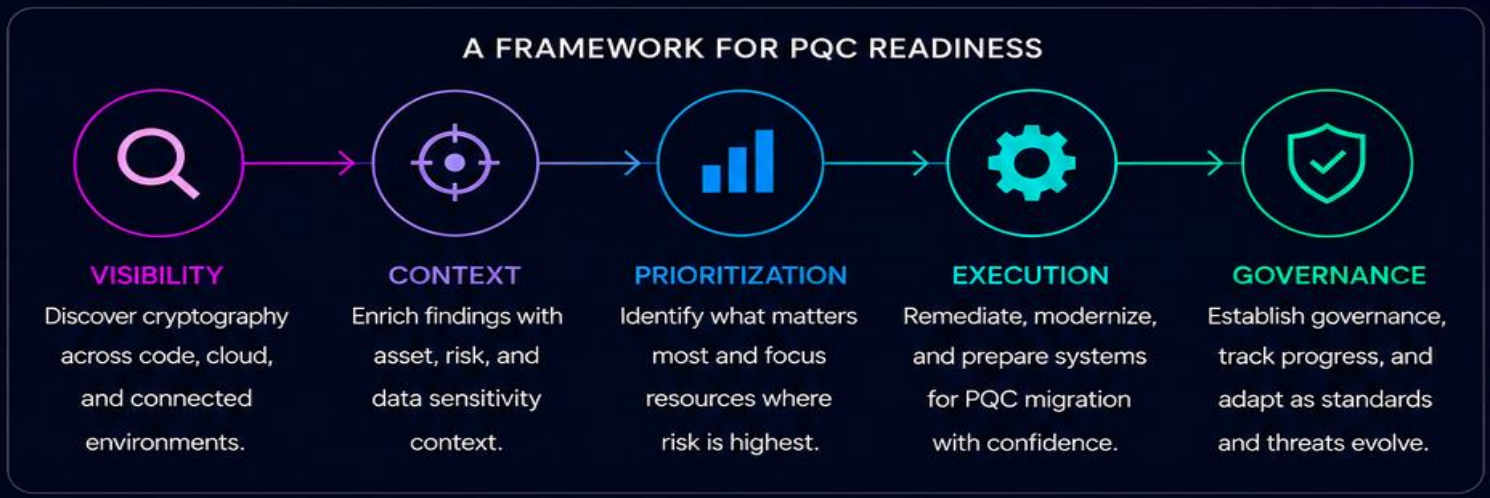
From Visibility to Action

Operationalizing Cryptographic Risk for PQC Migration in Federal Systems

Joint Accenture Federal Services (AFS) and Wiz Perspective

July 2026



Author

Raymond Beecham
Accenture Federal Services (AFS)

Technical Review and Collaboration

Bryan Rosensteel
Wiz

Addi Grinbaum
Wiz

Accenture Federal Services (AFS)

WIZ

Purpose and Intended Audience

Purpose

This joint Accenture Federal Services (AFS) and Wiz perspective presents a practical federal framework for reducing current cryptographic risk while preparing for post-quantum cryptography migration. It focuses on actions agencies can take now: establish cryptographic visibility, contextualize findings, prioritize mission risk, modernize trust systems, engage vendors, and build a phased path to execution.

Primary audience

- Federal chief information officers and chief information security officers.
- Program executives, mission owners, and modernization leaders.
- Chief architects, cloud leaders, and acquisition leadership.

Secondary audience

- Enterprise and solution architects.
- Cloud security, cybersecurity engineering, PKI, identity, and DevSecOps teams.
- Acquisition, vendor management, risk, and compliance stakeholders.

Intended use

The paper is designed to support executive decision-making, joint customer discussions, program planning, and potential external publication after partner, legal, marketing, and final leadership approvals.

Table of Contents

Executive Summary

Federal agencies do not need to wait for full post-quantum migration to begin reducing cryptographic risk. Classical weaknesses are addressable today, harvest now, decrypt later exposure can be reduced by prioritizing exposed systems and modern key establishment, and CBOM can provide the structure needed to make this work measurable and auditable. NIST sets the technical destination; the operational question is which systems agencies address first, on what evidence, and through which modernization path.

The federal policy environment changed materially in June 2026. Executive Order 14412 makes the transition of Federal information systems to NIST-approved PQC standards a national policy, requires agencies to identify CIO-aligned PQC migration leads, directs migration planning for high-value assets and high-impact systems, establishes 2030 and 2031 target dates for key establishment and digital signatures, and calls for federal CBOM guidance and acquisition rulemaking. These directives build on National Security Memorandum 10 and OMB M-23-02, which established the need for prioritized cryptographic inventories and highlighted harvest now, decrypt later exposure. [S22] [S1] [S2]

NIST has released the first principal PQC standards and states that organizations should begin migrating systems to quantum-resistant cryptography. FIPS 203 specifies ML-KEM for key establishment, FIPS 204 specifies ML-DSA for digital signatures, and FIPS 205 specifies SLH-DSA for digital signatures. Executive Order 14413 places this transition within a broader whole-of-government quantum strategy focused on research, commercialization, national security, and alignment of agency processes and programs. Standards are available, but operational readiness still requires discovery, systems integration, testing, sequencing, acquisition planning, and sustained governance. [S3] [S4] [S5] [S6] [S23]

The joint Accenture and Wiz approach is practical and complementary. Wiz strengthens cryptographic discovery, cloud context, and risk prioritization across connected environments. Accenture brings cybersecurity engineering, cloud and infrastructure transformation, enterprise architecture, systems integration, acquisition support, testing, modernization delivery, and federal mission experience. Together, the value is moving agencies from visibility to context to prioritized, enterprise-scale execution. [S15] [S17]

Federal Policy and Evidence Base

This paper is anchored in official and authoritative federal sources first, with Wiz and Accenture materials used to support implementation framing and partner positioning. It distinguishes between binding direction, federal guidance, technical standards, implementation references, and partner capabilities.

Source area	Use in the paper
Executive Order 14412	Migration leadership, deadlines, CBOM, procurement
Executive Order 14413	National quantum strategy and ecosystem alignment
OMB M-23-02	Inventory, governance, HNDL
NSM-10	Federal migration direction
NIST FIPS 203, 204, 205	PQC standards reference
CISA, NSA, NIST factsheet	Roadmap, inventory, HNDL, vendors
NIST NCCoE PQC Migration	Discovery, risk management, interoperability
NIST SP 800-131A Rev. 2	Classical crypto weaknesses
NIST SP 800-52 Rev. 2	TLS modernization
NIST SP 1800-37	TLS 1.3 visibility
NIST CSWP 39	Cryptographic agility
NSA CNSA 2.0	High-assurance reference for NSS

Source area	Use in the paper
GSA PQC Buyer's Guide	Acquisition and vendor engagement
CycloneDX CBOM	CBOM structure
Wiz public materials	Visibility, context, and prioritization
Accenture public materials	Federal integration and execution framing

NIST NCCoE describes its Migration to PQC project as focused on cryptographic visibility and risk management, which supports building and maintaining a comprehensive cryptographic inventory, and interoperability and benchmarking, which supports providers embedding PQC algorithms into products and services. [S8] [S9]

1. Why PQC Readiness Must Start Before Migration

PQC readiness should not begin with a broad mandate to replace every algorithm across the enterprise at once. For federal agencies, the more practical starting point is to understand where cryptography exists, what it protects, how long the protected data must remain confidential, and which systems are exposed to current or future cryptographic risks.

