EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 24, 2026

M-26-15

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Execution of the Migration to Post-Quantum Cryptography

## 1. OVERVIEW

The Executive Order *Securing the Nation Against Advanced Cryptographic Attacks*[1] (June 22, 2026), affirms the United States' leadership in the quantum revolution by accelerating the migration of Federal Government systems to post quantum cryptography (PQC). This memorandum implements that accelerated migration and advances the objective, as described in President Trump's Management Agenda, to "defend against and persistently combat cyber enemies."[2] It also fulfills the Office of Management and Budget's (OMB's) responsibility under the Quantum Computing Cybersecurity Preparedness Act (the Act)[3] to issue guidance directing each agency to prioritize critical information technology (IT) for migration to post-quantum cryptography (PQC) and to develop a plan for that migration.

This memorandum does not apply to national security systems.[4]

## 2. BACKGROUND

For decades, strong cryptography has enabled the United States Government to protect Federal information, securely deliver critical services to the American people, and guard against cyber-enabled fraud. Americans depend heavily on encryption to protect their individual privacy and for everyday tasks such as starting their cars, paying for groceries, and messaging friends and family. Accordingly, the Trump-Vance Administration has made support of strong cryptography throughout the Government and private sector a priority.

---

[1] Available at https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/.
[2] Available at https://www.whitehouse.gov/wp-content/uploads/2025/12/M-26-03-Presidents-Management-Agenda.pdf.
[3] Pub. L. No. 117-260, § 4(c) (2022) (6 U.S.C. § 1526 note).
[4] For the purposes of this memorandum, "national security system" has the meaning given in 44 U.S.C. § 3552(b)(6).

A quantum computer of sufficient power and sophistication (a cryptographically relevant quantum computer, or CRQC) will be able to decrypt data protected by many forms of cryptography that are commonly used today and thwart existing authentication protocols. After defeating such protections, a CRQC could take control of or impersonate devices, systems, and people. A CRQC is not yet known to exist, but steady advancements in the quantum computing field may yield a CRQC in the coming decade. The United States must be a leader in harnessing the numerous benefits that quantum computers will offer in fields ranging from pharmaceuticals to materials science while preparing for their ability to break widely used cryptographic algorithms.

Unlike classical public-key cryptography, PQC uses algorithms believed to be sufficiently secure even against quantum computers. The United States has led the way in the development of these algorithms through a 10-year standardization process conducted by the National Institute of Standards and Technology (NIST). Through this process, many of the world's most respected cryptographers and security researchers have thoroughly evaluated candidate algorithms to determine whether they could be compromised or broken by a CRQC.

## 3. REQUIRED AGENCY ACTIONS

### *A. Action One:*

Agencies must execute a prioritized migration of cryptographic systems used in information systems that they own or operate with the objective of mitigating as much quantum risk as feasible by December 31, 2030. To execute this migration effectively, agencies must integrate PQC readiness and implementation functions into their existing governance structures. Agencies should ensure that their migration strategy aligns with existing principles of cybersecurity governance, including comprehensive asset management and managed supply chain risk.

### *B. Action Two:*

Agencies must develop and submit a PQC Migration Plan to OMB and the Office of the National Cyber Director (ONCD), no later than 120 days from the date of this memorandum. See Subsection D for more detailed requirements.

### *C. Further Guidance and Considerations:*

1. Agency-Wide Governance and Roles

Agencies must establish or update an internal governance structure to oversee PQC migration. This migration is *not* only the responsibility of the agency-level Chief Information Officer (CIO) and Chief Information Security Officer (CISO). Instead, a successful migration requires accountability and responsibility for each member of an agency's leadership teams, both in the front office and in agency components. Roles and responsibilities must be clearly defined. Appendix B to this memorandum provides examples of appropriately delineated roles and responsibilities.

2. Risk-Based Prioritization

Agencies must prioritize PQC migration based on risk and plan accordingly. For the purposes of this memorandum, agencies must prioritize the following in their migration plans:

- A high impact system;[5]
- A High Value Asset (HVA);[6]
- Any other system with highly-sensitive data or systems that an agency determines is likely to be particularly vulnerable to CRQC-based attacks.[7] Agencies should include information systems or components that:
  - Are logical access control systems based in asymmetric encryption (such as Public Key infrastructure) that use any of the algorithms listed in Appendix A of this memorandum; or
  - Contain data expected to remain mission-sensitive in 2030.

