MARCH 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

GOVERNMENT & DEFENSE EXTENSION

National Security Systems, Federal Agencies, Defense Industrial Base, and Allied Interoperability Providers
— Industry-Specific Challenges and Framework Adaptations

Version 1.1 — March 2026

Marin Ivezic
CEO, Applied Quantum
Author, PostQuantum.com

PQCFramework.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. This document does not contain or reference any classified information. Organizations should consult appropriate classification authorities, legal counsel, and regulatory bodies for guidance specific to their jurisdiction, classification level, and operational context.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of March 2026. Readers should verify current status against primary sources (NSA, NIST, CISA, national defense agencies, vendor documentation) before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2025–2026. Federal agencies and their contractors should reference the final published version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent Document	The Applied Quantum PQC Migration Framework — Universal — v1.1 (March 2026)

Intended audience	CISOs, security architects, program managers, and compliance officers in government agencies, defense departments, intelligence organizations, and defense industrial base contractors
Assumed knowledge	Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of CNSA 2.0, NSM-10, NIST SP 800-series, and government/defense security architectures
Scope	Sector-specific challenges and phase-by-phase framework adaptations for government and defense organizations. Not a standalone document — intended to be used alongside the Universal Framework.

HOW TO USE THIS EXTENSION

This document is a companion to the Applied Quantum PQC Migration Framework (Universal). It does not replace the Universal Framework but extends it with telecommunications-specific guidance. For each topic, this extension identifies unique sector challenges and then maps specific adaptations to the relevant Universal Framework phase. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

ACCOMPANYING RESOURCES

Every aspect of this framework — from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance — has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Quantum Readiness Starting page: https://postquantum.com/quantum-readiness-starting/ — but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com — a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

TABLE OF CONTENTS

WHY GOVERNMENT AND DEFENSE REQUIRES A SECTOR EXTENSION

The Universal PQC Migration Framework provides a comprehensive 8-phase methodology applicable to any enterprise. Government and defense organizations can and should follow that methodology. However, this sector faces a unique combination of constraints that make PQC migration simultaneously more urgent, more regulated, and more complex than in any other industry. Government and defense is the one sector where PQC migration is not optional or aspirational — it is mandated, with hard deadlines, by the very authorities that define cryptographic standards.

The Only Sector with Mandatory PQC Timelines

Government and defense is unique in having explicit, non-negotiable PQC migration deadlines. CNSA 2.0 (Commercial National Security Algorithm Suite 2.0), published by NSA, mandates that all national security systems (NSS) must transition to quantum-resistant algorithms by 2030 for software and firmware, with full disallowance of classical asymmetric algorithms by 2035. These are not recommendations — they are requirements that will be enforced through procurement specifications, system accreditation, and authority-to-operate (ATO) decisions.

In the United States, NSM-10 (National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems) directed federal agencies to inventory their cryptographic systems and develop migration plans. OMB M-23-02 required agencies to submit inventories of cryptographic systems vulnerable to quantum computers. Similar mandates exist or are emerging in the UK, EU, Australia, Canada, and other Five Eyes and NATO nations.

This mandatory context means the Universal Framework's Phase 0 (Executive Mandate) is largely pre-established by policy — but the implementation phases become more

complex because they must satisfy specific government accreditation and compliance requirements that commercial enterprises do not face.

HNDL as an Active, Present-Tense Threat

For most enterprises, Harvest Now, Decrypt Later (HNDL) is a theoretical future risk. For government and defense, it is an active, ongoing operation by nation-state adversaries. Intelligence agencies worldwide assess with high confidence that strategic competitors are already harvesting encrypted government communications, diplomatic cables, military planning data, and intelligence products for future quantum decryption.

Government data often has classification periods of 25–75 years or more. Classified intelligence, weapons design data, nuclear secrets, and diplomatic communications intercepted today will still be sensitive decades from now. This means the HNDL threat window is already open — every day that passes with quantum-vulnerable encryption on classified systems is a day that adversaries accumulate material for future exploitation. The urgency calculus is fundamentally different from commercial enterprises.