2026 Executive Orders accelerate the federal mandate

Executive Order 14412 converts PQC readiness from a long-range planning objective into a time-bound federal execution requirement. It establishes agency ownership, directs OMB guidance for high-value assets and high-impact systems, sets transition targets, requires a federal view of minimum CBOM elements, and initiates acquisition rulemaking. Executive Order 14413 complements this security mandate by directing an updated National Quantum Strategy and agency alignment with a broader national quantum innovation agenda. [S22] [S23]

EO 14412 directive	Operational implication for agencies
Name a PQC migration lead within 30 days	Establish CIO-aligned ownership and cross-agency coordination
OMB guidance within 90 days	Validate HVA and high-impact inventories and submit migration plans
PQC key establishment by December 31, 2030	Prioritize transport, session establishment, and exposed mission systems
PQC digital signatures by December 31, 2031	Plan PKI, signing, identity, software, and firmware trust transitions
Federal CBOM guidance within 270 days	Align inventory design with forthcoming minimum automated-assessment elements
FAR rulemaking within 180 and 270 days	Build PQC and cryptographic vulnerability expectations into acquisition

OMB M-23-02 establishes a concrete federal requirement for this work. It directs agencies to conduct prioritized inventories of cryptographic systems, beginning with high-value assets, high-impact systems, systems likely to be vulnerable to quantum attacks, systems containing data expected to remain mission-sensitive in 2035, and logical access control systems based on asymmetric encryption. [S1]

The urgency is not limited to a future quantum event. Harvest now, decrypt later exposure means that encrypted data can be collected today and decrypted later when a cryptanalytically relevant quantum computer becomes available. The joint CISA, NSA, and NIST quantum-readiness factsheet states that successful PQC migration will take time and urges organizations to begin preparing now through roadmaps, inventories, risk assessments, analysis, and vendor engagement. [S7]

NIST's finalized PQC standards make migration planning more concrete, but the availability of standards does not create operational readiness by itself. Agencies still need discovery, inventory, risk context, testing, sequencing, acquisition planning, and vendor engagement. The NIST NCCoE Migration to PQC project reinforces this point by emphasizing cryptographic inventory and interoperability as core workstreams for migration. [S8] [S9]

The near-term objective should be defensible prioritization. Agencies should identify where classical weaknesses can be remediated today, where harvest now, decrypt later exposure creates urgency, where vendor dependencies constrain migration, and where modernization windows create opportunities to embed cryptographic agility.

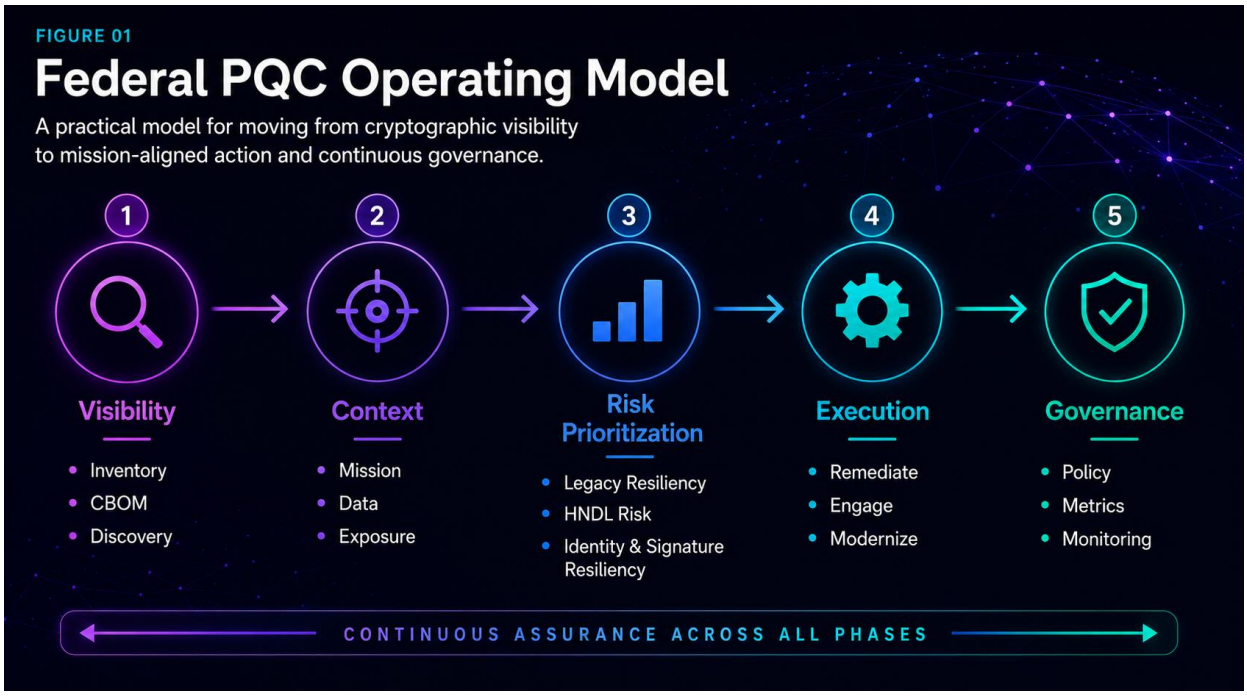


Figure 1. A staged model for moving from cryptographic visibility to mission-aligned action and continuous governance.

2. The Federal Cryptographic Visibility Problem

Federal cryptography is not confined to a single product, system, or architecture layer. It is distributed across applications, infrastructure, identity systems, APIs, certificates, keys, SaaS platforms, cloud-managed services, PKI, remote access, DevSecOps pipelines, software libraries, firmware, and vendor-managed products.

OMB's inventory requirements reflect this complexity. Agencies are expected to capture information such as the algorithm used, the cryptographic service provided, key length, product or software package information, vendor or developer, hosting model, cloud provider, and data lifecycle attributes. This shows that PQC readiness is not simply a standards mapping exercise. It requires asset, data, mission, vendor, and operational context. [S1]

The joint CISA, NSA, and NIST factsheet states that organizations are often unaware of the breadth of application and functional dependencies on public-key cryptography within deployed products, applications, and services. It recommends proactive cryptographic discovery across network protocols, endpoints, servers, applications, libraries, firmware and software updates, and CI/CD dependencies. [S7]

For federal agencies, this visibility problem is compounded by cloud and vendor-managed cryptography. Agencies may not directly control every certificate, key, protocol configuration, cryptographic library, or

managed service in their environment. A practical inventory therefore needs to include agency-managed assets, cloud-managed services, vendor-provided products, COTS software, custom code, and mission systems that rely on third-party integrations.

