TYTO Athene

TYTO PQC DEFENSE MATURITY MODEL

Table of Contents

TYTO PQC DEFENSE MATURITY MODEL

The federal government has adopted a proactive and urgent posture toward Post-Quantum Cryptography (PQC) readiness, recognizing that quantum computing poses an existential threat to current cryptographic standards across both civilian and national security systems. This position is anchored in a suite of legislative actions, executive orders, and memoranda—most notably the Quantum Computing Cybersecurity Preparedness Act (QCCPA), National Security Memorandum 10 (NSM-10), and recent OMB directives such as M-23-02. Together, these mandates require agencies to inventory all cryptographic assets, assess vulnerabilities, and prioritize the migration of high-value and high-impact systems to quantum-resistant algorithms. The posture extends beyond federal departments to require third-party vendors to comply with PQC standards and for agencies to aggressively test emerging PQC protocols in live environments before the 2030 government-wide transition deadline.

Strategically, the government emphasizes early risk assessment, governance, and cross-agency collaboration in its PQC transition. Agencies are required not only to report cryptographic asset inventories and vulnerabilities but also to plan for systems that cannot be upgraded. Agencies are also responsible for estimating funding endeavors and identifying resource gaps for migration efforts. OMB and the White House have built mechanisms for continuous oversight to reflect their understanding of modern best practices. This includes PQC migration working groups, and cross-coordination with organizations like NIST and CISA, to ensure agencies are in alignment with evolving standards and the advancement of attack vectors. This comprehensive, forward-leaning approach signifies a determined drive to achieve full quantum resilience across federal infrastructure before adversarial quantum attack capabilities can materialize.

Key Mandates and Legislative Actions

- **Quantum Computing Cybersecurity Preparedness Act (QCCPA):**
  Requires federal agencies to inventory cryptographic systems vulnerable to quantum computing and prepare for migration to PQC.
- **Executive Orders:**
  - **EO 14028 (Improving the Nation's Cybersecurity):** Directs agencies to implement modern encryption to explicitly highlight quantum-resistant cryptography.
  - **EO 13800:** Prioritizes federal cybersecurity resilience measures and forms the foundation for PQC transition.
- **National Security Memorandum 10 (NSM-10):**
  Directs U.S. federal agencies to transition cryptographic systems to quantum-resistant algorithms by 2035, establishes interagency working groups, and instructs OMB to issue related guidance.
- **2023 National Cybersecurity Strategy:**
  Stresses the urgency to replace or modernize government systems unable to defend against quantum-era threats and incorporates PQC into agency modernization strategies.

Critical OMB Memoranda and Guidance

Memo / Document	Key Requirements & Focus	Date
OMB M-23-02	- Mandates cryptographic system inventories. - Prioritizes PQC migration for high-value assets. - Urges real-world testing of pre-standardized PQC. - Establishes a PQC migration working group. - Sets planning and funding estimation requirements.	Nov 2022
Draft OMB PQC Memo8	- Formalizes requirement for agencies and third-party vendors to adhere to PQC standards. - Sets expectations for agency governance, third-party compliance, and asset inventory automation. - Defines agency/vendor PQC transition timelines.	Jul 2025 (draft)
Pending OMB Guidance	- To be issued within one year of NIST's PQC standard finalization. - Will direct agencies to develop prioritized PQC migration plans and funding strategies. - Issued in coordination with CISA and NIST.	Expected late 2025

MOSCA'S THEOREM

Dr. Michele Mosca, a renowned expert in cryptography, and the Co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, has proposed a theorem to identify the path to post-quantum preparation. Dr. Mosca has advocated using an equation to evaluate an organization's readiness for the quantum era. This theory is based on the (X+Y)>Z risk model. According to Mosca's Theorem, if the amount of time that data must remain secure (X), plus the time it takes to upgrade cryptographic systems (Y), is greater than when quantum computers come online with enough power to break cryptography (Z), then we have already run out of time.

Mosca's theorem serves as a clear reminder of the need for diligent PQC readiness preparation. Mosca's theory presents an optimistic strategy to evaluate the best forms of crypto-agility that can keep your systems safe and secure in advance of the quantum future .