Bifurcated Classified and Unclassified Environments

Government organizations operate in at least two distinct security domains: classified (national security systems, often multiple classification levels) and unclassified (including Controlled Unclassified Information / CUI, and public-facing systems). Each domain has different cryptographic requirements, different accreditation authorities, different vendor ecosystems, and different migration timelines. Classified systems must follow NSA/CNSA 2.0 algorithm guidance; unclassified systems follow NIST standards. Cross-domain solutions that bridge these environments add a third layer of complexity.

PQC migration must be planned and executed separately for each domain, with coordination at the boundaries. This bifurcation doubles the effective scope of the migration program and introduces classification-handling constraints on program documentation, testing environments, and vendor engagement.

Defense Industrial Base as Extended Attack Surface

Government and defense organizations do not operate in isolation. The Defense Industrial Base (DIB) — comprising thousands of contractors, subcontractors, and suppliers — handles classified and CUI data that is subject to the same quantum threats. A PQC migration program that secures the government's own systems but leaves the DIB on

classical cryptography has not eliminated the HNDL exposure; it has merely shifted the collection point to the supply chain.

CMMC (Cybersecurity Maturity Model Certification), DFARS clauses, and FedRAMP requirements must evolve to incorporate PQC. Government agencies must drive PQC readiness down through the supply chain while managing the reality that many DIB contractors are small and medium enterprises with limited cryptographic expertise.

Weapons Systems and Long-Lived Platforms

Military weapons systems, satellites, aircraft, naval vessels, and command-and-control platforms have operational lifecycles of 20–50 years. Many contain embedded cryptographic modules that cannot be easily updated in the field. A fighter aircraft delivered in 2026 will be in service until 2060 or beyond; its cryptographic capabilities must either be quantum-resistant from delivery or upgradable to PQC during its service life.

This creates a hard procurement constraint: all new weapons system acquisitions should require PQC capability or a credible PQC upgrade path. Existing platforms must be assessed for cryptographic upgrade feasibility, with remediation plans integrated into platform sustainment programs. This is analogous to the OT lifecycle challenge in critical infrastructure, but with the added dimension of operational deployment in hostile environments.

Coalition and Allied Interoperability

Modern military operations are almost always conducted in coalition with allies (NATO, Five Eyes, bilateral partners). Cryptographic interoperability between allies is essential for secure communications, intelligence sharing, and combined operations. PQC migration must be coordinated across allied nations, each of which may be on a different migration timeline, using different approved algorithms (CNSA 2.0 for US/Five Eyes, national algorithms for some European and Asian allies), and operating under different classification authorities.

If one ally migrates to PQC while another remains on classical cryptography, the interoperability mechanisms (cross-domain gateways, coalition networks, shared communication systems) must support both — adding years of hybrid operation to the migration timeline. NATO’s cryptographic standards bodies must coordinate PQC adoption across 32 member nations.

INDUSTRY-SPECIFIC CHALLENGES

This section details the technical and operational challenges unique to government and defense PQC migration.

Challenge 1: CNSA 2.0 Compliance Under Hard Deadlines

CNSA 2.0 specifies exact algorithms and key sizes: ML-KEM-1024 for key establishment, ML-DSA-87 or SLH-DSA for digital signatures, AES-256 for symmetric encryption, and SHA-384/SHA-512 for hashing. These are not flexible recommendations — they are the only approved algorithms for national security systems. The timeline requires software/firmware implementations by 2030 and hardware implementations by 2033, with full disallowance of classical asymmetric algorithms by 2035.

Organizations that miss these deadlines face loss of authority to operate (ATO), inability to accredit new systems, and potential inability to connect to classified networks. Unlike commercial compliance frameworks where penalties are financial, failure to comply with CNSA 2.0 means the system cannot be used for its intended mission.

