configurations in the Norseman integration lab before production.
- Produce a phased, funded PQC migration plan aligned to OMB M-26-15 (federal) or to the organization's risk appetite (commercial).

Typical Outcomes

- A living cryptographic inventory, including a starting point for a cryptographic bill of materials
- A ranked list of systems to migrate first, with cost estimates
- Lab evidence of what works with your current hardware and software
- A plan built for crypto agility, so future algorithm changes are easier

Cost of Waiting

Migration takes years, while discovery and testing take months. Every month of delay adds to the amount of data an adversary may already be harvesting, and it shortens the runway to the 2030 and 2031 deadlines.

Procurement Paths

- GSA MAS for assessment and engineering services
- NASA SEWP VI (Category A) for security products, hardware security modules and network upgrades
- DoD ESI where eligible components apply
- **Commercial:** direct purchase and financing

Compare vehicles and ordering steps on **How to buy**.

Technology Categories

- Cryptographic discovery
- Certificate lifecycle management
- Hardware security modules and key management
- Network encryption
- Software composition analysis
- Asset inventory

Frequently Asked Questions

Do private companies have to meet the federal post quantum deadlines?

The federal deadlines bind agencies, and M-26-15 also points requirements toward federal suppliers. Commercial organizations face the same threat to long lived data and are increasingly following the same timeline.

Can we just wait for vendors to update products?

Vendor updates matter, but you still need to know where each product and library is used and in what order to update them. That is what the inventory provides.

What is crypto agility?

The ability to change algorithms without rebuilding systems. It is cheaper to design it in during migration than to add it later.

Book a Post Quantum Inventory Workshop

Find out where your cryptography lives and what to migrate first.

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.