The central challenge is not only finding cryptography. It is finding cryptography with enough operational context to determine risk. A certificate, library, protocol, or key exchange mechanism becomes actionable only when it is connected to an asset, system owner, data type, exposure path, mission function, vendor dependency, and modernization path.

3. CBOM and Cryptographic Asset Inventory

A CBOM gives agencies a structured way to represent cryptographic assets and dependencies. For this paper, CBOM means Cryptographic Bill of Materials. CBOM can help agencies document algorithms, keys, certificates, protocols, libraries, cryptographic services, and relationships to software or cloud components.

CycloneDX describes CBOM as a way to provide transparency into cryptographic assets such as algorithms, keys, and certificates, assess resilience against deprecated algorithms and quantum threats, enable proactive management of cryptographic assets and policies, and align with post-quantum cryptography standards. [S14]

For federal agencies, CBOM should be treated as part of a broader cryptographic asset inventory. This distinction is important. A CBOM can structure cryptographic transparency, but it should not be treated as the entire readiness program. Agencies need a broader inventory and operating model that connects cryptographic assets to mission systems, data sensitivity, exposure, ownership, vendors, cloud services, modernization status, and remediation decisions. This broader view is particularly important in cloud environments where cryptographic assets, services, and dependencies may span multiple operational layers.

Executive Order 14412 raises CBOM from a useful transparency practice to an emerging federal policy requirement. It directs CISA, in coordination with NIST, to release public guidance describing minimum CBOM elements that enable automated assessment of cryptographic assets used by hardware or software. Agencies should design inventories that can evolve toward those federal minimum elements without delaying discovery work already underway. [S22]

Wiz helps agencies extend cryptographic inventory across cloud-managed services, workloads, certificates, keys, and runtime context. By connecting cryptographic metadata to exposure paths, identity relationships, sensitive data, ownership, and service dependencies, Wiz can help turn CBOM and broader inventory outputs into prioritized security decisions. [S15] [S16]

Recommended framing
CBOM can provide structure for cryptographic transparency, but agencies still need context, prioritization, and execution.

This helps avoid treating CBOM as a checklist artifact. CBOM is most valuable when it becomes an input to risk analysis, vendor engagement, acquisition planning, modernization sequencing, and governance.

4. From Inventory to Prioritization

A CBOM tells an agency where cryptography exists. It does not, on its own, tell the agency what to fix first. The next step is to layer mission, data, exposure, and feasibility context onto the inventory so that finite remediation capacity is spent on the systems that matter most.

NIST CSWP 39 defines cryptographic agility as the capabilities needed to replace and adapt cryptographic algorithms in protocols, applications, software, hardware, firmware, and infrastructure while preserving security and ongoing operations. This matters because PQC readiness is not only a discovery problem. It is an operational change problem that spans architecture, policy, vendor engagement, modernization, and governance. [S13]

A high-value cryptographic inventory must connect technical findings to operational context. Agencies need to know whether an issue affects a mission-critical system, protects sensitive data, creates public exposure, supports identity or trust, depends on a vendor roadmap, or aligns with an upcoming modernization effort.

The prioritization question should be practical:

- Which systems are exposed?
- Which systems protect long-lived sensitive data?
- Which cryptographic weaknesses are exploitable by traditional computers today?
- Which assets are internet-facing?
- Which assets have access to mission or citizen data?
- Which systems rely on vendor-managed cryptography?
- Which systems are already scheduled for modernization?
- Which systems can adapt cryptography without major redesign?

This is where environment context becomes critical. A weak cryptographic configuration is more urgent when it is tied to an internet-facing service, sensitive data access, mission-critical function, or known attack path. A PQC-relevant dependency may be less urgent if it is isolated, vendor-managed, and already scheduled for modernization. The goal is not to treat every cryptographic finding equally. The goal is defensible prioritization.

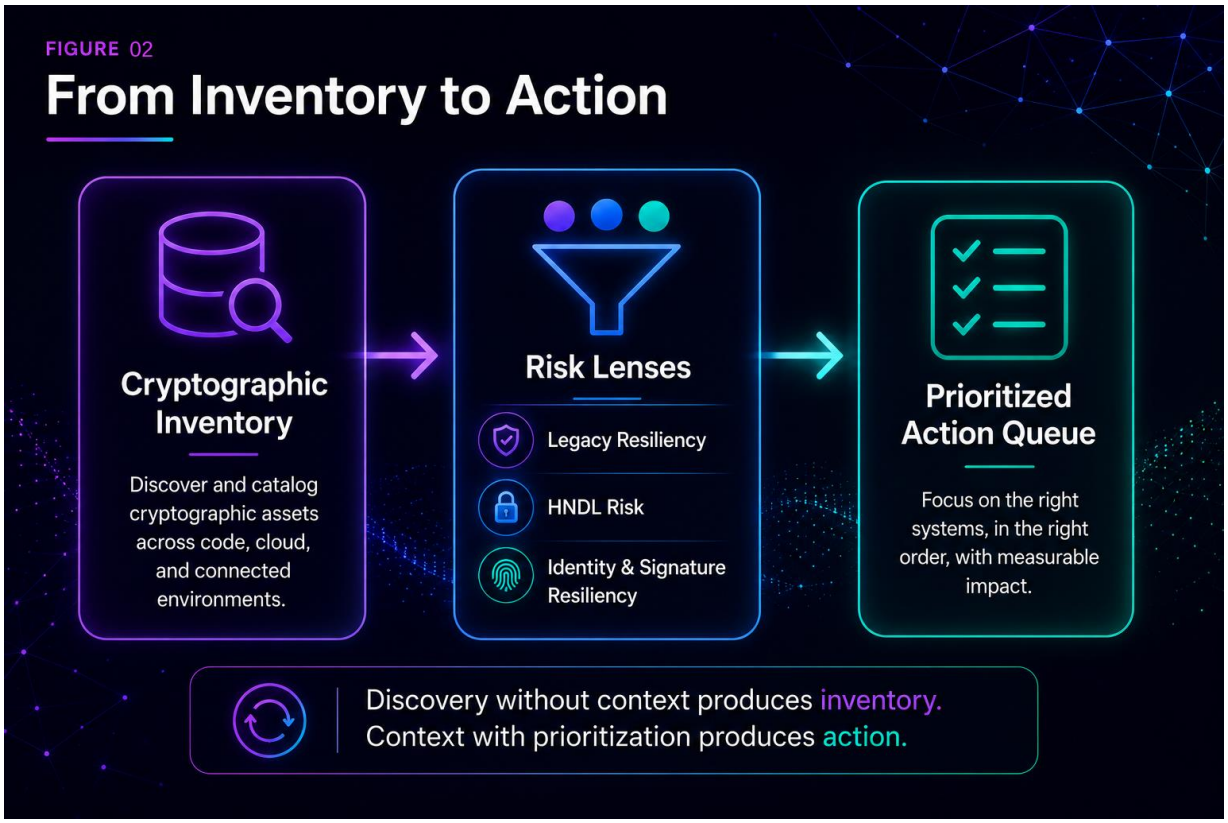


Figure 2. Cryptographic inventory becomes actionable when contextualized through risk-based prioritization.

