Preparing for the Post-Quantum Era

Best Practices for Federal Agencies

Theodore Noah, Post-Quantum Cryptography Transition Architect, Maveris and Rod Fontecilla, Ph.D., Chief Innovation and AI Officer, Harmonia

Unlike classical computers that process information sequentially using binary states (1's and 0's), quantum computers leverage quantum mechanical properties such as superposition and entanglement to perform parallel calculations at unprecedented scales. This quantum advantage enables them to solve certain mathematical problems exponentially faster than classical systems. This ability will make traditional encryption algorithms including RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) vulnerable to attack and essentially obsolete.

The transition to post-quantum cryptography (PQC) is not merely a technical upgrade, it represents a fundamental shift in how federal agencies must approach cybersecurity. With experts projecting that cryptographically relevant quantum computers (CRQCs) may emerge within the next decade, agencies cannot afford to delay preparation.

As far back as 2022, the National Security Memorandum 10 (NSM-10) mandated that all federal agencies begin implementing PQC standards to protect vulnerable systems before quantum threats materialize. The cyber-focused Executive Order 14306 issued in June of 2025 directed the National Security Agency and the Office of Management and Budget to issue government agency standards for PQC by December 2025 so that tougher security protections are in place by 2030.

In this whitepaper we'll detail three critical requirements established by federal PQC guidance:

Asset Inventory and System Assessment

The foundation of any successful post quantum cryptography (PQC) transition begins with a comprehensive understanding of an organization's cryptographic landscape. OMB M-23-02 provides detailed guidance for conducting systematic inventories that identify systems vulnerable to quantum attacks.

Federal agencies must catalog all systems that rely on public-key cryptography, with particular emphasis on high-value assets (HVA) and FISMA high-impact systems. This inventory process requires collaboration between cybersecurity teams, system administrators, and business process owners.

Look beyond IT

The inventory process should extend beyond obvious cryptographic applications to include embedded systems, Internet of Things (IoT) devices, and legacy infrastructure that may contain hidden cryptographic dependencies.

For example, a federal building's HVAC system may use IoT sensors that authenticate to the network using RSA certificates, while legacy industrial control systems may rely on embedded cryptographic modules for secure communications that are not immediately apparent to IT teams. Similarly, network printers, surveillance cameras, and even elevator control systems often contain cryptographic components that could be vulnerable to quantum attacks. Documentation should include detailed technical specifications, vendor information, maintenance schedules, and interdependencies between systems. This comprehensive mapping enables agencies to prioritize migration efforts based on risk levels and operational impact, ensuring that the most critical systems receive attention first while maintaining continuity of essential services.

Comprehensive mapping supports prioritization

In documenting the cryptographic algorithms currently in use, agencies should also note their implementation contexts, data sensitivity levels, and operational criticality. Documentation should include detailed technical specifications, vendor information, maintenance schedules, and interdependencies between systems.

This comprehensive mapping enables agencies to prioritize migration efforts based on risk levels and operational impact, ensuring that the most critical systems receive attention first while maintaining continuity of essential services.

Vendor Communication and Supply Chain Management

Engaging Vendors to Prepare Your Supply Chain for the Post-Quantum Era

Effective stakeholder outreach to vendors is essential for gathering detailed cryptographic information about commercial products and services. As agencies are encouraged to rely more and more on Commercial Off-The-Shelf (COTS) solutions, ongoing vendor communication becomes even more critical, requiring regular touchpoints with suppliers to monitor progress and ensure alignment with federal timeline requirements. Agencies must proactively engage with their technology suppliers to understand current cryptographic implementations and future post-quantum roadmaps.

Effective stakeholder outreach to vendors is essential for gathering detailed cryptographic information about commercial products and services.

The vendor engagement process requires a nuanced approach that recognizes the diverse landscape of technology suppliers. Large enterprise vendors may already have established PQC strategies, while smaller specialized vendors may lack awareness of quantum threats entirely. Agencies must tailor their communication strategies accordingly, providing education and support where needed while demanding accountability and transparency from all suppliers.

Developing a communication strategy

This communication strategy should begin with updating contract language and service level agreements to include specific post quantum cryptography (PQC) requirements and compliance expectations. For example, contracts should specify that vendors must provide migration roadmaps by a certain date, implement NIST-approved PQC algorithms within defined timeframes, and maintain system security throughout the transition period. Service level agreements might include requirements for vendors to notify agencies within 30 days of any changes to their PQC implementation timelines or if quantum vulnerabilities are discovered in their products. Additionally, agencies should request detailed surveys or comprehensive roadmaps that demonstrate how vendors are preparing for the PQC transition, including timelines for algorithm updates, testing procedures, and migration support services.