Implementation Requirements

- **Federal agency mandates include:**
  - Collecting the inventory of all deployed cryptographic systems, with a focus on prioritizing high-value assets and high-impact systems7.
  - Testing PQC algorithms (including pre-standardized versions) in production-like or live environments to verify real-world operability and identify migration blockers.
  - Early identification of systems and legacy technologies that cannot be upgraded to PQC, plus planning for replacements where needed.
  - Working with third-party vendors to ensure supply chain and software comply with PQC migration requirements.
- **NSM-10 and OMB M-23-02:**
  - Requiring agencies to report progress, funding needs, and ongoing cryptographic inventory results to inter-agency working groups and policy committees.
  - Encouraging continuous engagement with emerging NIST PQC standards and alignment with CISA advisories65.

Key OMB timelines and requirements

Mandatory migration deadline

All U.S. federal agencies must migrate to PQC by 2035.

Annual inventory submissions

Since May 2023, and annually until 2035, agencies must submit an inventory of all information systems and assets vulnerable to a Cryptanalytically-Relevant Quantum Computer (CRQC). High-value assets must be prioritized as well.

Funding assessments

No later than 30 days after submitting the annual inventory, agencies must provide a funding assessment for their PQC migration in the following fiscal year.

Upcoming OMB guidance

Following NIST's release of its initial PQC standards in August 2024, the OMB is required to issue guidance detailing a concrete plan for agencies to migrate their IT systems. As of July 2025, a draft memo is still in circulation.

Vendor requirements

The upcoming OMB memo will include requirements for third-party technology vendors to ensure their products comply with PQC standards during refresh cycles, cloud migrations, and other updates.

The Tyto PQC Maturity Model - Swim Lanes and Stepwise Progression

This PQC Defense Maturity Model is designed to assist federal agencies and defense-aligned enterprises through a structured, risk-informed transition toward quantum-resistant cryptographic readiness. This model addresses readiness assessment, key exchange vulnerabilities, and algorithmic changeover, while recognizing the constraints and operational imperatives of national security systems and the broader defense industrial base.

Key Concepts of the PQC Maturity Model

Understanding the Threat:

The model helps organizations understand the potential impact of quantum computing on current cryptographic systems. This is heavily influenced by the current concern of “harvest now, decrypt later” (HNDL) since cryptographically relevant computers do not presently exist.

Assessing Current State:

The model provides a way of evaluating an organization's current level of crypto-agility and cryptographic security practices.

Defining Maturity Levels:

The model outlines different stages of PQC readiness, from basic awareness to advanced, proactive security measures.

Guiding the Transition:

The model offers a roadmap for migrating to post-quantum cryptography to include the identification of key areas for improvement and the development of a transition plan.

Benefits of Using a PQC Maturity Model:

- **Enhanced Security:** Protects against future quantum threats by proactively transitioning to quantum-resistant algorithms.
- **Improved Crypto-Agility:** Positions organizations to adapt quickly to new cryptographic standards and technologies as they will continue to evolve in the future.
- **Reduced Risk:** Minimizes the potential for data breaches and other security incidents related to quantum computing.
- **Streamlined Transition:** Simplifies the process of migrating to PQC by providing a clear roadmap and guidance.

Practical Steps for Organizations:

- **Assess your current cryptographic posture:** Identify all cryptographic systems, algorithms, and keys that are in use. In some cases, PQC resistant algorithms have already been deployed. In some cases, one must identify the legacy systems that can't be upgraded . An organization must also identify appropriate risk analysis and possible remediation steps.
- **Evaluate your organization's crypto-agility:** Determine how easily your existing systems can adapt to PQC resistant cryptographic standards.
- **Develop a PQC migration plan:** Outline the steps needed to transition to quantum-resistant algorithms.
- **Leverage tools and resources:** Utilize tools like PQC test centers and cryptographic lifecycle Swim Lanes

This model is structured for organizations transitioning to PQC, particularly those with high-assurance, regulated, or defense-oriented requirements. It defines maturity across key domains ("swim lanes") with five layers for each to reflect increasing organizational capability, alignment with best practices, and readiness for cryptographic agility and zero trust.

Core Swim Lanes

The core swim lanes are fundamental to the maturity of the PQC defense roadmap and includes the following elements:

- **PQC Algorithm Adoption**
- **Key Exchange & Management**
- **Workforce Skills & Awareness**
- **Supply Chain & Vendor Quantum Security**

The Maturity Matrix

The U.S. government, including the Department of Defense (DoD) and civilian agencies, does not use a single codified maturity model for PQC readiness and defense. However, it has codified a set of strategic, phased requirements and best practices—grounded in NIST standards, OMB memoranda, Executive Orders, and CISA guidance—that closely mimic maturity model logic and structure. A partial list of resources is available in the Reference Links section.

