

Post-Quantum Cryptography Migration Plan Instructions

Agency/Component	[AGENCY/COMPONENT NAME]
Version	[e.g., v1.0—Initial Submission]
Submission Date	[DATE] (Initial plan due October 22, 2026—120 days from the June 24, 2026, memorandum date to OMB and the Office of the National Cyber Director [ONCD] at PQC@omb.eop.gov)
Accountable Official	[NAME, TITLE (e.g., CIO or CISO)]
Approving Official	[NAME, TITLE]
Handling/Classification	[e.g., Controlled Unclassified Information (CUI)] (This plan may describe cryptographic inventory details, PKI architecture, and unmitigated vulnerabilities. Handle and disseminate it accordingly.)
Next Scheduled Update	[DATE] (Recommend at least an annual revision; see Section 0.)

0. How to Use This Template: Scope Note

This template operationalizes the minimum elements for the initial agency PQC migration plan described in Appendix B, Section 2 of [OMB Memorandum M-26-15](#), “Execution of the Migration to Post-Quantum Cryptography,” due October 22, 2026. Bracketed text, such as [AGENCY NAME], marks fields for the agency to complete. The italicized paragraphs marked “Guidance:” explain the memorandum requirements in that section and are intended for deletion or conversion to normal text once the section is complete. Short illustrative sample language is included in some sections to show the level of specificity expected; agencies should replace this sample language with the agency’s own facts rather than submit it as is.

Guidance: The memorandum states that it does not apply to national security systems (as defined in 44 U.S.C. § 3552(b)(6)).

Guidance: M-26-15 describes the migration plan as a dynamic document that will mature over time across a multiyear effort (2026–2035, in five phases). The initial submission must contain, at a minimum, timelines and milestones to achieve the first three migration phases and the TLSv1.3 testing and deployment timeline. Phases 4 and 5 are addressed at a strategic level in the initial plan and will be elaborated as the plan matures. Agencies should treat this document as a living plan, version it, and update it at least annually and whenever the cryptographic inventory, prioritization, or resourcing changes materially. Track revisions in the Appendix revision history table.

Section 1 of this template is a compliance crosswalk. It is provided as an internal quality-control tool. Before submission, confirm that every minimum element in the memorandum is addressed somewhere in the plan and record the corresponding section reference.

1. Compliance Crosswalk: M-26-15 Minimum Elements

Guidance: This crosswalk reproduces the nine minimum elements listed in Appendix B, Section 2 of M-26-15 for the initial plan submission. Update the “Section” column to reference the actual page or section numbers in the final document, and mark the status before submission.

See Section 1 in Template.

2. Governance Roles and Responsibilities

Guidance: M-26-15 states that PQC migration is not solely the responsibility of the agency-level CIO and CISO; accountability and responsibility must extend across agency leadership, both front office and components, with clearly defined roles. Appendix B, Section 1, of the memorandum provides a sample allocation of responsibilities, reproduced and adapted in the RACI table later in this document as a starting point.

2.1 Accountable Officials

[Example: The [CIO/CISO] is designated as the agency’s accountable official for PQC migration under this plan and is accountable for prioritization, risk acceptance, and resource allocation. The PQC Cryptographic Inventory and Migration Lead or Migration Program Manager coordinates agency-wide migration activities, ensures plan alignment, and reports to senior leadership.]

2.2 Governance Body

[Describe the governance structure, e.g., a PQC Migration Steering Committee or Working Group, its charter, meeting cadence, and reporting lines to agency leadership and to OMB or ONCD as applicable.]

2.3 Roles and Responsibilities (RACI)

Guidance: Sample roles (e.g., CIO/CISO, Program Office/Requirement Owner, CFO, PQC Migration Lead/Program Manager, PQC Technical Lead, Security Architect, and Application and System Owners) and their described functions are adapted from Appendix B, Section 1, of M-26-15. Add or rename rows to match the agency's actual organizational structure.

See Section 2.2 in Template.