5. Acting Today: Legacy Resiliency and HNDL Risk

Federal agencies can reduce cryptographic risk before full PQC migration by identifying and remediating weaknesses that matter today. While enterprise-wide migration may take years, agencies can begin improving security immediately by addressing known cryptographic weaknesses, reducing technical debt, and preparing systems for future transition.

Near-term discovery should include:

- Weak encryption algorithms.
- Weak hash functions.
- Weak key exchange.
- Weak signatures.
- Deprecated TLS or protocol configurations.
- Downgrade or fallback exposure.
- Poor certificate lifecycle management.
- Exposed private keys or unmanaged secrets.
- Vendor-managed cryptography.
- Long-lived sensitive data.
- Lack of cryptographic agility.

NIST SP 800-131A Rev. 2 provides direct support for classical cryptographic hygiene. It provides guidance for transitioning to stronger cryptographic keys and more robust algorithms, and NIST explains that these transitions address new cryptanalysis, increasing classical computing power, and the potential emergence of quantum computers. [S10]

Specific legacy-debt examples should include SHA-1, TDEA, weak key lengths, weak signatures, and deprecated key exchange mechanisms. NIST formally deprecated SHA-1 for new digital signatures in 2011 and disallowed its use for creating and verifying digital signatures in 2013. Practical collision attacks against SHA-1 were publicly demonstrated in 2017, reinforcing the need to transition to stronger alternatives. NIST has since announced that all remaining SHA-1 usage should be phased out by December 31, 2030, and recommends that organizations relying on SHA-1 for security migrate to SHA-2 or SHA-3 as soon as possible. [S20]

TLS modernization should also be treated as both a current security action and a PQC readiness enabler. NIST SP 800-52 Rev. 2 requires that TLS 1.2 configured with FIPS-based cipher suites be supported by government TLS servers and clients and requires support for TLS 1.3 by January 1, 2024. [S11]

Harvest Now, Decrypt Later (HNDL) risk should be assessed by asking whether encrypted traffic or stored encrypted data captured today would remain sensitive in the future. OMB M-23-02 points to data that, if recorded now and later decrypted by a cryptanalytically relevant quantum computer (CRQC) in 2035, would still be considered mission-sensitive. [S1]

Practical near-term message
In 2026, the most defensible agency action is not to wait for every PQC capability to mature. It is to build a cryptographic inventory, identify current classical weaknesses, prioritize harvest now, decrypt later exposure, and sequence remediation into modernization and acquisition activity.

Figure 3. Three risk pillars for organizing cryptographic risk reduction and PQC readiness activities.

6. Strengthened Risk Pillars: Legacy Resiliency, HNDL Risk, and Identity and Signature Resiliency

Federal agencies should not treat cryptographic risk as a single category. A more practical approach is to group findings into three risk pillars:

1. Legacy Resiliency
2. Harvest Now, Decrypt Later (HNDL) Risk
3. Identity and Signature Resiliency

This framing aligns with Wiz input and helps turn a broad inventory into a usable action model.

6.1 Legacy Resiliency

Legacy debt includes deprecated algorithms, weak hashes, weak signatures, weak key exchange mechanisms, outdated protocol configurations, and cryptographic libraries that no longer meet current security expectations. These findings represent immediate risk because they may be exploitable by threat actors using classical computing methods available today, independent of future cryptanalytically relevant quantum computer (CRQC) capabilities.

For that reason, legacy debt should generally be prioritized first within a cryptographic risk reduction program. Addressing known weaknesses can improve current security posture, reduce technical debt, and establish a stronger foundation for future PQC migration activities.

Examples include:

- SHA-1 used for security-sensitive applications.

- SHA-1 used for digital signature generation.
- Weak encryption algorithms.
- TDEA dependencies that should be retired or governed.
- Weak key lengths.
- Weak SSH key exchange.
- Deprecated TLS versions.
- Weak signatures.
- Unsupported or outdated cryptographic libraries.
- Misconfigured certificate or key practices.
- Hard-coded keys or unmanaged secrets.

This pillar gives agencies a way to show near-term value. Even before full PQC migration, agencies can improve cryptographic posture by reducing current weaknesses. NIST SP 800-131A Rev. 2 and NIST's SHA-1 retirement guidance provide the strongest anchors for this section. [S10] [S20]

6.2 HNDL Risk

Harvest now, decrypt later (HNDL) risk should be considered a near-term priority for organizations that must protect sensitive data beyond the current planning horizon for quantum risk. Systems protecting long-lived sensitive information may require earlier assessment and mitigation because encrypted data collected today could remain valuable long enough to be targeted by future quantum-enabled decryption capabilities.

Because the timeline for cryptanalytically relevant quantum computer (CRQC) remains uncertain, organizations should prioritize planning based on data confidentiality requirements, exposure, and mission impact rather than a specific projected date.

Scenario	Why it matters
Citizen data with long-term privacy impact	Data may remain sensitive for years
Investigative or case records	Disclosure may harm operations or individuals
Health or benefits data	Privacy and mission impact can persist
Mission telemetry	May reveal operational patterns
Interagency data exchanges	Cross-boundary exposure increases risk
Identity or credential traffic	Trust compromise can cascade
National security adjacent data	Higher sensitivity and longer secrecy needs

A practical HNDL priority would include assets that are:

- Publicly exposed.
- Protecting sensitive or long-lived data.
- Limited to weaker protocol posture.
- Missing modern or hybrid PQC key exchange options.
- Reachable through cloud or identity relationships.
- Tied to mission-critical processes.
- Difficult to modernize quickly.

The joint CISA, NSA, and NIST factsheet explicitly recommends that organizations consider harvest now, decrypt later (HNDL) risk when developing quantum-readiness roadmaps. [S7]

6.3 Identity and Signature Resiliency

The Identity and Signature Resiliency pillar extends beyond encryption. While encryption protects confidentiality, digital signatures and identity systems protect authenticity, integrity, and non-repudiation. PQC therefore affects not only encrypted connections, but also the mechanisms agencies use to establish trust, validate software and firmware, authenticate users and devices, and verify information has not been altered.

Unlike Legacy Debt, which may represent exploitable risk today, and HNDL risk, which can affect sensitive data currently being transmitted or stored, Identity and Signature Resiliency is generally a longer-term migration priority. However, it remains a critical component of PQC readiness because many trust systems rely on public-key cryptography that is expected to become vulnerable to future cryptanalytically relevant quantum computers (CRQCs).

If these trust mechanisms are not transitioned to quantum-resistant cryptography, future attackers could theoretically perform signature forgery attacks, impersonate trusted entities, undermine software and firmware validation processes, or compromise digital trust relationships that federal systems depend upon.

Identity and Signature Resiliency include:

- PKI.
- Certificate authorities.
- Intermediate and root trust chains.
- Certificate lifecycle management.
- Code signing.
- Firmware signing.
- Software update validation.
- Identity federation.
- Workload identity.
- API signing.
- Document signing.
- Machine identity.
- Key management and rotation.
- Revocation, renewal, and ownership processes.

