

# Post-Quantum Cryptography Migration Plan

|                         |  |
|-------------------------|--|
| Agency/Component        |  |
| Version                 |  |
| Submission Date         |  |
| Accountable Official    |  |
| Approving Official      |  |
| Handling/Classification |  |
| Next Scheduled Update   |  |

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

## Section 1

| # | M-26-15 minimum element                                                                                     | Addressed in section | Status<br>[Complete/Incomplete/Not Started] |
|---|-------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------|
| 1 | System prioritization strategy with risk-based justification                                                | Section 4            |                                             |
| 2 | Timelines and milestones to achieve first three migration phases                                            | Section 5            |                                             |
| 3 | Timelines and milestones for testing and deployment to meet the TLS 1.3 support deadline of January 2, 2030 | Section 5.2          |                                             |
| 4 | Methodologies and automated tools used for cryptographic inventory                                          | Section 3            |                                             |
| 5 | Plan for implementing a cryptographically agile architecture                                                | Section 6            |                                             |
| 6 | Third-party coordination plan                                                                               | Section 7            |                                             |
| 7 | Estimate of funding and personnel resources required                                                        | Section 8            |                                             |
| 8 | Risk management strategy for the migration period                                                           | Section 9            |                                             |
| 9 | Governance roles and responsibilities                                                                       | Section 2            |                                             |

## 2. Governance Roles and Responsibilities

### Section 2.3

| Function                                                                   | Responsible | Accountable | Consulted | Informed |
|----------------------------------------------------------------------------|-------------|-------------|-----------|----------|
| Overall prioritization, risk acceptance, and resource allocation           |             |             |           |          |
| Agency-wide migration coordination and plan alignment                      |             |             |           |          |
| Cryptographic inventory, algorithm selection, testing, and deployment      |             |             |           |          |
| Integration of PQC into zero trust architecture/ interoperability          |             |             |           |          |
| Budget and resource planning; PQC costs reflected in annual budget request |             |             |           |          |
| Vendor requirements include PQC readiness and crypto-agility provisions    |             |             |           |          |
| Implementation of crypto-agile, PQC-compatible technology in owned systems |             |             |           |          |

### 3. Cryptographic Inventory: Methodology and Automated Tools

#### Section 3.3

| Tool / capability                                                                                 | Discovery method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Coverage<br>(systems/environments)                                                                                                                                                                              | Owner |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>Palo Alto Networks Quantum-Safe Security (Strata Cloud Manager app)</b>                        | Agentless telemetry from NGFW/Prisma Access: SSL/TLS decryption logs, Traffic logs, and Tunnel Inspection logs, analyzed for protocol, key exchange algorithm, encryption/authentication algorithm, and certificate metadata                                                                                                                                                                                                                                                                                | Applications, user devices, infrastructure, and IoT devices traversing agency NGFW (managed by Strata Cloud Manager) and/or Prisma Access — requires Quantum-Safe Security license and Device Telemetry enabled |       |
| <b>Palo Alto Networks Quantum-Safe Security — risk, readiness, and criticality classification</b> | Automated classification of each discovered asset into Cryptography Risk categories (Data Exposure Risk, Harvest Now Decrypt Later (HNDL) Risk, or Quantum-Secure), Quantum Readiness status (Not Ready, Ready, or Quantum Safe), and Business Impact (High or Standard); recommendation engine surfaces hardware/software upgrade paths and, for non-upgradable legacy or IoT assets, Cipher Translation Proxy remediation (NGFW re-encrypts classical traffic to ML-KEM in real time at the network edge) | Assets classified via the Inventory and Overview dashboard, scoped as above                                                                                                                                     |       |
| <b>e.g., SCA/SBOM tool</b>                                                                        | Software Composition Analysis of SBOMs                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                 |       |
| <b>e.g., SAST/DAST tool</b>                                                                       | Static/dynamic testing to find cryptographic functions in code                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                 |       |
| <b>PKI/CA and key management export; manual review</b>                                            | Certificate/key inventory export; legacy/air-gapped/OT systems                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                 |       |