Several other organizations (e.g., DigiCert, FS-ISAC, GDIT) provide a variety of PQC maturity models that may be adopted or referenced within some federal programs. These typically use stages such as “Novice – Apprentice – Practitioner – Leader,” and align closely with federal mandates for inventory, risk assessment, migration, and sustainment. As a proven Federal Systems Integrator, this model articulates how Tyto Athene leads federal agencies through the maze of PQC readiness to reflect OMB requirements based on evaluated tools and market solutions.

In the exercise outlined below, we assume that all organizations begin at level 0 in the maturity model and infer Level 0 as having only ad-hoc and unknown cryptographic practices, with no clear understanding of the PQC threat.

Core Swim Lanes

Maturity Level	PQC Algorithm Adoption	Key Exchange & Management	Workforce Skills & Awareness	Supply Chain & Vendor Quantum Security
Level 1: Initial: Reactive approach to security, limited understanding of cryptographic assets, and potential threats.	Organization is tracking PQC developments; inventory of legacy cryptography is incomplete or missing.	Key management is static, with basic practices (e.g., manual key rotation, limited auditability).	Awareness limited to specialized cryptographers; IT staff workforce largely uninformed about quantum threats or PQC.	No visibility into supplier PQC readiness or dependence on quantum-vulnerable components.
Level 2: Managed: Cryptographic assets are managed on a project level, with some awareness of PQC.	Initial inventory and risk assessment of all cryptographic assets; high-level planning for migration to PQC.	Map key-exchange protocols; identify quantum-vulnerable exchanges; develop replacement roadmap.	Key personnel receive PQC/quantum-threat awareness training. Inclusion in onboarding for relevant roles.	Map supplier dependencies and collect disclosures on cryptographic standards used.
Level 3: Defined: Proactive approach to security, with defined processes for managing cryptographic assets and planning for PQC transition.	Begin pilot transitions of select assets for interop testing; vendor engagement and procurement of NIST candidate algorithms.	Integrate PQC-resilient protocols (e.g., Kyber, SIKE) in isolated environments; implement hybrid exchanges.	Train IT, developers, and security teams in PQC integration and migration practices. Develop skill maps and training plans.	Include PQC compliance as a requirement for supply chain partners and new acquisitions.

Table continues on next page.

Level 4: Quantitatively Managed: Data-driven approach to security, with metrics and measurements for assessing PQC readiness.	Systematic phased migration; use of hybrid (classical + PQC) cryptography in production environments.	Deploy new key management and exchange systems organization-wide. Integrate with certificate authorities, HSMs, and automations.	Organization demonstrates capability for PQC risk assessments, cryptographic migrations, and incident response. Regular practical exercises.	Conduct regular third-party assessments and audits of supply chain PQC posture, including security contract clauses.
Level 5: Optimizing: Continuous improvement of cryptographic security practices, with a focus on automation and proactive risk management.	Full PQC adoption across critical systems; automated lifecycle management for crypto agility; continuous algorithm evaluation.	Automated, real-time key management, quantum-safe posture monitoring, and compliance enforcement.	Workforce is not only skilled, but actively contributes to standards, open source, and industry/DoD PQC initiatives. Internal expertise leveraged to drive ongoing PQC readiness.	Ongoing automated monitoring and vetting of supplier crypto; threat intelligence informs proactive supplier engagement and risk mitigation.

Enhancing PQC Defense Strategy Maturity with MBSE

Model-Based Systems Engineering (MBSE) offers a formalized, model-driven approach that can significantly enhance a PQC defense strategy. Defense organizations can gain a holistic, data-driven view of complexity and provide key advantages in risk management, agility, compliance, and assurance by integrating PQC adoption into an MBSE framework.