PQC as part of supply chain strategy

Integration with existing supply chain risk management processes is also crucial for success. PQC considerations should be seamlessly incorporated into established workflows, including requesting specific timelines, understanding technical dependencies, and evaluating vendor capacity to support migration efforts. Agencies should leverage Software Bills of Materials (SBOMs) to identify cryptographic components not only in primary systems but also in third-party libraries, dependencies, and subcomponents that may contain quantum-vulnerable algorithms. This component-level visibility is essential because cryptographic vulnerabilities can exist deep within supply chains, requiring agencies to understand the complete cryptographic footprint of their technology stack, not just surface-level implementations.

Creating a communication framework

We recommend developing a framework that outlines how system owners for COTS solutions discuss PQC migration with their systems vendors. This should be done during the inventory and discovery phase to identify critical dependencies, hardware, and infrastructure needs. An organization's Supply Chain Risk Management should consider making updates to their annual third-party assessment process and conduct surveys with solution providers on their roadmap and current programs on the plan to meet PQC compliance.

Budgeting and Cost Projections

Budgeting for a PQC Future

Accurate cost estimation for post quantum cryptography (PQC) transitions is not only a financial planning requirement but also a federal mandate under NSM-10, which requires agencies to provide cost estimates for updating or replacing systems to meet future cryptography standards. This budgeting requirement ensures agencies can secure adequate funding and avoid mission disruptions due to insufficient resources during the quantum transition.

Developing accurate cost estimates for PQC transitions requires comprehensive analysis of multiple interconnected factors that extend far beyond simple technology replacement costs.

Developing accurate cost estimates for PQC transitions requires comprehensive analysis of multiple interconnected factors that extend far beyond simple technology replacement costs.

Direct technology costs typically include new hardware capable of supporting PQC algorithms, updated software licenses, and professional services for system integration and testing. However, these visible expenses often represent only a fraction of total transition costs. Agencies must also account for workforce development, including specialized training for cybersecurity professionals, system administrators, and end users who will interact with new cryptographic systems.

Beyond these technology expenses, operational considerations significantly impact cost projections. Agencies must account for potential system downtime during migrations, parallel operation requirements during transition periods, and ongoing maintenance of hybrid cryptographic environments. Risk mitigation strategies also carry financial implications, including enhanced monitoring capabilities, incident response preparations, and contingency planning for accelerated migration timelines if quantum threats emerge earlier than expected.

Long-term operational costs must be factored into financial planning, including increased computational requirements for post-quantum algorithms and enhanced key management systems. Agencies should make an effort to build a framework that provides considerations to factor many, if not all, of these costs when developing cost projections for migration to PQC.

Migration Planning and Strategic Considerations to Lead in the Post-Quantum World

Successful post quantum cryptography (PQC) migration requires careful orchestration of asset discovery, technical upgrades, operational procedures, and organizational change management. Agencies must develop comprehensive migration strategies that balance security requirements, operational continuity, and resource constraints while maintaining mission-critical capabilities throughout the transition period. As agencies develop their migration plans, the following elements are critical:

- Risk-based prioritization allows agencies to consider both quantum vulnerability and operational criticality. Systems protecting the most sensitive data or supporting essential mission functions should typically receive priority, while lower-risk applications may be addressed in later implementation phases.
- Testing and validation procedures are critical components of migration planning, requiring comprehensive evaluation of PQC algorithms in operational environments before full deployment.
- Change management considerations include user training programs, updated operational procedures, and communication strategies that help stakeholders understand the importance and implications of PQC transitions.
- Contingency planning should address potential acceleration scenarios where quantum threats emerge more rapidly than anticipated, requiring compressed migration timelines and emergency response procedures.
- Hybrid implementation strategies often provide the most practical approach for large-scale migrations, allowing agencies to gradually transition from classical to PQC cryptography while maintaining operational capabilities.

How to Lead on PQC

The transition to PQC represents one of the most significant cybersecurity challenges facing federal agencies in the coming decade. Federal leadership in PQC preparedness not only protects government operations but also sets important precedents for private sector adoption and international cooperation. Success requires proactive planning, comprehensive preparation, and sustained organizational commitment to implementing new cryptographic standards before quantum threats materialize.

The transition to PQC represents one of the most significant cybersecurity challenges facing federal agencies in the coming decade.

At the U.S. Department of Veterans Affairs (VA), we are actively working to support this transition through our work in conducting thorough asset inventories, establishing effective vendor communication strategies, and developing accurate cost projections. These foundational contributions are intended to help the VA achieve an orderly, secure, and successful post-quantum transition.

The quantum transition timeline remains uncertain, but the imperative for preparation is clear. Agencies that begin comprehensive planning efforts today will be best positioned to maintain mission-critical capabilities while meeting federal compliance requirements. We can help guide you through that process, with our proven experience and documented framework.

To begin talking through your PQC future, contact tic@harmonia.com.