3. System Modernization

OMB Circular No. A-130 requires agencies to "consider information security . . . for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed." Migration to PQC must be a primary information security consideration for agencies.

Through their inventories, agencies have already identified legacy systems for which migration would be too difficult or costly. Agencies must incorporate PQC upgrades into planned cloud migrations, software development lifecycles, and hardware-refresh schedules to maximize efficiency and minimize costs. Systems incapable of supporting PQC or hybrid cryptography must be identified and given priority for replacement or decommissioning.

Additionally, within 60 days of this memorandum's publication, the General Services Administration (GSA) will establish an inter-agency working-group on modernizing Federal Identity, Credential, and Access Management (FICAM) to support PQC.

4. Vendor and Third-Party Software

Agencies should reference the Cybersecurity and Infrastructure Security Agency (CISA) publication "Product Categories for Technologies That Use Post-Quantum

[5] Defined by National Security Memorandum 10 (NSM-10), *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (May 2022), as "an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards (FIPS) 199 potential impact value of 'high.'"
[6] As defined in OMB Memorandum M-19-03 or successor policies.
[7] Agencies are encouraged to consult with CISA to help make these determinations.

Cryptography Standards"[8] and should ensure that any requirements for products used by the agency in those categories include PQC integration.

Agencies should engage their FedRAMP-authorized cloud service providers to delineate PQC migration responsibilities within the shared responsibility model. CISA and the Department of War (DOW), in coordination with GSA, will lead PQC migration efforts for FedRAMP-authorized cloud service providers as well as software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) solutions that are used at more than one agency.

5. Making Use of Automation

Given the scale and complexity of Federal IT environments, manual approaches to discovery and management of cryptography are often insufficient. Agencies should use automation when feasible and appropriate to achieve a comprehensive and continuously updated understanding of their cryptographic posture. Automation is critical for inventory management, policy enforcement, and compliance reporting. Agencies should consider engaging their providers of cybersecurity services to determine if they offer automated solutions.

### *D. Plan Submission*

Each agency must develop and submit a PQC Migration Plan to OMB and ONCD no later than 120 days from the date of this memorandum. The plan should be treated as a dynamic document that will mature over time. The plan should treat migration as a multi-year effort executed in phases:

- **Phase 1 (Strategy, Planning, and Discovery – 2026 - 2027):** The initial period should focus on inventory (including HVAs and high impact systems), assessment, strategy definition, awareness and training, and development of further plans for migration. During this phase, agencies should also establish governance frameworks, designate accountable officials, and assess relative risk to lay the foundation for a phased PQC migration approach.

- **Phase 2 (Pilots and Early Migration – 2027 - 2028):** The subsequent period should focus on pilots,[9] executing early migrations of prioritized systems, and refining the migration plan based on lessons learned.

- **Phase 3 (Prioritized Migration – 2028 - 2030):** The prioritized migration phase should migrate to the use of PQC for key establishment all HVAs, high impact systems, systems with highly sensitive data, and systems that an agency

[8] Available at https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards.
[9] GSA's FICAM Office is working with interested Federal agencies to test PQC-ready physical and logical access systems. Agencies interested in participating can contact icam@gsa.gov.

determines are likely to be particularly vulnerable to CRQC-based attacks.[10] Ensure all systems are cryptographically agile.

- **Phase 4 (Signature Migration – 2031):** The signature migration phase should migrate to the use of PQC for digital signatures all HVAs, high impact systems, systems with highly sensitive data, and systems that an agency determines are likely to be particularly vulnerable to CRQC-based attacks.[11] Ensure that all systems are cryptographically agile.

- **Phase 5 (Full Migration – 2035):** The final phase should focus on completing the migration of remaining systems with consideration based on risk assessment and the availability of commercial offerings by 2035.

Agencies must align their plans with NIST Internal Report (IR) 8547, *Transition to Post-Quantum Cryptography Standards*, or successor document.[12]Descriptions of required plan sections can be found in Appendix B of this memorandum. Agencies must submit their plans to PQC@omb.eop.gov.