## 4. System Prioritization Strategy

### Section 4.2

| Required priority category                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Agency systems identified (count/examples)                                                                                                                                                                                                                                                                           | Justification/evidence |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| High Impact systems (FIPS 199 "high" on any security objective, per NSM-10). Supporting evidence, where applicable: assets rated Business Impact = High and/or Cryptography Risk = Harvest Now, Decrypt Later in Palo Alto Networks Quantum-Safe Security.)                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                      |                        |
| High Value Assets (HVAs) (per OMB M-19-03 or successor). Supporting evidence, where applicable: assets rated Business Impact = High and/or Cryptography Risk = Harvest Now, Decrypt Later in Palo Alto Networks Quantum-Safe Security.)                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                      |                        |
| Systems with highly sensitive data or determined by the agency to be particularly vulnerable to CRQC-based attacks, including logical access control systems based in asymmetric encryption (such as PKI) using an Appendix A algorithm. Supporting evidence, where applicable: assets rated Cryptography Risk = Data Exposure Risk (sessions/certificates using NIST-deprecated algorithms) or Harvest Now, Decrypt Later in Palo Alto Networks Quantum-Safe Security, including certificates flagged by Certificate Key Algorithm/Key Size/Certificate Signing Algorithm metadata. |                                                                                                                                                                                                                                                                                                                      |                        |
| Systems containing data expected to remain mission-sensitive in 2030. Supporting evidence, where applicable: assets rated Cryptography Risk = Harvest Now, Decrypt Later and/or Business Impact = High (the tool's High rating considers assets that must protect data over long periods) in Palo Alto Networks Quantum-Safe Security.                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                      |                        |
| Configuration prerequisite for tool-based evidence above                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Confirm the agency has configured Asset Criticality in Quantum-Safe Security (automated rules by App-ID category/user group, or manual assignment) so Business Impact ratings and related report sections are populated; unconfigured assets default to Standard impact and will understate prioritization evidence. |                        |

## 5. Migration Timelines and Milestones

### Section 5.1

| Phase                                                                 | M-26-15 window | Agency milestones/<br>deliverables                                                                                                                                                                                                                                                                                                                                            | Target completion |
|-----------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Phase 1 —<br>Strategy, Planning,<br>and Discovery                     | 2026–2027      | Cryptographic inventory (incl. HVAs and High Impact systems); risk assessment; strategy definition; awareness and training; governance frameworks established; accountable officials designated; further migration planning developed                                                                                                                                         |                   |
| Phase 2 —<br>Pilots and Early Migration                               | 2027–2028      | Pilot(s) selected and executed — note GSA's FICAM Office is coordinating interested agencies on testing PQC-ready physical/ logical access systems (icam@gsa.gov); early migration of prioritized systems; lessons learned incorporated into plan revision                                                                                                                    |                   |
| Phase 3 —<br>Prioritized Migration                                    | 2028–2030      | Migrate HVAs, High Impact systems, highly sensitive/CRQC-vulnerable systems to PQC for key establishment (see NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard); achieve cryptographic agility across these systems; meet TLS 1.3 deadline (see 5.2); mitigate as much quantum risk as feasible by December 31, 2030 per Action One of the memorandum |                   |
| Phase 4 —<br>Signature Migration<br>(post-initial-submission horizon) | 2031           | Migrate same priority systems to PQC for digital signatures (see NIST FIPS 186-5, Digital Signature Standard); confirm cryptographic agility. Addressed here at a strategic level; will be elaborated as the plan matures.                                                                                                                                                    |                   |
| Phase 5 —<br>Full Migration<br>(post-initial-submission horizon)      | By 2035        | Complete migration of remaining systems, sequenced by risk assessment and availability of commercial PQC offerings, aligned with NIST IR 8547, Transition to Post-Quantum Cryptography Standards, or successor document. Addressed here at a strategic level; will be elaborated as the plan matures.                                                                         |                   |

### Section 5.2

| Milestone                                                                                                           | Target date                               | Owner |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------|
| Inventory of systems/services not yet supporting TLS 1.3                                                            |                                           |       |
| Remediation plan for non-conforming systems approved                                                                |                                           |       |
| TLS 1.3 (or successor) enabled in test/staging environments, including hybrid key exchange testing where applicable |                                           |       |
| TLS 1.3 production deployment and validation testing                                                                |                                           |       |
| Full TLS 1.3 (or successor) support confirmed agency-wide                                                           | Not later than January 2, 2030 (deadline) |       |

