

Defining a Practical Path to Post-Quantum Cryptography

Public-key encryption like RSA and ECC currently secure the world's global data, including the personal and financial systems that we rely on for security. But the moment when quantum computers become powerful enough to break this public encryption ("Q-day") looms, forcing a new standard as quantum-enabled threats rise and the timeline to prepare shrinks. The common approach of "harvest now, decrypt later" is a risk management issue and government mandated timelines for Post-Quantum Cryptography (PQC) leave no room for error. Delays increase both exposure and cost and threaten to disrupt an organization's progress in Zero Trust.

Getting Clarity on the Path to PQC

Organizations that are moving to meet these PQC mandates must first define clear objectives and evaluate legacy and embedded cryptographic algorithms as well as manual and automated inventory. Resource allocation and cultural resistance are also critical factors to the success of new PQC initiatives. This is often a cumbersome task, with manual inventories, legacy PKI systems, and limited tooling making it difficult to know where to start, especially as the threat landscape continues to change. Red River provides expert diagnostics and guidance to facilitate this process and support organizations in defining and executing on their unique path to PQC.

Red River's PQC Accelerator Streamlines Readiness

Red River's Post-Quantum Cryptography Accelerator provides a practical, workshop-based engagement that helps organizations:

- Understand PQC threats and mandates
- Identify where quantum-vulnerable encryption exists in your environment
- Prioritize high-value assets and long-term data
- Build a tailored, actionable roadmap aligned with OMB M-23-02, FIPS 203–205, and Zero Trust requirements



The OMB is estimating an **investment of \$7.9 Billion in Federal PQC compliance** to protect high value data types that must remain confidential for 10-30+ years including:

- Healthcare records (PHI)
- Genomic and research data
- National security and law-enforcement data

PQC Timeline Requirements

- **2023**
Cryptography Inventory Begins
Agencies must submit a prioritized inventory of systems using quantum-vulnerable cryptography.
(OMB M-23-02 — annual reporting through 2035)
- **2030**
Transition Key Establishment Mechanisms
(e.g., ML-KEM) For High Value Assets and High Impact Systems
- **2031**
Transition Digital Signature Algorithms
(e.g., ML-DSA) For High Value Assets and High Impact Systems
- **2035**
Full PQC Migration Target
U.S. federal government completes transition to quantum-resistant cryptography.

Strategy & Planning from Experts in PQC Execution

Red River's data management and cybersecurity experts provide guidance across critical steps in PQC planning to deliver a custom roadmap that supports your organization's mission.

Key Elements of the PQC Accelerator include:



Educational Workshop to Align Internal Teams

Align stakeholders, explain PQC threats, mandates and provide guidance on essential concepts around crypto-agility.



Data Collection to Determine Current State PQC Maturity

Administer in-depth questionnaire and conduct discovery of TLS endpoints, cert chains, PKI, apps, VPNs and data at rest to understand current tooling.



PQC Dynamic Roadmap to Align with Agency Priorities

Deliver a custom, structured roadmap that prioritizes HVAs, aligns to FIPS 203–205 and OMB M-23-02 and defines mitigations.



OEM Mapping & Testing

Identify PQC-ready solutions and validate integrations to provide a pilot and deployment support.

PQC Naturally Complements Other Federal Priorities in Cyber

Zero Trust

PQC strengthens encryption requirements.

Compliance & Reporting

PQC supports mandated cryptographic inventories & migration plans.

IT Modernization

New hardware/software implementations improve cyber posture.

PQC Roadmap At-a-Glance



CRAWL

Initial inventory using existing tools



WALK

Focused HVA and long-retention data mapping



RUN

Mitigate PQC risk for critical assets



FLY

Continuous automated discovery and posture

Interested in learning more? Get a no-cost, introductory PQC session (virtual or on-site) to help your team assess readiness and outline next steps at info@redriver.com.



ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, AI, cybersecurity, modern infrastructure, collaboration and cloud solutions.

Learn more at redriver.com.