## 4. COORDINATION AND SUPPORT

OMB, ONCD, NIST, and CISA will continue to support PQC migration through the PQC Migration Working Group, agency-specific consultations, and technical publications. OMB, in coordination with ONCD, will assess agency-wide progress and release further guidance as needed based on evolving standards, risk environment, and implementation maturity.

**Contact Information:** For questions or support, agencies should contact the Office of the Federal Chief Information Officer at PQC@omb.eop.gov.

[10] For more information on key establishment, see NIST FIPS 203, "Module-Lattice-Based Key-Encapsulation Mechanism Standard."
[11] For more information on digital signatures, see NIST FIPS 186-5, "Digital Signature Standard (DSS)."
[13] Agencies should work with CISA and vendors of products that utilize asymmetric algorithms not enumerated in this table to determine if those algorithms are quantum-vulnerable. Agencies are encouraged to treat as quantum-vulnerable any asymmetric algorithm that is not definitively known to be quantum-resistant.

# Appendix A: Technical Implementation Guidance

## 1. PQC ALGORITHM SELECTION

### *1. FIPS 203 ML-KEM (Key Encapsulation Mechanism (KEM)/Encryption)*

Pros:
Efficient, moderate key sizes, widely recommended for near-term PQC needs.

Cons:
Larger overhead than classical Elliptical Curve Technology (ECC).

Future Considerations:
Might see additional parameter sets or improvements in speed/size.

### *2. FIPS 204 ML-DSA (Digital Signature Algorithm)*

Pros:
Balanced performance for signatures, solid lattice foundation.

Cons:
~1–2 KB signatures can strain bandwidth in certain use cases.

Future Considerations:
NIST may finalize new lattice optimizations or next-generation signature variants.

### *3. FIPS 205 SLH-DSA (Digital Signature Algorithm)*

Pros:
Hash-based approach, robust fallback independent of lattice/code assumptions.

Cons:
Larger signatures (tens of KB), slower signing.

Future Considerations:
Parameter refinements may reduce size or increase speed; new hash-based algorithms might appear.

### *4. Future Standards*

Notably, additional signature or KEM schemes may be announced in the future as part of continuing efforts to standardize more signature algorithms beyond the initial set. If future cryptanalysis reveals weaknesses or improvements, NIST might recommend different parameter levels (e.g., higher security, smaller keys) such as FALCON and HQC.

## 2. QUANTUM-VULNERABLE ALGORITHMS

| Algorithm | Function | Specification |
|---|---|---|
| Elliptic Curve Diffie-Hellman (ECDH) Key Exchange | Asymmetric algorithm used for key establishment | NIST SP 800-56A/B/C |
| Menezes-Qu-Vanstone (MQV) Key Exchange | Asymmetric algorithm used for key establishment | NIST SP 800-56A rev3 |
| Elliptic Curve Digital Signature Algorithm (ECDSA) | Asymmetric algorithms used for digital signatures | FIPS PUB 186-5 |
| Diffie-Hellman (DH) Key Exchange and variants | Asymmetric algorithm used for key establishment | NIST 800-56A rev3 |
| Rivest-Shamir-Adleman (RSA) Signature Algorithm | Asymmetric algorithm used for signatures | FIPS SP 800-56B rev 1 |
| RSA Key Establishment | Asymmetric algorithm used for key establishment | SP 800-56B rev1 |
| Digital Signature Algorithm | Asymmetric algorithm used for digital signatures | FIPS 186-5 |
| Other non-PQC Asymmetric Algorithms[13] | Remaining asymmetric algorithms not enumerated in the list above | Not applicable |

Symmetric-key-based protocols should also be avoided.

## 3. HYBRID ARCHITECTURE

A hybrid architecture[14] is an implementation model that combines a traditional cryptographic algorithm, such as ECDH or ECDSA, with a PQC algorithm, such as FIPS 203 ML-KEM or FIPS 204 ML-DSA. Compromising the security of the operation requires an attacker to break both the classical and the PQC schemes if properly implemented. This model can be a useful tool for managing risk during the migration from traditional to post-quantum cryptographic systems; however, because it introduces its own risks and complexities, agencies considering this approach should perform a thorough evaluation of its tradeoffs, as it is an intricate and resource-intensive stopgap.