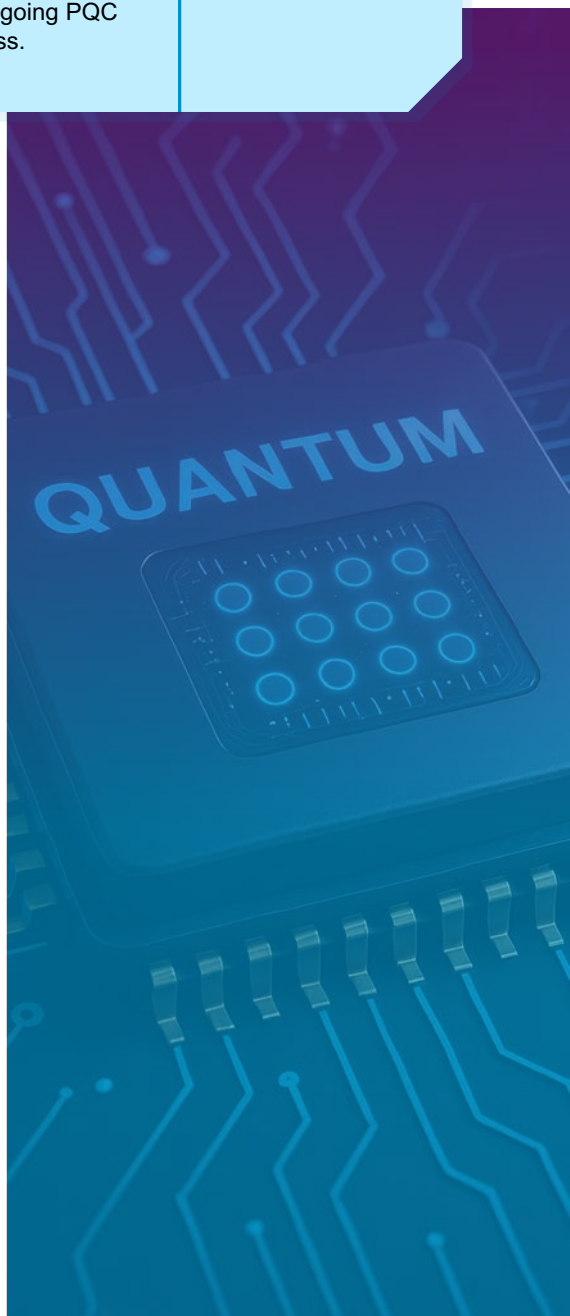
How MBSE Improves PQC Defense Strategy Maturity

Integrated Threat Modeling from Inception

- **Proactive Security by Design:** MBSE allows security requirements—including PQC— to be modeled from the earliest architectural stages. This ensures cryptographic requirements are not retrofitted but inherently organized throughout the lifecycle[12].
- **Comprehensive Threat Assessment:** Visual system models highlight potential attack surfaces and vulnerabilities created by quantum threats. This enhancement enables organizations to update their defense posture before a quantum adversary emerges[13].

Traceability and Compliance

- **Requirements Traceability:** MBSE provides direct links between requirements, design artifacts, test cases, and PQC protocols. This full traceability ensures compliance with emerging NIST and DoD cryptographic standards[4][5].
- **Regulatory Readiness:** MBSE streamlines and maintains the documentation and evidence for audits (e.g., NIST PQC standards, NSA guidance) throughout the system's evolution[6].



Agile Adaptation to Technology and Threat Evolution

- **Scenario Simulation & Analysis:** MBSE models facilitate rapid evaluation of design alternatives and PQC algorithm integration. This allows organizations to simulate “what if” scenarios under different threat models and technology choices47.
- **Change Propagation:** When new PQC standards or vulnerabilities emerge, MBSE models automatically analyze system-wide impacts to reduce risk and accelerate compliance updates46.

Stakeholder Collaboration and Efficient Governance

- **Cross-Functional Alignment:** The model fosters transparent communication and rapid decision-making byserving as a shared language for engineering, cybersecurity, policy, and operational teams81.
- **Governance Automation:** Consistent, validated models support efficient governance and assurance processes to ensure that PQC controls meet both technical and operational requirements41.