> **Framework Impact:** Phase 0 must anchor the entire program timeline to CNSA 2.0 deadlines. Phase 4 must build a roadmap that achieves compliance milestones in 2030/2033/2035 with margin for testing and accreditation.

Challenge 2: Classified System Accreditation Overhead

Every change to a classified system must go through a formal accreditation process (Risk Management Framework / RMF under NIST SP 800-37 for US systems, or equivalent national processes). Changing the cryptographic algorithms in a system's security architecture is a significant modification that triggers re-assessment and re-authorization. For complex systems, this process can take 12–24 months.

The accreditation pipeline will become a bottleneck as hundreds or thousands of systems simultaneously require re-authorization for PQC migration. Accreditation bodies (e.g.,

DISA, NSA, national security authorities) must scale their capacity to handle this surge, or migration timelines will slip regardless of technical readiness.

> **Framework Impact:** Phase 4 must model accreditation timelines for each system. Phase 6 must prepare accreditation documentation packages in parallel with technical migration. Engage accreditation authorities early to negotiate streamlined processes for PQC-specific changes.

Challenge 3: Cross-Domain Solution Migration

Cross-domain solutions (CDS) — the guarded gateways that allow controlled data transfer between different classification levels — are among the most security-critical systems in government. They use cryptography extensively for authentication, content inspection, and data labeling. CDS devices are subject to the most stringent accreditation requirements and are typically provided by a small number of approved vendors.

Migrating CDS to PQC requires coordinated action between the CDS vendor, the accrediting authority, and the organizations on both sides of the domain boundary. Because CDS failure could compromise classification boundaries, these systems will require especially thorough testing and conservative migration approaches.

> **Framework Impact:** Phase 3 must classify CDS as highest-priority/highest-difficulty systems. Phase 5 must include dedicated CDS PQC pilots in isolated lab environments. Phase 7 must engage CDS vendors on PQC roadmaps.

Challenge 4: Weapons System Embedded Cryptography

Weapons systems contain embedded cryptographic modules (Type 1 encryptors, HAIPE devices, cryptographic ignition keys) that implement classified algorithms. These modules are typically hardware-based, vendor-specific, and subject to NSA product certification. Replacing or upgrading them requires coordination with the weapons system program office, the cryptographic module vendor, NSA's Commercial Solutions for Classified (CSfC) or Type 1 certification program, and the operational commands that use the system.

Many weapons platforms — aircraft, ships, submarines, missile systems — operate in austere environments where hardware upgrades require depot-level maintenance. The logistics of replacing cryptographic modules across a fleet of hundreds of aircraft or dozens of ships are measured in years and billions of dollars.

> **Framework Impact:** Phase 1 must inventory all Type 1 and CSfC-listed cryptographic modules across weapons platforms. Phase 4 must integrate PQC migration into platform sustainment and modernization schedules. Phase 7 must coordinate with NSA and cryptographic module vendors on next-generation PQC-capable devices.

Challenge 5: Satellite and Space System Constraints

Military and intelligence satellites operate in the most constrained and least accessible environment possible. Once launched, a satellite's cryptographic hardware cannot be physically upgraded. Satellites use embedded encryption for telemetry, command uplinks, data downlinks, and inter-satellite links. These systems must be quantum-resistant for their entire orbital lifetime (often 15–20 years).

Satellites currently in design and production must incorporate PQC from launch. Satellites already in orbit with classical cryptography represent a fixed HNDL exposure that can only be mitigated by encrypting ground-station-to-satellite links with PQC at the ground segment, layering PQC protection over classical satellite encryption where protocol flexibility allows, or accepting the risk for the satellite's remaining operational life.

> **Framework Impact:** Phase 1 must inventory all satellite and space system cryptographic implementations. Phase 4 must distinguish between in-orbit (non-upgradable) and future-launch (must-be-PQC) systems. Phase 7 must coordinate with satellite manufacturers on PQC-by-design requirements.