- For Key Exchange: In a hybrid key exchange, the client and server generate two sets of public/private keys—one traditional and one PQC. The resulting shared secrets are cryptographically combined (e.g., through the use of a key derivation function taking both as inputs) to derive the final session keys.

- For Digital Signatures: A hybrid signature involves creating two distinct signatures on the same data—one with a traditional algorithm and one with a PQC algorithm. The verifier

[13] Agencies should work with CISA and vendors of products that utilize asymmetric algorithms not enumerated in this table to determine if those algorithms are quantum-vulnerable. Agencies are encouraged to treat as quantum-vulnerable any asymmetric algorithm that is not definitively known to be quantum-resistant.
[14] For more information, see NIST IR 8547, available at https://csrc.nist.gov/pubs/ir/8547/ipd.

must validate both signatures for the data to be considered authentic.

The purpose of this model is to provide defense-in-depth against both traditional and quantum computing threats and in some cases maintain interoperability. Agencies may choose to implement hybrid architectures based on their own risk assessments and technical requirements.

## 4. THE ROLE OF TLS 1.3 IN PQC MIGRATION

Consistent with Executive Order 14306, agencies must support Transport Layer Security (TLS) protocol version 1.3 or a successor version as soon as practicable, but not later than January 2, 2030. TLS 1.3 is foundational for deploying PQC at the network level. Its redesigned handshake is more efficient and extensible than those of its predecessors, making it well-suited for implementing a hybrid key exchange model when needed.

The standard mechanism for a hybrid key exchange in TLS 1.3 is as follows:

1. ClientHello: The client signals its support for a hybrid key exchange by sending key shares for *both* a traditional group (e.g., x25519) and a PQC KEM (e.g., FIPS 203 ML-KEM-768) in the key_share extension.
2. ServerHello: If the server supports the proposed hybrid scheme, it generates its own corresponding key shares and sends them back in its key share extension.
3. Key Derivation: Both the client and server now independently compute two shared secrets—one from the classical exchange and one from the PQC exchange. These two secrets are then combined (e.g., concatenated) and used as the input to the TLS 1.3 key derivation function to generate the session's traffic keys.

This mechanism ensures that the session's security relies on the hardness of both the traditional and quantum-safe problems.

## 5. CRYPTOGRAPHIC AGILITY

Cryptographic agility[15] is an architectural principle that enables an organization to switch its cryptographic algorithms with minimal disruption. It is essential for responding not only to the quantum threat but also to any future cryptographic vulnerability (or to take advantage of any performance breakthroughs with new cryptography, such as when RSA use began to diminish in favor of elliptic curve cryptography). Achieving cryptographic agility requires more than simply avoiding hardcoded algorithm names. It may also require one or more of the following:

- Use Modern Cryptographic Libraries: Draw on frameworks explicitly designed for agility. For example, OpenSSL 3.x uses a "provider" architecture that allows new algorithm implementations to be plugged in and selected via configuration. Similarly, Java's JCA/JCE allows for the registration of different cryptographic providers.

- Implement Configuration-Driven Cryptography: The choice of which algorithm or hybrid scheme to use must be specified in external configuration files, not compiled into the

[15] For more, see https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/final.

application binary. This allows administrators to update the cryptography of a running service without needing a new software release.

- Design for Cipher Suite Negotiation in Protocols: Where possible, communication protocols should include fields for negotiating cryptographic capabilities. This allows endpoints to discover mutual support for PQC and gracefully transition away from older algorithms. To avoid downgrade attacks, ensure that devices can be configured to use only acceptable algorithms.

- Ensure an Agile Key Management Infrastructure: The systems responsible for managing cryptographic keys (Key Management Service (KMS), Hardware Security Module (HSMs)) must also be agile. They must be able to generate, store, and manage different types of keys (e.g., both ECC and PQC keys) and support the new PQC algorithms natively.

## 6. LEVERAGING AUTOMATION FOR DISCOVERY AND ENFORCEMENT

Manual processes are often inadequate for a migration of this scope. Agencies should take advantage of automation for discovery, policy enforcement, and compliance.