This pillar matters because two of NIST's first three PQC standards are digital signature standards. FIPS 204 specifies ML-DSA, a post-quantum digital signature scheme used to generate and verify digital signatures. FIPS 205 specifies SLH-DSA, a stateless hash-based digital signature algorithm used to detect unauthorized modification and authenticate the signatory. [S5] [S6]

Agencies should assess trust workflows that depend on RSA, ECDSA, DSA, or other quantum-vulnerable public-key cryptographic mechanisms. This includes certificates, digital signatures, software signing, device identity, workload identity, and validation of software or firmware updates.

7. Certificate and Key Lifecycle Management

Certificate and key lifecycle management should be treated as a core part of the Identity and Signature Resiliency pillar. Weak certificate or key governance can undermine both current cryptographic security and future PQC migration.

Agencies should identify:

- Expired certificates.
- Long-lived certificates.
- Certificates using weak signature algorithms.
- Certificates tied to internet-facing services.
- Private keys stored in code, workloads, or unmanaged secrets.
- Hard-coded keys.
- Incomplete certificate ownership.
- Unclear certificate rotation processes.
- Weak revocation and renewal processes.
- Certificate authorities and intermediate trust chain dependencies.
- Certificates used for APIs, workload identity, code signing, firmware signing, and document signing.

NIST SP 800-52 Rev. 2 includes guidance on certificates and TLS extensions that affect security, reinforcing the importance of certificate posture within federal TLS and cryptographic readiness efforts. [S11]

Practical message

Agencies should not wait until PQC migration to clean up certificate and key lifecycle issues. Certificate lifecycle management is a near-term crypto hygiene priority and a prerequisite for trustworthy migration planning.

8. Code-to-Cloud Visibility Model

For each risk pillar, agencies should seek visibility across code, workloads, cloud services, and runtime or event context. This model helps agencies avoid a narrow inventory that only captures one layer of cryptographic exposure.

Layer	What to identify
Code	Crypto libraries and algorithm usage
Workloads	Keys, certificates, configs, runtime assets
Cloud services	Managed certificates, load balancers, APIs, identity services
Runtime and events	Observed protocol usage and configuration drift

Wiz extends cryptographic visibility across cloud and connected environments. Its PQC readiness capabilities surface cryptographic metadata, scan public-facing services for active protocols and weak SSH key exchange methods, inspect secrets and host configurations, and associate findings with cloud assets and services. [S15]

The value of this code-to-cloud model is context. Cryptographic risk is rarely determined by an algorithm alone; it depends on where the asset runs, what data it can access, how it is exposed, which identities can reach it, and whether remediation depends on a cloud or software provider. The Wiz Security Graph can connect these relationships so agencies can prioritize combinations of risk rather than isolated findings. [S15] [S16]

Recommended language

A code-to-cloud model helps agencies connect cryptographic findings to where they originate, where they run, how they are configured, and how they are exposed. This is essential for prioritization because risk is rarely determined by algorithms alone. Risk depends on the asset, data, exposure, identity relationships, vendor dependency, and mission function surrounding that cryptographic asset.

9. TLS Modernization, Downgrade Risk, and Visibility

TLS modernization should be part of the agency's near-term readiness work. NIST SP 800-52 Rev. 2 provides federal guidance for TLS implementation and requires TLS 1.2 configured with FIPS-based cipher suites for government TLS servers and clients, as well as support for TLS 1.3 by January 1, 2024. [S11]

Agencies should not treat "supports TLS 1.3" as the only question. A service may support TLS 1.3 but still allow negotiation to weaker configurations. Agencies should validate not only what is supported, but what can be negotiated by clients and what downgrade or fallback paths remain reachable.

TLS posture questions:

- Does the service support TLS 1.3?
- Does it still allow TLS 1.0 or TLS 1.1?
- Does it allow weak cipher suites?
- Does it allow weak key exchange?
- Does it rely on static key exchange?
- Can sessions be negotiated down to weaker configurations?
- Are certificates current and properly managed?
- Is the service publicly exposed?
- Does the service protect long-lived sensitive data?
- Does monitoring or inspection depend on older TLS visibility assumptions?

NIST SP 1800-37 adds an important nuance. TLS 1.3 provides forward secrecy, which protects prior TLS communications even if a TLS-enabled server is later compromised, but the mechanisms used to achieve forward secrecy may interfere with passive decryption techniques that enterprises used for TLS 1.2 traffic visibility. NIST SP 1800-37 provides practical approaches for gaining visibility into TLS 1.3-protected traffic within controlled enterprise data center environments. [S12]

The practical message is that TLS modernization is a readiness enabler, not a complete solution. Agencies should validate protocol posture, downgrade and fallback exposure, certificate lifecycle practices, monitoring impacts, and future PQC or hybrid key exchange support.

10. CNSA 2.0 as a High-Assurance Reference Point

CNSA 2.0 should be used carefully in this paper. It is directly relevant to National Security Systems and high-assurance environments, but it should not be presented as a blanket requirement for all civilian federal systems.

Recommended framing
CNSA 2.0 provides a useful high-assurance reference point for agencies operating National Security Systems, NSS-adjacent environments, or mission systems that must account for NSA cryptographic transition expectations.

NSA's CNSA 2.0 guidance includes transition timelines for categories such as software and firmware signing, web browsers and servers, cloud services, traditional networking equipment, operating systems, niche equipment, custom applications, and legacy equipment. NSA recommends software and firmware signing begin transitioning immediately, and it anticipates different target dates for support and exclusive use of CNSA 2.0 across categories such as cloud services, networking equipment, operating systems, and custom applications. [S19]

This source strengthens the Identity and Signature Resiliency pillar because NSA highlights software and firmware signing as an urgent use case. It also supports the need to evaluate certificates, signatures, firmware validation, software update integrity, and trust chains as part of cryptographic migration planning.

11. Practical Prioritization Model for Federal Agencies

This model helps agencies move from a long inventory to a defensible action plan.

Prioritization principle
The goal is not enterprise-wide replacement all at once. The goal is defensible prioritization.

11.1 Prioritization criteria

Criterion	What it tells the agency
Mission criticality	Whether the asset supports essential mission delivery
Data sensitivity	Whether protected data creates privacy, mission, legal, or national security risk
Confidentiality lifetime	Whether data must remain protected into the CRQC planning horizon
HNDL risk	Whether data or traffic could be captured today
Current crypto weakness	Whether the issue is exploitable by classical methods now
Public exposure	Whether the asset is internet-facing or externally reachable
Attack path	Whether compromise could lead to higher-value systems
Vendor dependency	Whether remediation depends on COTS, SaaS, or cloud providers
Modernization feasibility	Whether changes can be sequenced into planned upgrades
Cryptographic agility	Whether algorithms and libraries can be changed without major redesign

The GSA PQC Buyer's Guide also supports this type of prioritization. It recommends considering whether a system is a High Value Asset (HVA), what it protects, what other systems it communicates with, whether it communicates outside the agency, whether it shares data with other agencies or organizations, and whether it supports critical infrastructure. [S18]

11.2 Action buckets

Bucket	Use when
Assess now	Exposure or uncertainty is high
Remediate now	A classical weakness is confirmed
Plan migration	PQC impact is likely but dependent
Align to modernization	A planned upgrade can absorb the work
Govern and monitor	Risk is lower or vendor-controlled

11.3 Example prioritization logic

A public-facing service that uses weak key exchange, supports legacy protocols, and has access to sensitive data should be prioritized for immediate assessment and remediation. If that service also protects data with a long confidentiality lifetime, it should be evaluated for HNDL risk and future PQC key exchange planning.