Challenge 6: Defense Industrial Base Supply Chain Cascade

The DIB comprises tens of thousands of contractors who handle classified and CUI data. These contractors use cryptography to protect data at rest, in transit (VPNs, TLS), and in use (encrypted enclaves). A government agency's PQC migration is incomplete if its contractors remain on classical cryptography — the data is only as secure as the weakest link in the chain.

Driving PQC adoption through the DIB is complicated by the diversity of contractor size and sophistication (from major primes like Lockheed Martin to small machine shops), the cost burden on small businesses, and the challenge of enforcing cryptographic standards through contract mechanisms. CMMC and DFARS 252.204-7012 provide frameworks for cybersecurity requirements, but PQC-specific requirements are not yet fully integrated.

> **Framework Impact:** Phase 7 must extend to DIB PQC readiness assessment. Phase 0 should include contractor PQC requirements in contract modifications. Phase 3 must score contractor-held data for HNDL exposure.

Challenge 7: Coalition Cryptographic Interoperability

Allied military operations depend on shared cryptographic standards for secure voice, data, and messaging. NATO's cryptographic interoperability standards (e.g., STANAG 4774/4778 for metadata binding, KMI/KMS for key management) must be updated for PQC. The transition period — where some allies have migrated and others have not — requires dual-stack or gateway-mediated interoperability that could last a decade or more.

Non-Five Eyes allies may use national cryptographic algorithms that differ from CNSA 2.0 recommendations. Interoperability with these allies requires protocol negotiation mechanisms that can handle multiple PQC algorithm families, adding complexity to coalition communication architectures.

> **Framework Impact:** Phase 4 must model coalition interoperability requirements. Phase 5 must include joint testing with key allies. Phase 7 must include engagement with NATO and bilateral cryptographic standards bodies.

Challenge 8: PKI at Government Scale

Government PKI systems (e.g., US DoD PKI, which issues millions of certificates for personnel, devices, and servers) are among the largest and most complex certificate infrastructures in the world. Migrating government PKI to PQC algorithms means re-issuing millions of certificates, updating all relying-party systems to validate PQC signatures, and managing a transition period where both classical and PQC certificates must coexist.

PQC certificates are significantly larger than classical certificates. ML-DSA-87 certificates are approximately 10x larger than RSA-2048 certificates. This size increase affects smart card storage (CAC/PIV cards), certificate chain validation performance, OCSP/CRL bandwidth, and LDAP directory sizes. The DoD CAC (Common Access Card) replacement cycle and PIV card infrastructure must be planned to accommodate PQC certificates and the corresponding key sizes.

> **Framework Impact:** Phase 2 must document all PKI trust hierarchies and certificate counts. Phase 6 must benchmark PQC certificate performance across

> identity, authentication, and signature use cases. Phase 4 must align PKI migration with smart card refresh cycles.

Challenge 9: Sovereign Cryptography and National Algorithm Requirements

While CNSA 2.0 standardizes algorithm choices for US national security systems, allied and partner nations may have additional or different requirements. Some nations mandate national cryptographic algorithms for sovereignty reasons (e.g., certain European or Asian nations requiring nationally-developed or nationally-evaluated algorithms alongside NIST standards). Organizations operating across multiple jurisdictions must accommodate these variations.

Sovereign cryptography requirements can conflict with interoperability goals. A system that must use CNSA 2.0 algorithms for US data and a different national algorithm for partner-nation data needs crypto-agility at the protocol level — a capability that most current systems do not have.

> **Framework Impact:** Phase 0 must map all applicable national cryptographic requirements. Phase 5 must architect for multi-algorithm PQC support where sovereign requirements exist. Phase 7 must engage with national cryptographic authorities.

