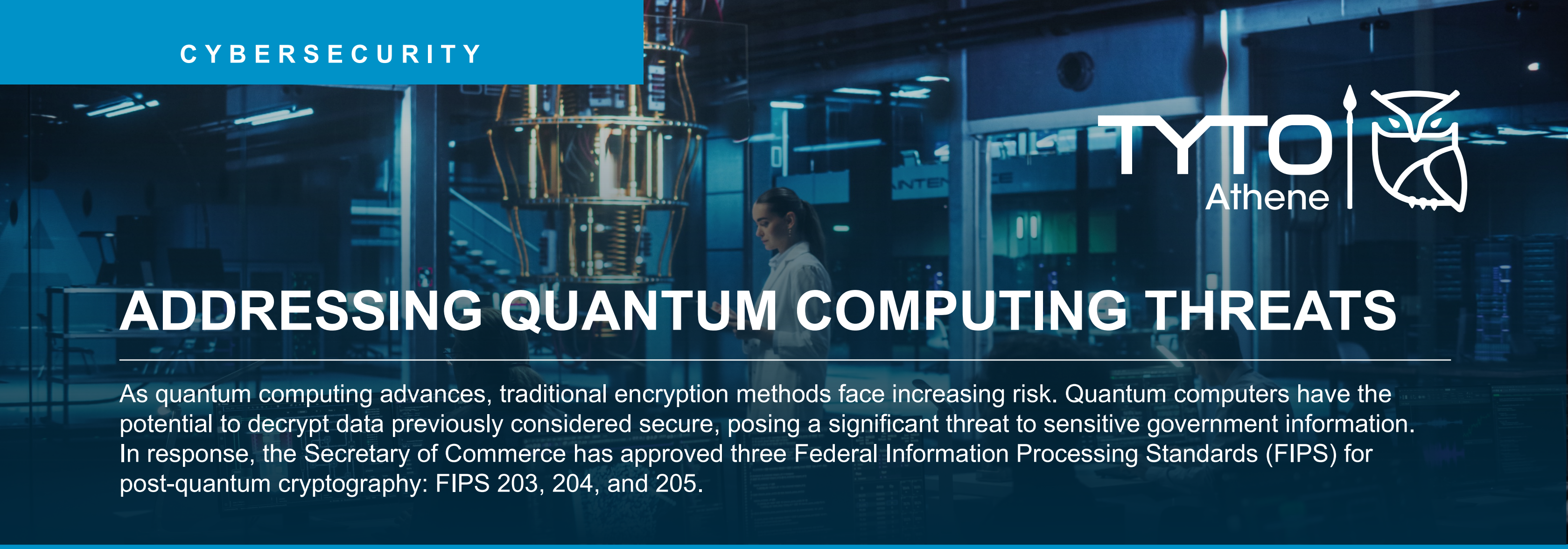
CYBERSECURITY



ADDRESSING QUANTUM COMPUTING THREATS

As quantum computing advances, traditional encryption methods face increasing risk. Quantum computers have the potential to decrypt data previously considered secure, posing a significant threat to sensitive government information. In response, the Secretary of Commerce has approved three Federal Information Processing Standards (FIPS) for post-quantum cryptography: FIPS 203, 204, and 205.

Highlights

Post-Quantum Cryptography (PQC) is the next frontier in cybersecurity, protecting your organization from the imminent threats posed by quantum computing. Tyto Athene offers a comprehensive PQC service designed to secure your systems against both quantum and conventional attacks, ensuring long-term data integrity and compliance with evolving national security standards.

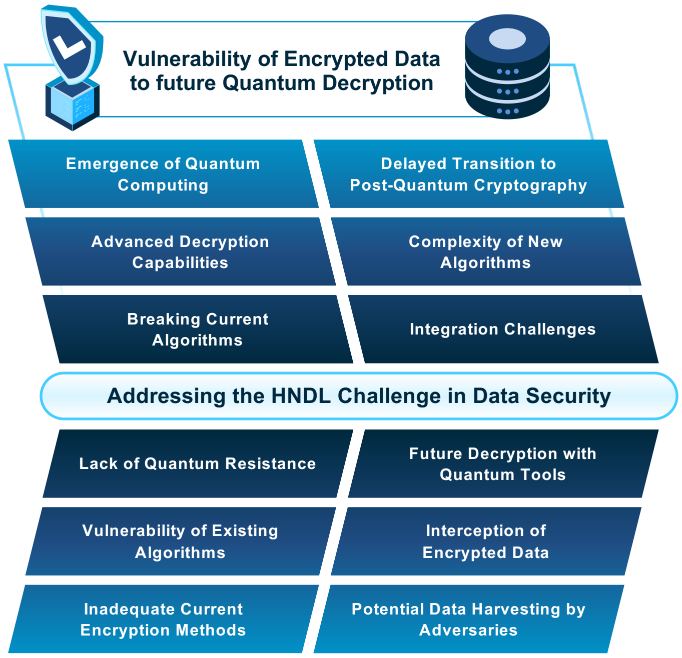
The cryptanalytic threat model has shifted from speculative to imminent. Agencies recognize harvest-now decrypt-later (HNDL) risk where adversaries intercept and store encrypted material today to decrypt later once crypto-relevant quantum compute (CRQC) capability exists. While experts estimate CRQC to become available within the next two years, HNDL is the precursor threat that exists today.