A vendor-managed SaaS dependency with no confirmed classical weakness but a likely PQC dependency may not be technically remediable by the agency today. It should be moved into vendor engagement, roadmap tracking, acquisition language, and governance.

A low-impact internal system using acceptable classical cryptography but limited cryptographic agility may be governed and monitored until the next modernization window.

This approach gives agencies a defensible way to explain why some findings receive immediate action while others are sequenced into planning, acquisition, or modernization.

12. Vendor Engagement and Acquisition Language

Vendor engagement is a critical component of federal PQC execution. Agencies will not control every cryptographic implementation directly. Many cryptographic dependencies sit inside COTS products, SaaS platforms, cloud-managed services, identity providers, APIs, firmware, software updates, and managed service offerings.

The CISA, NSA, and NIST factsheet recommend vendor engagement as part of quantum-readiness roadmaps, while the GSA PQC Buyer's Guide encourages agencies to assess software security, review supplier practices, and identify evidence of conformance with secure encryption requirements. Executive Order 14412 adds a procurement imperative by directing proposed FAR rulemaking for covered contractors to comply with applicable NIST FIPS incorporating PQC by December 31, 2030, and to include cryptographic vulnerabilities in contractor vulnerability disclosure requirements. [S7] [S18] [S22]

12.1 Vendor Questions

Agencies should tailor vendor questions based on the role the vendor plays in PQC readiness.

PQC Readiness and Discovery Providers

Agencies may ask providers that support cryptographic discovery, inventory, visibility, assessment, or prioritization activities:

- What cryptographic assets, protocols, certificates, keys, libraries, and dependencies can be identified?
- Does the solution provide a CBOM or comparable cryptographic inventory?
- What visibility is available across code, workloads, cloud services, managed services, and runtime environments?
- How are cryptographic findings contextualized using exposure, identity relationships, data sensitivity, ownership, and mission impact?
- What telemetry, reporting, dashboards, or evidence can be provided to support agency inventory, governance, and readiness activities?
- How does the solution support prioritization of Legacy Resiliency, Harvest Now, Decrypt Later (HNDL) Risk, and Identity and Signature Resiliency activities?

Technology Providers and Service Vendors

Agencies may ask software vendors, cloud providers, managed service providers, PKI vendors, identity providers, network vendors, and other technology suppliers:

- What cryptography is embedded in the product or service?
- Which algorithms, protocols, certificates, key lengths, and libraries are used?
- Which components use RSA, DH, ECDH, ECDSA, DSA, or other quantum-vulnerable public-key mechanisms?
- Which NIST PQC standards will be supported?

- What is the vendor's PQC roadmap?
- What is the expected timeline for testing and production support?
- Will migration require customer action, service updates, firmware updates, certificate replacement, API changes, new product versions, or configuration changes?
- How will the vendor address TLS, SSH, IPsec, PKI, key management, code signing, firmware signing, identity federation, and workload identity?

12.2 Sample RFI and Vendor Engagement Language

Agencies should tailor vendor questions based on the role the vendor plays in PQC readiness. In practice, two categories are common: PQC readiness and discovery providers, and technology providers whose products or services must support post-quantum cryptography.

PQC Readiness and Discovery Providers

Agencies may ask providers that support cryptographic discovery, inventory, visibility, assessment, or prioritization activities:

- What cryptographic assets, protocols, certificates, keys, libraries, and dependencies can be identified?
- Does the solution provide cryptographic inventory, CBOM outputs, or comparable reporting?
- What visibility is available across code, workloads, cloud services, managed services, and runtime environments?
- How are cryptographic findings contextualized using factors such as exposure, identity relationships, data sensitivity, ownership, and mission impact?
- What reporting, evidence, dashboards, or governance outputs are available to support agency PQC readiness programs?
- How does the solution support prioritization of Legacy Resiliency, Harvest Now, Decrypt Later (HNDL) risk, and Identity and Signature Resiliency activities?

Technology Providers and Service Vendors

Agencies may ask software vendors, cloud providers, managed service providers, identity providers, PKI vendors, network vendors, and other technology suppliers:

- What cryptography is embedded in the product or service?
- Which algorithms, protocols, certificates, key lengths, libraries, and cryptographic services are used?
- Which components use RSA, DH, ECDH, ECDSA, DSA, or other quantum-vulnerable public-key mechanisms?
- What is the vendor's roadmap for supporting NIST-standardized PQC algorithms, including FIPS 203 ML-KEM, FIPS 204 ML-DSA, and FIPS 205 SLH-DSA, where applicable?
- Which PQC-relevant capabilities are currently supported, planned, or not planned for TLS, SSH, IPsec, PKI, key management, code signing, firmware signing, identity federation, API signing, and workload identity?
- Will migration require customer action, product updates, firmware updates, service-side changes, certificate replacement, API changes, configuration changes, or new product versions?
- What evidence can be provided to demonstrate cryptographic agility and support future algorithm transitions without unacceptable operational disruption?

This language should be viewed as a starting point for discussion and tailored to agency mission requirements, acquisition strategy, and vendor role.

13. What Agencies Can Do in 2026

Federal agencies can begin meaningful PQC readiness work now. The following actions are practical, near-term, and aligned with federal guidance.

13.1 Name and empower the PQC migration lead

Executive Order 14412 requires each agency head to identify a PQC migration lead who reports to the CIO and oversees cryptographic inventory management, prioritized migration planning, and cross-agency coordination. Agencies should use that role to establish decision rights across the CIO, CISO, enterprise architecture, cloud, identity, PKI, mission, acquisition, data, and modernization communities. [S22]

13.2 Review priority inventories and build the migration plan

Review high-value asset and high-impact system inventories, then identify internet-facing services, cloud-managed services, PKI and certificate services, identity and access systems, remote access, long-lived mission data, and vendor-managed dependencies. Use the results to build a plan for PQC key establishment by 2030 and digital signatures by 2031, while continuing to address classical weaknesses immediately. [S22] [S1]

13.3 Build a cryptographic inventory

Use existing sources first, then expand coverage. Potential data sources include asset inventory, CMDB, CDM data, cloud asset inventory, CNAPP or CSPM data, vulnerability management data, EDR telemetry, ICAM systems, certificate management systems, source code and dependency scanning, and network protocol scanning. [S7]

13.4 Use CBOM as a structuring mechanism

A CBOM should help structure cryptographic inventory, but it should be connected to ownership, mission, data, vendor, exposure, and modernization context. [S14]

13.5 Identify and remediate legacy debt

Agencies should identify weak encryption, weak hashes, weak key exchange, weak signatures, deprecated protocols, unsupported libraries, and certificate lifecycle issues. [S10] [S11]

13.6 Assess HNDL risk

Prioritize systems that combine public exposure, sensitive or long-lived data, mission impact, classical key exchange, weak TLS or SSH posture, vendor or cloud dependency, and difficult modernization path. [S1] [S7]

13.7 Assess Identity and Signature Resiliency

Agencies should identify trust systems that rely on quantum-vulnerable public-key cryptography and assess the potential operational impact of future migration. Attention should be given to digital signature and trust mechanisms that support authentication, integrity, software validation, and identity management functions.