- Automated Cryptographic Inventory: The foundation of the migration plan is a dynamic, continuously updated inventory of all cryptographic assets. This inventory should be created and maintained through automated tools wherever possible, including by use of Software Composition Analysis (SCA) to analyze Software Bills of Materials (SBOMs), Static/Dynamic Application Security Testing (SAST/DAST) to find cryptographic functions in code, and network scanners to detect protocols and cipher suites. This data should populate a central Cryptographic Bill of Materials (CBOM) to provide a real-time view of the agency's cryptographic posture.

- Automated Compliance and Monitoring: Data from the automated inventory and policy checks, when possible, should feed directly into dashboards for continuous monitoring. These dashboards can track migration progress against agency timelines, and provide metrics for leadership and compliance reports.

## 7. INTEGRATING PQC INTO A ZERO TRUST ARCHITECTURE

PQC is a foundational dependency for advancing a durable zero-trust architecture (ZTA) into an optimal state as defined by the CISA ZTA Maturity Model. The core ZTA principle of “never trust, always verify” is compromised if the cryptography used for verification is vulnerable. PQC must be integrated across the ZTA pillars.

- Devices: ZTA demands strong validation of device health and identity before granting access. Cryptographic device attestation, often rooted in a Trusted Platform Module (TPM), must be migrated to PQC algorithms to prevent device spoofing. Agencies must procure physical access control systems that are included on the GSA maintained

Approved Products List.[16]

- Networks: The ZTA tenet of "encrypt all traffic" relies on secure protocols. All network infrastructure that terminates TLS or IPsec sessions or other relevant protocols—including firewalls, Virtual Private Network concentrators, cloud gateways, and Application Programming Interface (API) proxies—must be configured to support PQC-capable key exchanges that utilize NIST PQC algorithms. Ideally, such terminators should be located architecturally as close to the endpoint as feasible to minimize the risk of their exploitation.

- Applications and Workloads: ZTA requires secure inter-service communication, often achieved with signed API requests or tokens (e.g., JavaScript Object Notation Web Tokens (JWTs)). API gateways and application workloads must be configured to issue and validate PQC-signed tokens. Secure software development practices must mandate the use of PQC-agile libraries for all new applications.

- Data: Data must be protected at rest and in transit. Agencies must prioritize identifying and re-encrypting long-lived sensitive data using keys protected by PQC mechanisms. Data Loss Prevention (DLP) and other data-centric security tools must be updated to recognize and properly handle PQC-protected data.

[16] Available at https://www.idmanagement.gov/fips201.

## Appendix B: Sample Allocation of Responsibilities and Planning Requirements

### 1. RESPONSIBILITIES

| | |
|---|---|
| **Chief Information Officer and Chief Information Security Officer** | Accountable for prioritization, risk acceptance, and resource allocation. |
| **Program Office or Requirement Owner** | Ensures vendor requirements include PQC-readiness and cryptographic agility provisions. |
| **Chief Financial Officer** | Works with the CIO and CISO, in collaboration with PQC Migration Program Manager, to ensure that PQC migration resource requirements are accurately represented in the agency's annual budget request. |
| **PQC Cryptographic Inventory and Migration Lead/Migration Program Manager** | Coordinates agency-wide migration activities, ensures plan alignment, and reports to senior leadership. |
| **PQC Technical Lead** | Oversees inventory, algorithm selection, testing, and deployment of PQC (and if implemented, hybrid cryptography) |
| **Security Architect** | Integrates PQC into ZTA components and supports interoperability planning. |
| **Application and System Owners** | Responsible for implementation of crypto-agile and PQC-compatible technologies of their owned systems. |

### 2. AGENCY MIGRATION PLAN REQUIREMENTS

The initial plan submission described on page 4 of the main body of this memorandum must contain, at a minimum:

- A system prioritization strategy with risk-based justification;
- Timelines and milestones to achieve all three migration phases;
- Timelines and milestones for testing and deployment to meet the TLS 1.3 support deadline established by this memorandum;
- The methodologies and automated tools used for the cryptographic inventory;
- A plan for implementing a cryptographic agile architecture;
- A third-party coordination plan;
- An estimate of funding and personnel resources required;
- A risk management strategy for the migration period; and
- A section defining governance roles and responsibilities.