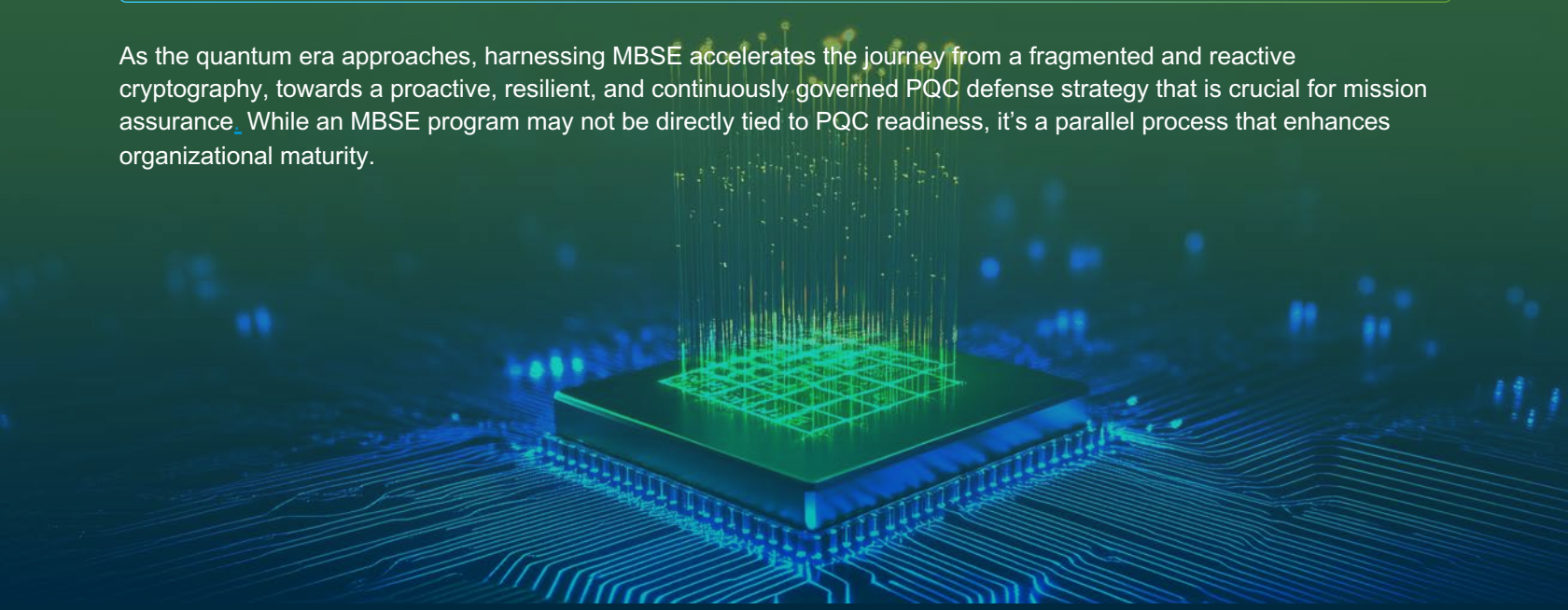
Lifecycle Security and Continuous Assurance

- **Continuous Validation:** MBSE reduces late-stage issues and costly rework by enabling ongoing verification of PQC controls via simulation and model checking before deployment23.
- **Automated Monitoring Protocols:** The MBSE models and specifies post-deployment monitoring and patching to support ongoing compliance and rapid response to quantum-related threats2.

Actionable MBSE-Specific Recommendations

- Mandate MBSE for all new PQC-sensitive system designs and upgrades.
- Model PQC requirements, vulnerabilities, and compliance artifacts from the outset.
- Integrate MBSE with cybersecurity and IT governance processes for ongoing lifecycle assurance.
- Leverage iterative simulation and model-based analysis to forecast and ensure protection against evolving quantum threats.