Priority areas may include:

- Public Key Infrastructure (PKI).
- Certificate authorities and trust chains.

- Code signing and software update validation.
- Firmware signing.
- Identity federation and authentication services.
- API signing and workload identity.
- Machine identity and certificate lifecycle management.
- Digital signature implementations using RSA, ECDSA, DSA, or related public-key mechanisms.

While Identity and Signature Resiliency may not present the same immediate risk as legacy cryptographic weaknesses or Harvest Now, Decrypt Later (HNDL) risk, these trust systems often require significant planning, coordination, testing, and vendor engagement. Early assessment helps agencies understand dependencies, sequence modernization efforts, and prepare for future adoption of post-quantum digital signature standards. [S5] [S6] [S7]

13.8 Engage vendors and cloud providers

Agencies should use the vendor questions and sample RFI language above to turn cryptographic findings into acquisition and roadmap action. The goal is to understand which risks can be remediated internally, which require vendor action, and which require contract language, roadmap tracking, or modernization alignment. [S7] [S18]

13.9 Align PQC with modernization

Agencies should not create a disconnected PQC program. They should align PQC readiness with Zero Trust, cloud modernization, PKI modernization, identity modernization, DevSecOps, application modernization, FedRAMP and cloud service review, acquisition planning, and data protection strategy. [S17]

Accenture brings systems integration, cybersecurity engineering, cloud transformation, and federal mission delivery capabilities that can align PQC readiness with Zero Trust, PKI and identity modernization, DevSecOps, cloud migration, application transformation, acquisition, and data protection programs. This enables agencies to absorb cryptographic change through existing modernization portfolios rather than create an isolated PQC initiative. [S17]

14. Role of Wiz: Visibility, Context, and Prioritization

Wiz strengthens discovery and contextual understanding across cloud and connected environments. In PQC readiness, this means helping agencies identify cryptographic blind spots, understand cryptographic dependencies, and prioritize remediation activities based on exposure, data sensitivity, and operational risk.

This approach aligns with Wiz's Post-Quantum Readiness Framework, which organizes cryptographic findings into actionable readiness phases focused on Legacy Resiliency, Harvest Now, Decrypt Later (HNDL) risk, and Identity and Signature Resiliency, helping organizations prioritize cryptographic risk reduction efforts. [S21]

The Wiz for Post-Quantum Readiness Security Framework surfaces cryptographic metadata across cloud environments and builds a risk-prioritized view of findings. It helps reduce blind spots, identify legacy cryptographic debt, and support readiness planning across cloud services, workloads, configuration, and runtime context. Inventory is treated as an input to prioritization rather than an end state. [S15]

Wiz provides capabilities related to cryptographic discovery and visibility, including TLS termination on load balancers and web services, key management posture, secret scanning, host configuration auditing, and weak SSH key exchange identification. These findings are integrated into the Wiz Security Graph, allowing

organizations to evaluate cryptographic risk alongside broader cloud context such as exposure paths, identity permissions, sensitive data findings, workload posture, and configuration risk. [S15]

By combining cryptographic findings with broader environmental context, Wiz helps organizations identify high-priority risk combinations and focus remediation efforts where they can have the greatest operational impact. This supports both near-term risk reduction activities, such as addressing legacy cryptographic weaknesses, and longer-term PQC migration planning.

Wiz can also help agencies evaluate operational migration paths by identifying cryptographic dependencies associated with vendor-managed services, cloud-native platforms, and third-party technologies. By understanding where cryptographic risk is tied to specific vendors, managed services, or external dependencies, agencies can better assess vendor readiness, prioritize engagement activities, align migration planning with vendor roadmaps, and identify areas where remediation is dependent on supplier support rather than direct agency action. This additional context helps transform cryptographic discovery into actionable modernization and acquisition planning.

Wiz aligns cryptographic visibility with the risk conditions that make HNDL actionable: public exposure, sensitive data access, protocol posture, identity relationships, and the use of vulnerable key establishment. Runtime telemetry and environmental context can help agencies understand active TLS and SSH usage and identify where modernization can reduce present and future exposure. [S15] [S16] [S21]

While no technology platform can solve PQC migration independently, Wiz helps agencies improve the visibility, context, and prioritization needed to support risk-informed planning and execution.

15. Role of Accenture: Integrating Technology, Mission, and Federal Execution

Accenture helps agencies translate cryptographic visibility into enterprise-scale modernization. Its role is not limited to advisory support. As a federal systems integrator, Accenture can architect, engineer, integrate, test, deploy, and sustain cryptographic change across heterogeneous agency environments.

This end-to-end role combines cybersecurity engineering, cloud and infrastructure transformation, enterprise architecture, application modernization, PKI and identity expertise, DevSecOps, acquisition support, program delivery, and federal mission operations. Accenture connects cryptographic findings to mission priorities, target architectures, modernization portfolios, vendor ecosystems, and policy requirements.

Accenture can help agencies determine which risks require immediate remediation, which dependencies require vendor action, which systems need pilots or interoperability testing, and which changes should be integrated into planned cloud, network, application, identity, or PKI modernization.

This role spans four integrated areas:

Strategy and mission alignment:

- Mission, executive, and stakeholder alignment.
- Risk prioritization, investment strategy, and policy alignment.
- Governance and operating model design.

Architecture, engineering, and systems integration:

- Enterprise architecture and target-state cryptographic design.

- Integration of CBOM and inventory data with CMDB, CDM, CNAPP, PKI, ICAM, DevSecOps, and vulnerability management.
- Application, cloud, network, identity, PKI, code-signing, and firmware-signing modernization.
- Testbeds, pilots, interoperability, performance, and deployment engineering.

Program execution and ecosystem integration:

- Acquisition support, vendor coordination, roadmap sequencing, and implementation at scale.
- Workforce enablement, change management, and cross-agency coordination.

Sustainment and cryptographic agility:

- Automation, metrics, monitoring, and continuous governance.
- Managed operational support and ongoing modernization as standards, threats, and vendor capabilities evolve.

Accenture's published crypto-agility approach emphasizes leadership alignment, cryptographic discovery, ecosystem coordination, crypto-agile architecture, testbeds, pilots, phased rollout, and continuous monitoring. These capabilities map directly to the federal operating model proposed in this paper and position Accenture to integrate technology and mission execution from strategy through sustainment. [S17]

Joint positioning
Wiz helps agencies discover and contextualize cryptographic risk. Accenture integrates technology and translates those insights into mission-aligned architecture, modernization, acquisition, implementation, and sustained operations.