Moving to PQC requires compatibility and interoperability with existing systems, many of which are legacy systems in government and enterprise organizations.

The shift to PQC demands skilled personnel with expertise in quantum computing and advanced cryptography. Existing IT staff often need extensive retraining to handle the new algorithms and understand PQC's implications on system design and risk management. Organizations also face challenges in establishing a centralized encryption policy and ensuring compliance, especially within departments where roles and responsibilities differ significantly.

Key Benefits of Quantum-Resistant Security

- **Enhanced Protection for Government and Sensitive Data**
  Safeguards critical information from quantum decryption threats, ensuring secure data storage and communication for years to come.
- **Compliance with Industry Standards**
  Meets Federal Information Processing Standards (QCCPA, EO14028,EO13800 and NSM-10, enabling trusted, government-grade security.
- **Future-Proof Encryption**
  Provides robust data security to address both current and future advancements in quantum computing.
- **Minimal Operational Disruption**
  Phased integration approach ensures that PQC implementation fits seamlessly with existing systems, reducing impact on daily operations.
- **Comprehensive Support and Training**
  Empowers internal teams with the knowledge and skills necessary to manage post-quantum cryptography securely and effectively.


Vulnerability of Encrypted Data to future Quantum Decryption

Emergence of Quantum Computing

Delayed Transition to Post-Quantum Cryptography

Advanced Decryption Capabilities

Complexity of New Algorithms

Breaking Current Algorithms

Integration Challenges

Addressing the HNDL Challenge in Data Security

Lack of Quantum Resistance

Future Decryption with Quantum Tools

Vulnerability of Existing Algorithms

Interception of Encrypted Data

Inadequate Current Encryption Methods

Potential Data Harvesting by Adversaries

PQC BOM Builder App

Tyto Athene has developed a tool to validate the current state of TLS 1.3 deployment to predict interim safety of your existing services.

In support of requirements to provide a PQC SBOM development is underway to build an automation scanning tool that will survey customer environments to assemble an SBOM for existing encryption hardware, software and algorithms. It will also help assess the hygiene of the PKI infrastructure.

Risks of Delayed Action on PQC Readiness

If government leaders fail to act on PQC readiness, the implications are profound. The four most significant risks are:

Mission and National Security Compromise

Adversaries with quantum capability could break today’s encryption, exposing classified systems, defense communications, and intelligence networks.

Data Harvest Now, Decrypt Later Attacks

Sensitive government, defense, healthcare, and financial data are already being stolen and stored by adversaries. Once quantum decryption is viable, decades of protected information, including personnel records, medical histories, diplomatic cables, and weapons designs, will be exposed in bulk.

Operational and Continuity Failures

Critical infrastructure and federal systems that cannot be upgraded in time risk catastrophic outages. Agencies without a migration plan will face mission disruption, cascading failures in dependent systems, and inability to maintain trust in essential services.

Economic, Industrial, and Strategic Disadvantage

If the U.S. lags in PQC adoption, competitors will secure their ecosystems first, dictating standards and locking out American vendors. This risks eroding public trust and undermining supply chain integrity.

Challenges in Implementing Post-Quantum Cryptography (PQC)

Transitioning to PQC in large government environments involves several critical challenges:

Technical — **Ensuring compatibility, integration, performance, interoperability, and scalability.**

Business — **Addressing security risk management, cost considerations, compliance, and standardization.**

Financial — **PQC migration is resource-intensive, requiring substantial investment.**

Cultural and Human Resources — **Addressing training and skill gaps among personnel.**

Successful PQC adoption requires a well-planned approach that extends beyond technology integration, involving strategic alignment across departments and balancing operational demands with new security requirements.