3. Cryptographic Inventory: Methodology and Automated Tools

Guidance: M-26-15 states that manual approaches to discovery and management of cryptography are often insufficient given the scale and complexity of federal IT environments. It encourages agencies to use automation for a comprehensive, continuously updated view of their cryptographic posture, feeding a central Cryptographic Bill of Materials (CBOM). Recommended methods include Software Composition Analysis (SCA) of Software Bills of Materials (SBOMs), Static or Dynamic Application Security Testing (SAST/DAST), and network scanners to detect protocols and cipher suites. This section must also cover High Value Assets (HVAs) and high impact systems, consistent with the Phase 1 (2026–2027) focus on inventory and assessment. Where the agency uses Palo Alto Networks Quantum-Safe Security as its inventory tool, describe it as a "live cryptographic inventory built from agentless NGFW and Prisma Access telemetry (SSL/TLS, SSH, and VPN tunnel sessions). It functions as the agency's dynamic CBOM, complementing SCA/SBOM and SAST/DAST tooling for coverage this app does not itself provide (e.g., static source-code and dependency scanning)."]

3.1 Inventory Scope

[Describe the scope of systems, applications, network devices, cloud environments, and cryptographic libraries covered, and confirm that all agency HVAs and FISMA High Impact systems are included. Note any systems (e.g., classified, OT/ICS, or third party-hosted) with a separate or deferred inventory approach and the rationale. Confirm whether any systems fall outside the scope as national security systems. Note on tool coverage: Where the agency uses Palo Alto Networks Quantum-Safe Security, its visibility is limited to applications, user devices, infrastructure, and IoT devices whose traffic traverses agency Palo Alto Networks Next-Generation Firewalls (NGFW), managed by Strata™ Cloud Manager, Prisma Access®, or both. It discovers assets from SSL/TLS, SSH, and VPN tunnel telemetry at those enforcement points. Systems that do not route through this telemetry path (e.g., air-gapped systems, classified networks, or wholly cloud-native environments outside agency-managed NGFW and Prisma Access) fall outside the tool's visibility. They still require the manual review and SCA/SBOM-based coverage that is described elsewhere in this section. The tool complements but does not replace that coverage.]

3.2 Methodology

[Example: The agency is conducting a phased cryptographic discovery combining Palo Alto Networks Quantum-Safe Security with the SCA of SBOMs, SAST/DAST to identify cryptographic functions in code and manual review of legacy and air-gapped systems that cannot be scanned. Quantum-Safe Security is an agentless, telemetry-based capability that uses the agency's NGFW and Prisma Access tenants as distributed sensors to analyze SSL/TLS decryption, Traffic, and Tunnel Inspection logs. This capability catalogs applications, user devices, infrastructure, and IoT devices along with their cryptographic dependencies (protocols, keys, algorithms, certificates) into a dynamic Cryptographic Bill of Materials (CBOM), feeding a central dashboard and continuous-monitoring reports that track migration progress.]

3.3 Automated Tools

See Section 3.3 in Template.

4. System Prioritization Strategy

Guidance: M-26-15 requires agencies to prioritize PQC migration based on risk. The memorandum requires the plan to prioritize: (1) a high impact system (an information system where at least one security objective—confidentiality, integrity, or availability—is assigned a FIPS 199 potential impact value of “high,” per National Security Memorandum 10 [NSM-10]); (2) an HVA (as defined in OMB Memorandum M-19-03 or a successor policy); and (3) any other system with highly sensitive data or that the agency determines is likely to be vulnerable to CRQC-based attacks. This system should include systems that are logical access control systems based in asymmetric encryption (such as PKI) using an algorithm listed in Appendix A of the memorandum, or that contain data that is expected to remain mission-sensitive in 2030. Agencies are encouraged to consult with CISA to help make these determinations. Where the agency uses Palo Alto Networks Quantum-Safe Security its asset-level classifications can evidence this prioritization: the app’s harvest now, decrypt later (HNDL) risk classification identifies assets by using classical algorithms that are currently secure but vulnerable to a future CRQC, its business impact rating (high or standard) reflects asset handling of sensitive data that is subject to regulatory requirements, or with the greatest HNDL exposure, and its Data Exposure Risk classification flags sessions using NIST-deprecated algorithms or protocols today. These classifications are asset-level risk signals generated by the tool and do not themselves constitute the agency’s high impact system or HVA designations, which remain governed by NSM-10 and OMB M-19-03 respectively.]