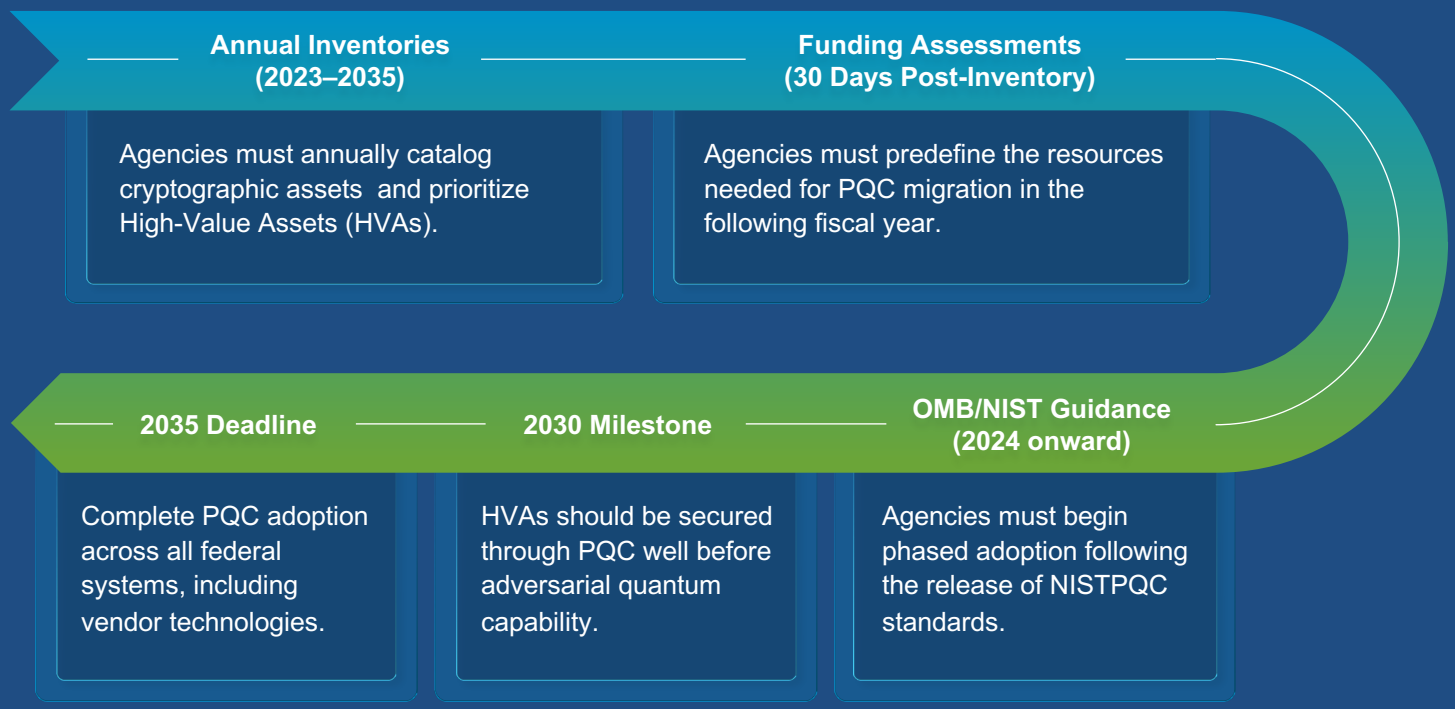
As the quantum era approaches, harnessing MBSE accelerates the journey from a fragmented and reactive cryptography, towards a proactive, resilient, and continuously governed PQC defense strategy that is crucial for mission assurance. While an MBSE program may not be directly tied to PQC readiness, it’s a parallel process that enhances organizational maturity.



PQC 3-year Readiness Roadmap

Example: Three-Year Maturity Progression Aligned to OMB Mandates

Federal Mandates Driving the Roadmap



This hypothetical roadmap compresses the maturity progression into a **three-year plan** to create measurable momentum toward the 2030 milestone.

Integrated Three-Year Roadmap

Year 1: Establishing the Foundation (Levels 1–2)

- **PQC Algorithm Adoption:** Agencies conduct comprehensive inventories to map all cryptographic assets and identify the algorithms at risk. A limited pilot begins with candidate PQC algorithms in non-critical systems.
- **Key Exchange & Management:** The roadmap catalogs all key exchange protocols are , flags the vulnerable mechanisms for replacement, documents the existing manual practices, and initiates themigration roadmaps.
- **Workforce Skills & Awareness:** Foundational PQC awareness training is then delivered to security, IT, and procurement staff, and leadership is briefed on PQC mandates and risks.
- **Supply Chain & Vendors:** Agencies collect disclosures from suppliers on cryptographic practices and assess dependencies. The roadmap adds early requirements for PQC readiness to facilitate vendor discussions.

Outcome: The roadmap helps ensure that the OMB annual inventory and funding submissions are met. Agencies move from reactive awareness to structured discovery to position themselves for proactive pilots.

Year 2: Pilot and Scale Governance (Levels 2–3)

- **PQC Algorithm Adoption:** Pilot PQC algorithms (e.g., Kyber) are deployed in controlled environments and tested for interoperability with legacy systems. Migration plans prioritize HVAs and high-impact systems.
- **Key Exchange & Management:** Hybrid key exchange protocols are tested in isolated networks. Early integration begins with certificate authorities and HSMs for PQC compatibility.
- **Workforce Skills & Awareness:** Role-specific training is initiated to expand across the development, operations, and cyber teams. Agencies establish internal migration playbooks and conduct tabletop exercises.
- **Supply Chain & Vendors:** PQC compliance becomes a contractual requirement for new procurements and refresh cycles. Supplier roadmaps are aligned with agency migration goals.

Outcome: Agencies achieve proactive pilot activity, demonstrate governance over PQC migration, and validate feasibility of transition strategies while meeting OMB's annual reporting.