## 7. Third-Party Coordination Plan

| Third-party category                                               | Coordination approach                                                                                                  | Contractual/acquisition levers                            | Target date |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-------------|
| FedRAMP-authorized cloud/SaaS/PaaS/IaaS providers                  | Engage on shared-responsibility model for PQC migration; note CISA/DOW/GSA-led coordination for multi-agency solutions | e.g., PQC readiness clauses in renewals                   |             |
| Software/hardware vendors (per CISA PQC product categories)        |                                                                                                                        | Require PQC integration for products in scoped categories |             |
| Contractors and system integrators                                 |                                                                                                                        |                                                           |             |
| Interagency / mission partners (e.g., GSA FICAM PQC working group) |                                                                                                                        |                                                           |             |

## 8. Resource Estimate: Funding and Personnel

| Phase   | Fiscal year(s) | Estimated funding | Personnel (FTE/contractor) | Funding source status [Budgeted/Unfunded requirement] |
|---------|----------------|-------------------|----------------------------|-------------------------------------------------------|
| Phase 1 | FY26–FY27      |                   |                            |                                                       |
| Phase 2 | FY27–FY28      |                   |                            |                                                       |
| Phase 3 | FY28–FY30      |                   |                            |                                                       |
| Phase 4 | FY31           |                   |                            |                                                       |
| Phase 5 | FY32–FY35      |                   |                            |                                                       |

## 9. Risk Management Strategy for the Migration Period

| Risk                                                                                                                                                             | Likelihood | Impact | Mitigation                                                                                                                                                                                                                                                                                                   | Owner |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Continued harvest-now, decrypt-later exposure of mission-sensitive data during migration                                                                         |            |        | e.g., prioritize highly sensitive/2030 mission-sensitive systems in Phase 3                                                                                                                                                                                                                                  |       |
| Legacy systems incapable of supporting PQC or hybrid cryptography                                                                                                |            |        | Identify and prioritize for replacement or decommissioning; align with cloud migration, SDLC, and hardware refresh schedules                                                                                                                                                                                 |       |
| Vendor/commercial PQC product availability delays, including FedRAMP cloud/SaaS/PaaS/IaaS providers                                                              |            |        |                                                                                                                                                                                                                                                                                                              |       |
| Interoperability failures or downgrade attacks in hybrid classical/PQC architectures                                                                             |            |        |                                                                                                                                                                                                                                                                                                              |       |
| Workforce/skills shortage; insufficient/unfunded budget for migration activities                                                                                 |            |        |                                                                                                                                                                                                                                                                                                              |       |
| Network-telemetry-based inventory tools (e.g., Quantum-Safe Security) create a false sense of complete cryptographic visibility                                  |            |        | Maintain manual review and SCA/SBOM coverage for air-gapped, classified, or non-NGFW/Prisma Access cloud-native systems outside the tool's telemetry path (see Section 3.1); do not treat tool-based inventory as comprehensive without confirming scope                                                     |       |
| PQC algorithms and hybrid classical/PQC architectures lack multi-year real-world validation, given the recency of NIST standardization                           |            |        | Favor hybrid key exchange (combining a classical KEM with one or more PQC KEMs, e.g., via RFC 9242/RFC 9370 on IKEv2 VPNs or PQC-Standard/PQC-Experimental TLS decryption profiles) during the transition period; monitor NIST guidance and vendor advisories for parameter or algorithm changes             |       |
| Cryptographic debt re-accumulates after initial remediation (e.g., unsanctioned PQC or weak ciphers introduced by developers, third parties, or internal actors) |            |        | Implement continuous monitoring/drift detection and automated compliance reporting (e.g., decryption/vulnerability-protection profiles configured to detect and block unsanctioned or weak ciphers, with documented exceptions for authorized penetration testing) rather than a one-time remediation effort |       |

## Appendix A. Revision History

| Version | Date | Summary of changes | Approved by |
|---------|------|--------------------|-------------|
| v1.0    |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |
|         |      |                    |             |



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](http://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-template\_101426