The Solution: Post-Quantum Cryptography (PQC)

Integrating PQC is crucial to mitigate quantum threats. PQC solutions are designed to secure data against both quantum and classical computing risks, providing future-proofed encryption as quantum technology continues to evolve.

Future-Proof Security

Safeguard your data from quantum computing threats before they emerge. PQC is designed to withstand attacks from both conventional and quantum computers.

National Standards Compliance

Align with the latest directives from NIST and the White House's National Security Memorandum 10, ensuring your agency meets upcoming federal requirements.

Seamless, Tailored Integration

Our team of experts follow a customized transition plan tailored to your agency's unique needs and mission to ensure your PQC solutions integrate with existing systems, minimizing disruption and maintaining operational efficiency.

Tyto Athene's Approach to PQC Implementation

Quantum Encryption Readiness Assessment

- Evaluate current systems to identify vulnerabilities.
- Conduct threat analysis and inventory resources.
- Prioritize high-risk systems with a multi-faceted scoring system.

Algorithm Impact Assessment & Performance Testing

- Select and test NIST-endorsed PQC resistant algorithms.
- Align business risk profiles with data sensitivity needs.
- Validate performance to ensure a seamless user experience.

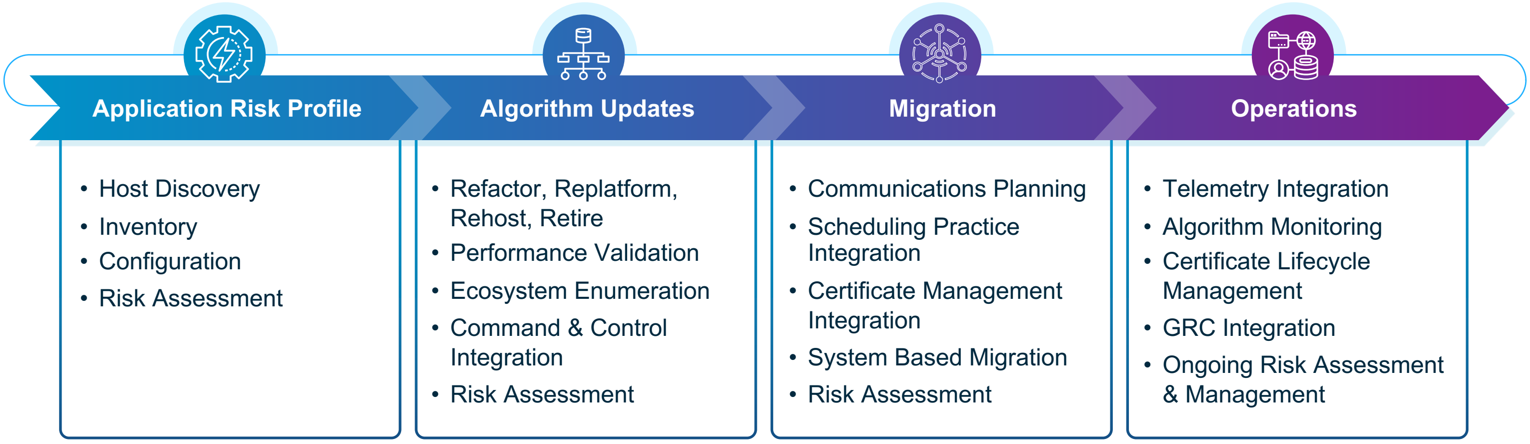
Seamless Migration & Integration

- Implement a phased migration strategy.
- Integrate PQC with SecDevSecOps pipelines.
- Train support staff to enable cross-team collaboration.

Ongoing Operations & Support

- Continuous monitoring and threat intelligence updates.
- Ensure compliance with NIST and global data protection regulations.
- Maintain scalability and performance of PQC systems.

Crypto Agility



Application Risk Profile

- Host Discovery
- Inventory
- Configuration
- Risk Assessment

Algorithm Updates

- Refactor, Replatform, Rehost, Retire
- Performance Validation
- Ecosystem Enumeration
- Command & Control Integration
- Risk Assessment

