

PQC Readiness Begins Before Algorithm Replacement

Federal agencies can reduce cryptographic risk today while preparing for the post-quantum transition.

FEDERAL POLICY MANDATE — JUNE 2026

Executive Order 14412

Establishes post-quantum cryptography as a government-wide cybersecurity priority. Directs agencies to designate PQC migration PQC migration leadership, inventory cryptographic assets, develop migration plans for high-value and high-impact systems, publish systems, publish federal CBOM guidance, and modernize acquisition requirements to accelerate adoption of quantum-resistant resistant cryptography.

Migration lead — 30 days

OMB guidance — 90 days

Key establishment — Dec 31, 2030

Digital signatures — Dec 31, 2031

CBOM guidance — 270 days

Builds on OMB M-23-02 (prioritized cryptographic inventories, harvest now decrypt later exposure) and National Security Memorandum 10 (federal migration direction).

Executive Order 14413

Establishes the next phase of the National Quantum Initiative by accelerating research, commercialization, workforce development, standards, and federal adoption of quantum technologies. Reinforces the need for agencies to prepare for quantum-enabled capabilities while aligning cybersecurity modernization with national quantum strategy.

THE FEDERAL CHALLENGE

Cryptography is everywhere. Visibility into it is not.

Cryptographic risk is distributed across applications, cloud services, identity systems, certificates and keys, software dependencies, network protocols, and vendor-managed products. Limited visibility makes prioritization difficult.

Applications

Cloud Services

Identity Systems

Certificates & Keys

Software Dependencies

Network Protocols

Vendor-Managed Products

THREE RISK PILLARS

Legacy Resiliency

Address weak algorithms, hashes, signatures, key exchange, protocols, and cryptographic dependencies that create risk today.

Harvest Now, Decrypt Later Risk

Prioritize publicly exposed systems and long-lived sensitive data that could be collected now and decrypted in the future.

Identity and Signature Resiliency

Prepare PKI, certificates, code signing, firmware validation, identity systems, and trust chains for post-quantum migration.

OPERATING MODEL

1

Visibility

Discover cryptographic assets

2

Context

Add mission, data, exposure, ownership

3

Prioritization

Focus resources on highest risk

4

Execution

Remediate, modernize, migrate

5

Governance

Track progress, sustain agility

WHAT AGENCIES CAN DO NOW

- Build a cryptographic inventory and CBOM.
- Identify weak and deprecated cryptography.
- Assess long-lived sensitive data and HNDL exposure.
- Review TLS, SSH, PKI, certificates, and key lifecycle practices.
- Engage vendors on PQC readiness and roadmaps.
- Align PQC work with Zero Trust, cloud modernization, acquisition, and DevSecOps.
- Establish ownership and continuous governance.

JOINT VALUE PROPOSITION

Wiz — Visibility and Context

Helps agencies identify cryptographic assets, configurations, exposure, cloud services, certificates, keys, and dependencies.

Accenture Federal Services — Federal Execution

Translates cryptographic findings into mission-aligned prioritization, systems integration, modernization planning, acquisition support, implementation, testing, and governance.

Wiz helps agencies understand cryptographic risk. Accenture Federal Services helps agencies operationalize that understanding at federal scale.

[FULL WHITEPAPER](#)

This one-page summary accompanies the full AFS and Wiz whitepaper, *From Visibility to Action: Operationalizing Cryptographic Risk for PQC Migration in Federal Systems*, which develops the policy basis, evidence, and detailed migration guidance in full.

AUTHOR
Raymond Beecham
Accenture Federal Services

TECHNICAL REVIEW & COLLABORATION
Bryan Rosensteel · Addi Grinbaum
Wiz

Accenture Federal Services

WIZ