Year 3: Enterprise Rollout and Measured Readiness (Levels 3–4)

- **PQC Algorithm Adoption:** Hybrid cryptography is rolled into production for priority systems, with clearly established metrics for coverage and performance. The next step in the adoption phase is to deploy early automation for cryptographic lifecycle management.
- **Key Exchange & Management:** Enterprise-level PQC key management systems are operational. Automation is introduced for key rotation and monitoring to reduce manual risk.
- **Workforce Skills & Awareness:** Staff participates in PQC migration exercises and red-team simulations. Skill inventories confirm coverage of critical roles.
- **Supply Chain & Vendors:** Independent third-party audits verify vendor PQC readiness. Supply chain security is embedded into vendor management systems with ongoing assessments.

Outcome: Agencies transition from pilot to enterprise-scale implementation. PQC becomes part of operational security posture, which is measurable through KPIs to ensure alignment with OMB oversight and accelerate progress toward the 2030 milestone.

Strategic Impact of 3 Year Roadmap

Agencies can not only comply with OMB mandates but proactively secure HVAs before the 2030 milestone by compressing maturity growth and adopting our three-year roadmap. This approach also gives agencies leverage with vendors, clarity in workforce development, and credibility in funding requests.

Year 1: Foundation Establishment	Year 2: Pilot and Governance	Year 3: Enterprise Rollout
Agencies conduct inventories and training to prepare for PQC adoption	Pilot PQC algorithms are tested and governance structures are established.	PQC is integrated into production system and vendor readiness is verified.

Result: Agencies can achieve measurable and enterprise-level PQC resilience within three years by setting conditions for continuous optimization and decisive leadership in the government-wide transition to PQC before 2035.

The Maturity Levels in Depth

Level 1: Achieving Awareness and the Readiness Assessment

Objective

At this level, we determine ad-hoc and unknown cryptographic practices with no clear understanding of the PQC threat.

To move from Level 1, some basic investigative processes need to occur. We outline this process below:

Actions

- Conduct an organizational PQC Readiness Assessment aligned to mission sensitivity, information lifespan, and current crypto dependency.
- Collect the inventory cryptographic assets (including hardcoded, embedded, and third-party systems) across classified and unclassified enclaves.
- Benchmark readiness against NIST and NSA guidance (e.g., CNSSP-15, NIST SP 800-208).
- Build leadership awareness and establish a crypto-agility governance team.
- Map supplier dependencies across the technology stack.

Outcomes

- Clear view of cryptographic dependencies.
- Executive alignment on urgency and scope.
- Baseline classification of high-value targets vulnerable to “harvest-now-decrypt-later” (HNDL) risk.
- Provide management platforms to streamline the transition.

Starting Point Algorithms to Consider

Algorithm	Type	FIPS/Status	Core Use Case	Key Info
ML-KEM (CRYSTALS-Kyber)	Lattice-based KEM	FIPS 203	Public-key encryption, key exchange	Main standard for key establishment in security protocols
ML-DSA (CRYSTALS-Dilithium)	Lattice-based signature	FIPS 204	Digital signatures	General-purpose signing and moderate key/signature size.
SLH-DSA (SPHINCS+)	Hash-based signature	FIPS 205	Stateless digital signatures	Conservative security, no state-tracking, and longer signatures.
FN-DSA (Falcon)	Lattice-based signature	FIPS 206 (draft, expected soon)	Digital signatures	Compact signatures, fast verification, and complex implementation
HQC (Hamming Quasi-Cyclic)	Code-based KEM	Selected March 2025, standard pending	Public-key encryption, key exchange	Chosen as backup to ML-KEM; larger keys/ciphertext, and mature cryptanalysis.

Level 2: Initiating Proactive Cryptographic Agility and Asset Management

Objective

Cryptographic assets are managed on a project level, with acute awareness of PQC.

Actions

- Implement crypto-agile architectures: abstract cryptographic libraries and APIs to support modular algorithm switching.
- Begin refactoring legacy applications to reduce hardcoded cryptographic logic.
- Establish automated cryptographic discovery and telemetry tools for real-time crypto inventory maintenance.
- Provide training for key personnel on PQC/quantum-threat awareness training.
- Map supplier dependencies and collect disclosures on the cryptographic standards used.

Key Exchange Focus

- Identify systems using vulnerable key exchange mechanisms (e.g., Diffie-Hellman, ECDH).
- Begin testing hybrid key exchange models to combine classical and post-quantum primitives (e.g., Kyber + X25519).