Migration

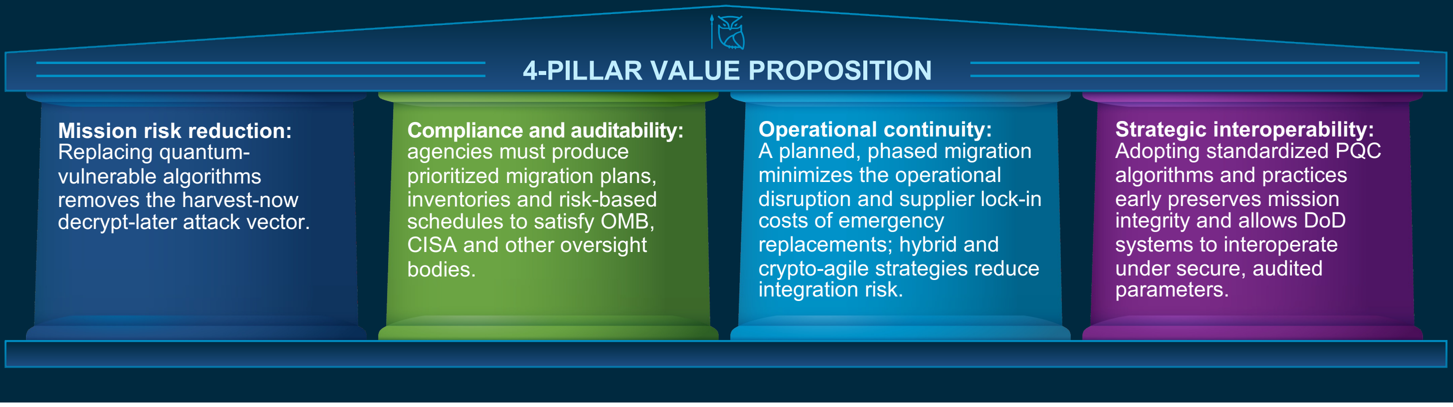
- Communications Planning
- Scheduling Practice Integration
- Certificate Management Integration
- System Based Migration
- Risk Assessment

Operations

- Telemetry Integration
- Algorithm Monitoring
- Certificate Lifecycle Management
- GRC Integration
- Ongoing Risk Assessment & Management

Why Tyto Athene?

With a proven track record in cybersecurity, Tyto Athene is uniquely positioned to guide organizations in transitioning to post-quantum cryptography. Through tailored roadmaps, expert project management, and end-to-end engineering solutions, Tyto Athene helps secure critical data and systems for the future.



4-PILLAR VALUE PROPOSITION

Mission risk reduction: Replacing quantum-vulnerable algorithms removes the harvest-now decrypt-later attack vector.

Compliance and auditability: agencies must produce prioritized migration plans, inventories and risk-based schedules to satisfy OMB, CISA and other oversight bodies.

Operational continuity: A planned, phased migration minimizes the operational disruption and supplier lock-in costs of emergency replacements; hybrid and crypto-agile strategies reduce integration risk.

Strategic interoperability: Adopting standardized PQC algorithms and practices early preserves mission integrity and allows DoD systems to interoperate under secure, audited parameters.

Future-Proof Data Security & Organizational Benefits

Tyto Athene's PQC strategy prepares organizations for both immediate and long-term cryptographic threats posed by quantum advancements.

Agility in Encryption:

Centralized policy management allows for updates as encryption standards evolve without full system overhauls.

Future-Proof Critical Systems:

Structured roadmap enables phased updates, keeping critical systems secure as PQC and regulatory needs advance.

Comprehensive Training and Knowledge:

Tyto Athene's training programs ensure internal teams are proficient in managing PQC, sustaining high security across the organization.

The Time Is Now

There are three converging drivers. First, the cryptanalytic threat model has shifted from speculative to imminent in policy terms. Agencies recognize harvest-now decrypt-later risk where adversaries intercept and store encrypted material today to decrypt later once quantum capability exists. Second, standards and policy milestones have arrived. NIST's decisions on candidate algorithms and public FIPS standards, plus White House and OMB directives and CISA/NSA guidance, create compliance timelines and expectations for federal agencies to produce migration plans. Third, vendor and product readiness is increasing. PQC primitives are being implemented and bench-tested in TLS stacks, PKI ecosystems and HSMs so migration is technically feasible now rather than purely theoretical. The aggregate effect is a narrowing window to prepare, prioritize and budget a paced migration while avoiding emergency, costly rip-and-replace in the future.

Our cryptographic and systems integration experts, along with industry leading vendors specializing in post-quantum encryption, are here to guide you through the selection and implementation phases. Migrating to PQC is crucial and demands a multi-year, multi-faceted approach to meet PQC requirements, such as M-23-02, and to protect your enterprise's digital assets from future quantum threats. Partnering with Tyto Athene and following our structured approach will ensure a seamless transition and uphold the highest standards of data security.

For more information about our cybersecurity services, please email bd@gotyto.com

https://gotyto.com

Tyto GSI is registered in System for Award Management (SAM) as a Large Business under NAICS Code 541519.

TYTO Athene

DATA TO DOMINANCE