4.1 Prioritization Criteria and Risk-Based Justification

[Describe the agency’s methodology for scoring and ranking systems—e.g., a weighted model combining FISMA impact level, HVA designation, data sensitivity or shelf-life (HNDL exposure through 2030 and beyond), reliance on vulnerable asymmetric algorithms listed in Appendix A, and operational criticality. Explain how the scoring drives the sequencing of migration in Phases 2–5. Where Quantum-Safe Security is deployed, describe how its business impact (high or standard) and cryptography risk (data exposure, HNDL, quantum-secure) filters and asset-level Quantum Readiness status (Not Ready, Ready, Quantum Safe) inform the weighting and sequencing of the agency’s remediation roadmap, alongside the mandatory FISMA/HVA/Appendix A/2030-mission-sensitivity criteria. Also, describe the agency’s approach under the M-26-15 system modernization guidance. Identify legacy systems that are incapable of supporting PQC or hybrid cryptography and prioritize them for replacement or decommissioning. (Or, where an upgrade is impractical, describe evaluating Quantum-Safe Security Cipher Translation Proxy as an interim mitigation for legacy or IoT assets.) Also, incorporate PQC upgrades into planned cloud migrations, software development lifecycles, and hardware refresh schedules.]

4.2 Mandatory Priority Categories

See Section 4.2 in Template.

4.3 Prioritization Tiers

[List or attach the resulting tiered system inventory (e.g., Tier 1 = mandatory priority systems above; Tier 2 = elevated risk; Tier 3 = standard) with counts of systems in each tier and the migration phase each tier is targeted for.]

5. Migration Timelines and Milestones

Guidance: M-26-15 sets a five-phase migration (2026–2035). The initial plan must include timelines and milestones for all three phases falling within the initial planning horizon (Phases 1–3), plus a dedicated timeline for testing and deployment to meet the TLSv1.3 deadline. Populate agency-specific target dates below; do not change the phase definitions or the memorandum-mandated deadlines. Agencies must align Phase 5 planning with [NIST Internal Report \(IR\) 8547](#), “Transition to Post-Quantum Cryptography Standards,” or a successor document.

5.1 Migration Phases

See Section 5.1 in Template.

5.2 TLSv1.3 Testing and Deployment Timeline (Deadline January 2, 2030)

Guidance: Consistent with Executive Order 14306, M-26-15 requires agencies to support TLSv1.3 or a successor version as soon as practicable, but not later than January 2, 2030. TLSv1.3 is foundational for deploying PQC at the network level and supports a hybrid key exchange in the ClientHello/ServerHello handshake. Provide a distinct milestone timeline for testing and deployment against this deadline, independent of the broader phase timelines above.

See Section 5.2 in Template.