Together, the focus is moving agencies from visibility to action through a practical, risk-informed approach to PQC readiness.

16. Federal Operating Model and Maturity Journey

PQC readiness should be managed as a lifecycle, not a one-time assessment. A simple operating model can help agencies organize the work.

16.1 Operating model

Stage	Agency action
Discover	Identify cryptographic assets and dependencies
Contextualize	Add mission, data, exposure, owner, and vendor context
Prioritize	Rank by risk, urgency, and feasibility
Plan	Sequence modernization, acquisition, and vendor actions
Execute	Remediate weaknesses and migrate in phases
Govern	Maintain inventory, CBOM, policy, and monitoring

16.2 Maturity journey

Maturity stage	Description
Stage 1: Ad hoc visibility	Crypto findings are isolated and incomplete
Stage 2: Initial inventory	Priority systems and cloud services are inventoried
Stage 3: Contextual inventory	Findings are mapped to mission, data, exposure, and ownership
Stage 4: Prioritized migration plan	Actions are sequenced by risk and feasibility
Stage 5: Continuous governance	CBOM, policy, monitoring, and modernization are sustained

The staged model reflects operational reality. Agencies cannot replace all cryptography at once. Early maturity focuses on discovery and inventory. Intermediate maturity adds mission, data, and exposure context. Advanced maturity integrates cryptographic findings into governance, acquisition, vendor management, modernization planning, and continuous monitoring.

NIST NCCoE's PQC migration FAQ describes six phases of the PQC migration journey and highlights cryptographic visibility and risk management as a core workstream focused on maintaining comprehensive inventory to guide migration. [S9]

17. Recommended Call to Action

> Federal agencies should begin with a focused cryptographic risk assessment across priority systems, use CBOM to structure cryptographic transparency, identify current classical weaknesses, assess Harvest Now, Decrypt Later (HNDL) risk, assess Identity and Signature Resiliency across trust systems, and build a phased migration roadmap that aligns to mission priorities, modernization plans, vendor readiness, and future trust requirements.

The practical implication is that agencies should use 2026 to establish leadership, validate priority inventories, identify execution dependencies, begin pilot planning, and connect cryptographic risk to acquisition and modernization decisions. The migration timeline is no longer abstract. [S22]

Agencies should not wait for full PQC migration to reduce cryptographic risk. They should begin now with visibility, context, prioritization, and action.

Readiness checklist

- Do we know where cryptography exists?
- Do we know which systems protect long-lived sensitive data?
- Do we know which assets are publicly exposed?
- Do we know where weak algorithms, weak hashes, weak key exchange, or weak signatures are used?
- Do we know which systems depend on vendor-managed cryptography?
- Do we have CBOM or comparable cryptographic inventory outputs?
- Do we have certificate and key lifecycle ownership?
- Do we know where code signing, firmware signing, and software update validation are used?
- Do we know where TLS downgrade or fallback exposure exists?
- Do we have a prioritized remediation and migration plan?
- Do we have governance to keep inventory current?

18. Conclusion

PQC readiness does not begin with algorithm replacement. It begins with visibility, context, prioritization, and action. Executive Order 14412 makes this work time-bound: agencies now need accountable leadership, validated inventories, prioritized plans, progress toward 2030 and 2031 transition targets, and acquisition practices that can absorb new federal requirements. Agencies that act in 2026 can enter 2027 with a defensible roadmap, initial pilots, CBOM-informed governance, and a stronger operating model for continued cryptographic change. [S22]

Wiz and Accenture support this work through complementary capabilities. Wiz strengthens discovery, cloud context, and risk prioritization. Accenture brings architecture, engineering, systems integration, program delivery, acquisition, testing, and federal mission capabilities needed to execute change at scale. The goal is

not enterprise-wide replacement all at once. It is defensible prioritization, practical risk reduction, and a durable operating model that adapts as cryptographic standards, technologies, vendor roadmaps, and threats evolve.

Appendix A. Source List

Source IDs are referenced throughout the paper. Sources are grouped by category to distinguish federal requirements, federal guidance, technical standards, implementation references, and partner materials.

Federal Policy and Direction

[S22] Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, The White House, June 22, 2026; 91 FR 38483

[S23] Executive Order 14413, Ushering in the Next Frontier of Quantum Innovation, The White House, June 22, 2026; 91 FR 38487

[S1] Office of Management and Budget (OMB) M-23-02, *Migrating to Post-Quantum Cryptography*, November 18, 2022

[S2] National Security Memorandum 10 (NSM-10), *Promoting U.S. Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, The White House, May 4, 2022

NIST Post-Quantum Cryptography Standards

[S3] NIST Post-Quantum Cryptography Project, NIST Computer Security Resource Center (CSRC)

[S4] FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*, NIST CSRC, August 13, 2024

[S5] FIPS 204, *Module-Lattice-Based Digital Signature Standard (ML-DSA)*, NIST CSRC, August 13, 2024

[S6] FIPS 205, *Stateless Hash-Based Digital Signature Standard (SLH-DSA)*, NIST CSRC, August 13, 2024

Federal PQC Readiness and Migration Guidance

[S7] *Quantum-Readiness: Migration to Post-Quantum Cryptography*, CISA, NSA, and NIST, August 21, 2023

[S8] *Migration to Post-Quantum Cryptography Project*, NIST National Cybersecurity Center of Excellence (NCCoE)

[S9] *NCCoE Migration to PQC Frequently Asked Questions*, NIST NCCoE

Cryptographic Standards and Technical Guidance

[S10] NIST SP 800-131A Rev. 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019

[S11] NIST SP 800-52 Rev. 2, *Guidelines for the Selection, Configuration, and Use of TLS Implementations*, August 2019

[S12] NIST SP 1800-37, *Addressing Visibility Challenges with TLS 1.3*, September 2025

[S13] NIST CSWP 39, *Considerations for Achieving Cryptographic Agility: Strategies and Practices*, December 19, 2025

[S20] *NIST Retires SHA-1 Cryptographic Algorithm*, NIST, December 15, 2022

CBOM and Software Transparency

[S14] *Cryptography Bill of Materials (CBOM) Capability*, CycloneDX

Federal Acquisition and High-Assurance References

[S18] *Post-Quantum Cryptography Buyer's Guide*, U.S. General Services Administration (GSA), 2025

[S19] *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Algorithms Guidance*, National Security Agency (NSA), May 2025

Wiz References

[S15] *Preparing for Post-Quantum Cryptography*, Wiz Blog, January 8, 2026

[S16] *Post-Quantum Cryptography: What It Is and How to Prepare*, Wiz Academy, January 16, 2026

[S21] *Wiz for PQC Readiness: Eliminate Cryptographic Blind Spots*, Wiz Blog, May 18, 2026

Accenture and Industry References

[S17] *The Future at Quantum Speed*, Accenture Federal Services and Market Connections, March 2025