carahsoft

TYCHON

What OMB M-26-15 Means for Federal Migration

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA Multiple Award Schedule (MAS), NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with TYCHON, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/TYCHONResources

Join Events & Webinars:
carah.io/TYCHONEvents

Discover Technology Solutions:
carah.io/TYCHON

Learn About Procurement:
carah.io/TYCHONContracts

Connect With Our Team:
Tychon@carahsoft.com
844-445-5688

TYCHON Blog

What OMB M-26-15 Means for Federal Migration

June 27, 2026, by Aaron Faulkner

On June 24, 2026, the Office of Management and Budget issued **Memorandum M-26-15**, "Execution of the Migration to Post-Quantum Cryptography." It implements Executive Order 14409 (June 22, 2026) and fulfills OMB's obligation under the Quantum Computing Cybersecurity Preparedness Act. For federal civilian agencies, it converts post-quantum cryptography from a planning topic into a funded, scheduled program of record.

Here is what the memo requires and what agencies should do now.

The Headline: A 120-Day Plan Deadline

M-26-15 directs every covered agency to develop and submit a PQC Migration Plan to OMB and the Office of the National Cyber Director within 120 days of the memo's date, roughly late October 2026. The plan is treated as a dynamic document expected to mature over time, but the initial submission carries specific required content.

Two of the required plan sections stand out:

- The methodologies and automated tools used for the cryptographic inventory.
- A plan for implementing a cryptographically agile architecture.

In other words, agencies are now required to name the tools they will use to discover and inventory their cryptography. That is a meaningful shift. Inventory is no longer a recommended practice. It is a documented, accountable plan element.

The Target: Mitigate Quantum Risk by 2030, Full Migration by 2035

The memo sets an objective to mitigate as much quantum risk as feasible by December 31, 2030, and lays out a five-phase timeline:

- **Phase 1 (2026 to 2027): Strategy, Planning, and Discovery.** Inventory of High Value Assets and high impact systems, risk assessment, governance setup, and migration planning.
- **Phase 2 (2027 to 2028): Pilots and Early Migration.** Pilots and early migration of prioritized systems.
- **Phase 3 (2028 to 2030): Prioritized Migration.** Migration of key establishment to PQC across the highest-priority systems.
- **Phase 4 (2031): Signature Migration.** Migration of digital signatures to PQC for priority systems.
- **Phase 5 (2035): Full Migration.** Completion across remaining systems.

Plans must align with NIST IR 8547, Transition to Post-Quantum Cryptography Standards.

The Foundation: Automated Cryptographic Inventory and the CBOM

The memo is unambiguous that this work begins with discovery. It states that manual approaches to discovery and management of cryptography are often insufficient given the scale and complexity of federal IT environments, and it directs agencies to use automation for inventory, policy enforcement, and compliance reporting.

It also names the artifact. Agencies should build a central Cryptographic Bill of Materials, or CBOM, populated through automated tools such as software composition analysis of SBOMs, application security testing, and network scanners, to provide a real-time view of the agency's cryptographic posture. That data should feed continuous-monitoring dashboards that track migration progress and produce metrics for leadership and compliance reports.

This is the center of gravity for Phase 1. Without a complete and current inventory, prioritization, risk assessment, and migration sequencing are all guesswork.

What Agencies Should Prioritize

M-26-15 directs risk-based prioritization. Agencies must prioritize:

- High impact systems.
- High Value Assets.
- Any system with highly sensitive data or particular vulnerability to a cryptographically relevant quantum computer.

It also points agencies toward asymmetric-based logical access control systems, such as PKI, and data expected to remain mission-sensitive in 2030. Appendix A enumerates the quantum-vulnerable algorithms agencies must account for, including RSA, ECDH, ECDSA, Diffie-Hellman, MQV, and DSA.

Other Provisions Worth Noting

- **TLS 1.3.** Agencies must support TLS 1.3 or a successor no later than January 2, 2030, consistent with Executive Order 14306. TLS 1.3 is foundational for deploying PQC at the network level.
- **Cryptographic agility.** The memo treats agility as an architectural requirement, achieved through modern libraries, configuration-driven algorithm selection, protocol negotiation, and agile key management.
- **Hybrid architecture.** Hybrid is permitted as a risk-management tool but framed as an intricate and resource-intensive stopgap that agencies should adopt only after evaluating the tradeoffs.
- **Zero Trust.** PQC is named a foundational dependency for advancing a durable Zero Trust architecture across devices, networks, applications, and data.
- **Vendors and cloud.** Agencies must build PQC requirements into procurement. CISA and the Department of War will lead PQC migration efforts for multi-agency FedRAMP-authorized cloud and SaaS, PaaS, and IaaS solutions.
- **Scope.** The memo does not apply to national security systems. NSS are governed separately, and that governance was reset days before M-26-15 (see below).

The NSS Half of the Picture: NSPM-12

M-26-15 governs civilian systems. The national security side moved at almost the same time. On June 12, 2026, the President signed National Security Presidential Memorandum 12 (NSPM-12), "National Policy for the Cybersecurity of National Security Systems."

NSPM-12 is a governance overhaul rather than a PQC migration directive, but it changes the authority structure that agencies and contractors have cited for NSS cryptography:

- It rescinds NSM-8 (2022) and NSD-42 (1990), the prior foundational NSS directives.
- It re-establishes the Committee on National Security Systems (CNSS) as the authoritative body for NSS cybersecurity standards and enforcement.
- It designates the Director of the NSA as National Manager for NSS, with expanded authority including the government's cryptologic authority for NSS.
- It sets NIST standards as the minimum NSS baseline unless CNSS issues a complementary standard, and names CNSS Policy 15 (CNSSP-15), or its successor, as the commercial cryptographic standard for NSS.

The practical takeaway: for NSS, references to NSM-8 should now point to NSPM-12, the CNSS, and CNSSP-15. The PQC objective for NSS still aligns to CNSA 2.0 and the 2035 target, but the authority and standards path now runs through the re-established CNSS and the National Manager.

Together, M-26-15 and NSPM-12 cover the two environments. Civilian PQC migration runs on the M-26-15 plan and timeline. NSS cryptographic governance runs through NSPM-12, CNSS, and CNSSP-15.

The Immediate Action

The 120-day clock makes one thing clear. The first deliverable is a documented, automated cryptographic inventory, and agencies have to name the tool that produces it.

TYCHON Quantum Command is a stateless, process-level, agentless Automated Cryptographic Discovery and Inventory platform that produces and continuously maintains a CBOM, with production deployments across DoD and federal civilian agencies and NIPR and SIPR ATOs. It is built to deliver exactly what M-26-15 Phase 1 requires (comprehensive automated discovery, risk-based prioritization, and continuous monitoring that feeds compliance reporting), and it operates in the classified NSS environments now governed under NSPM-12 as well.

If your agency is building its PQC Migration Plan, the inventory methodology and tooling section is where the work starts. We can help.