6. Cryptographic Agility Architecture Plan

Guidance: M-26-15 defines cryptographic agility as an architectural principle enabling an organization to switch cryptographic algorithms with minimal disruption, and identifies four supporting practices: (1) using modern cryptographic libraries designed for agility (e.g., OpenSSL 3.x provider architecture, Java JCA/JCE); (2) configuration-driven cryptography, so algorithm choice is set externally rather than compiled into application binaries; (3) designing protocols for cipher suite negotiation, while guarding against downgrade attacks; and (4) ensuring an agile key management infrastructure (KMS/HSMs) can generate, store, and manage both classical and PQC keys. Cryptographic agility is also an explicit exit criterion for Phases 3 and 4, and the memorandum ties PQC integration to the [CISA Zero Trust Architecture \(ZTA\) Maturity Model](#) across the device, network, application or workload, and data pillars. Where the agency's network perimeter runs NGFWs and Prisma Access, the following capabilities described in [Palo Alto Networks quantum security documentation](#) map to these four practices at the network layer: (1) configuration-driven PQC/hybrid key exchange selectable per decryption profile (PQC-standard covering ML-KEM/Kyber families, or PQC-Experimental covering Frodo/BIKE/HQC families) without requiring a software release; (2) IKEv2 VPN cryptographic agility via RFC 9242/RFC 9370 hybrid key exchange, which allows administrators to add or remove supported PQC key encapsulation mechanisms (KEMs) from the negotiation without software updates or network changes; and, (3) for legacy or IoT assets that cannot be upgraded to negotiate PQC natively, a Cipher Translation Proxy on NGFWs (PAN-OS® 12.1 or later) that intercepts classical-algorithm traffic and reencrypts it into quantum-safe algorithms (such as ML-KEM) at the network edge in real time, with no endpoint code changes. These network-layer capabilities support agility for traffic terminated at the firewall; they do not by themselves make application, endpoint, or library-level cryptography agile, which the agency must still address through the practices above.]

[Describe the target architecture and standards against each of the four practices above. Identify current gaps against this target state and the plan and resourcing to close them by the end of Phase 3. Address how PQC will be integrated into the agency's zero trust architecture, including device attestation (e.g., TPM-rooted), network termination points (firewalls, VPN concentrators, cloud gateways, API proxies), application or workload token signing, and re-encryption of long-lived sensitive data. State whether the agency will implement hybrid classical/PQC architectures during transition and, if so, summarize the risk tradeoffs considered. M-26-15 characterizes hybrid approaches as "an intricate and resource-intensive stopgap" requiring thorough evaluation. Where applicable, describe the agency's use of NGFWs and Prisma Access hybrid PQC key exchange and Cipher Translation Proxy as an interim network-layer mitigation for legacy and IoT assets, and identify which zero trust pillars (network termination points) this covers versus the application or workload and data pillars that require separate remediation.]

7. Third-Party Coordination Plan

Guidance: M-26-15 directs agencies to reference the CISA publication "Product Categories for Technologies That Use Post-Quantum Cryptography Standards" and ensure product requirements in those categories include PQC integration. Agencies should engage FedRAMP-authorized cloud service providers to delineate PQC migration responsibilities within the shared responsibility model; CISA and the Department of War (DOW), with GSA, will lead PQC migration for FedRAMP-authorized cloud, SaaS, PaaS, or IaaS solutions used at more than one agency.

See Section 7 in Template.

8. Resource Estimate: Funding and Personnel

Guidance: M-26-15 requires an estimate of the funding and personnel resources required to execute the plan. Appendix B, Section 1, offers a sample allocation of responsibilities in which the Chief Financial Officer, working with the CIO and CISO in collaboration with a PQC Migration Program Manager, ensures PQC migration resource requirements are represented in the agency's annual budget request. Agencies should adapt this allocation to their own governance structure rather than treat it as a required assignment. Break down the estimate by phase and fiscal year, and distinguish new and incremental resources from those already budgeted.

See Section 8 in Template.

9. Risk Management Strategy for the Migration Period

Guidance: M-26-15 requires a risk management strategy covering the migration period itself. Relevant risks flagged by the memorandum include continued HNDL exposure of mission-sensitive data during migration; the resource-intensive complexity and downgrade-attack risk of hybrid architectures; vendor or commercial PQC product availability; and legacy systems incapable of supporting PQC or hybrid cryptography that must be prioritized for replacement or decommissioning. Agencies should be aware that different inventorying and remediation tools have inherent advantages at different layers of IT infrastructure. Palo Alto Networks Quantum-Safe Security or related PAN-OS quantum security features, for instance, rely on network-level traffic traversing NGFWs and Prisma Access.

See section 9 in Template.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
pqc-migration-plan-instructions_101426