Outcomes

- Architectural preparedness for dual-stack and hybrid crypto operations.
- Initial mitigation of key exchange vulnerabilities with forward secrecy concerns.

Level 3: Deeper Algorithm Evaluation and Pilot Deployment

Objective

Proactive approach to security, with defined processes for managing cryptographic assets and planning for PQC transition.

Actions

- Begin pilot deployments of approved post-quantum algorithms (e.g., Kyber for key encapsulation, Dilithium for digital signatures) in non-mission-critical systems.
- Integrate PQC-resilient protocols (e.g., Kyber, SIKE) in isolated environments.
- Implement hybrid exchanges.
- Conduct performance benchmarking and interoperability tests.
- Formalize skill maps and training plans.
- Incorporate PQC compliance as a requirement for supply chain partners and new acquisitions.

Readiness Integration

- Create simulation scenarios and tabletop exercises that test crypto-failure and crypto-switch scenarios in operational contexts (including classified enclaves and tactical edge).

Outcomes

- Gain confidence in algorithm performance across operational environments (HQ, tactical, edge).
- Obtain lessons learned to refine migration strategy and update System Requirement Documents (SRDs).

Level 4: Quantitatively Managing Operational Integration

Objective

Data-driven approach to security, with metrics and measurements for assessing PQC readiness.

Actions

- Ensure systematic phased migration and the use of hybrid (classical + PQC) cryptography in production environments.
- Deploy new key management and exchange systems at organization-wide capacity. Integrate with certificate authorities, HSMs, and automations.
- Conduct regular practical exercises.
- Conduct regular third-party assessments and audits of supply chain PQC posture, including security contract clauses.

Key Exchange Focus

- Standardize use of PQC-based or hybrid key exchange methods within network transport, authentication, and storage protocols.

Outcomes

- Operationalization of PQC in line with national security priorities.
- Enterprise-wide PQC capability embedded within DevSecOps and continuous Authority to Operate (cATO) pipelines.

Level 5: Optimization, Monitoring, and Resilience

Objective

Continuous improvement of cryptographic security practices, with a focus on automation and proactive risk management.

Actions

- Full PQC adoption across enterprise systems.
- Automated lifecycle management for crypto agility; continuous algorithm evaluation.
- Automated, real-time key management, quantum-safe posture monitoring, and compliance enforcement.
- Ongoing automated monitoring and vetting of supplier crypto.
- Threat intelligence informs proactive supplier engagement and risk mitigation

Outcomes

- Enterprise cryptographic infrastructure is both quantum-resistant and dynamically adaptable.
- Institutionalized processes for responding to evolving quantum threat vectors and algorithmic advancements.

Summary

Tyto Athene's Maturity Model serves as a high confidence planning framework for agencies preparing for quantum disruption. It does not supersede or counteract any NIST or CISA strategy, but rather offers practical business thinking around achieving a viable level of readiness maturity. Our model balances the long-term cryptographic transition timeline with the immediate need to mitigate Harvest Now, Decrypt Later (HNDL) vulnerabilities and integrate crypto agility into federal IT modernization efforts

Reference Links

1. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
2. https://csrc.nist.gov/projects/post-quantum-cryptography
3. https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF
4. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf
5. https://www.encryptionconsulting.com/your-guide-to-the-new-federal-quantum-action-plan/
6. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf
7. https://postquantum.com/industry-news/executive-order-14144-quantum/

About Tyto Athene

Tyto Athene, LLC, a large portfolio company of Arlington Capital Partners, was established as an IT services and solutions providers specializing in mission-focused digital transformation. Our goal is to enhance client experience and drive successful outcomes through innovative technology solutions.

As a full-service systems integrator, Tyto Athene empowers clients with the ability to make informed, timely decisions by providing secure and ubiquitous access to enterprise information across their operating environments. We leverage cutting-edge technologies, strategic innovation, and proven methodologies to deliver successful results for clients worldwide. With a full spectrum of industry-leading capabilities, substantial scale, and extensive resources, we are equipped to meet the increasingly complex demands U.S. government agencies. Supporting the rapidly evolving mission requirements of federal clients remains our top priority.

Our combination of experience and forward-thinking technology solutions gives Tyto Athene customers a distinct strategic advantage. Our primary objective is to deliver the best solutions and services available in the market to our trusted partners and clients. Tyto Athene remains committed to providing our high-quality products, superior service, and world-class technical support.

TYTO Athene

DATA TO DOMINANCE

/company/gotyto

https://gotyto.com

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