Challenge 10: Tactical and Deployed System Constraints

Military systems deployed in the field — tactical radios, mobile command posts, forward-deployed servers, unmanned systems — operate under bandwidth, power, and computational constraints similar to OT environments, but with the added challenges of mobility, adversarial electromagnetic environments, and intermittent connectivity. PQC's larger key and signature sizes impact tactical network bandwidth, which is often the scarcest resource in deployed environments.

Software-defined radios, tactical data links (Link 16/22), and satellite communications terminals all embed cryptographic functions that must eventually support PQC. The NSA's HAIPE (High Assurance Internet Protocol Encryptor) program must deliver PQC-capable encryptors that meet the form factor, power, and environmental requirements of tactical deployment.

> **Framework Impact:** Phase 6 must benchmark PQC overhead against tactical bandwidth and latency budgets. Phase 1 must inventory deployed cryptographic equipment. Phase 7 must track NSA/HAIPE PQC device timelines.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR GOVERNMENT AND DEFENSE

This section specifies the adaptations required for government and defense. Implement alongside the Universal Framework's phase guidance.

Phase 0 — Executive Mandate & Business Case

Mandate Context

In government and defense, the executive mandate largely exists by policy (NSM-10, CNSA 2.0, national directives). The Phase 0 challenge is not securing executive buy-in but translating policy mandates into funded, resourced, staffed programs with realistic timelines. The business case should quantify the HNDL exposure of classified data, model the accreditation pipeline capacity constraints, and establish the program's relationship to existing modernization and sustainment budgets.

Governance Adaptation

Establish a Quantum Migration Program Office (PMO) with authority across both classified and unclassified domains. Include representation from CIO, CISO, Chief Cryptographic Officer (where applicable), acquisition/procurement, accreditation authority, and operational commands. For defense organizations, align the PMO with existing weapons system program offices to integrate PQC migration into platform sustainment schedules.

Phase 1 — Discovery & Inventory

Government-Specific Inventory Tracks

- **Classified system inventory:** All national security systems by classification level, accreditation boundary, cryptographic module type (Type 1, CSfC, COTS), and algorithm in use.
- **Unclassified/CUI system inventory:** Federal information systems, cloud services (FedRAMP), CUI-handling systems, and external-facing services.
- **Cross-domain solution inventory:** All CDS devices, their cryptographic configurations, accreditation status, and vendor support timelines.
- **Weapons system and platform inventory:** Cryptographic modules in aircraft, ships, vehicles, satellites, unmanned systems, and tactical communications equipment.
- **PKI and identity inventory:** Certificate authorities, certificate counts, smart card populations (CAC/PIV), and certificate management infrastructure.
- **DIB contractor inventory:** Map which contractors handle classified or CUI data, what cryptographic protections they use, and their PQC readiness status.

Phase 2 — CBOM & Documentation

Classification-Aware CBOM

Government CBOMs must be produced at the appropriate classification level. CBOM data for classified systems is itself sensitive (potentially classified) because it reveals cryptographic architecture. Establish CBOM classification handling procedures, secure storage, and need-to-know access controls. Use the Minimum Viable CBOM approach for unclassified systems; for classified systems, work with accreditation authorities to determine the appropriate CBOM detail level that balances operational security with migration planning utility.

Phase 3 — Risk Scoring & Prioritization

Adapted Risk Scoring

Add two dimensions to the Universal Framework's risk scoring:

- **Data classification sensitivity:** Systems handling TOP SECRET/SCI data score highest for HNDL risk. Systems handling CUI score lower but remain significant due to aggregation risk.

- **Accreditation complexity:** Systems with complex accreditation boundaries, multiple interconnections, or cross-domain dependencies score higher on migration difficulty.

Government Priority Tiers

Priority	System Category	Rationale
Tier 1	Classified network backbone (TLS/IPsec), cross-domain solutions, intelligence collection/processing systems, satellite ground stations	Highest HNDL exposure. Mandatory CNSA 2.0 compliance. Active nation-state collection threat.
Tier 2	Weapons system communications, command and control networks, PKI/identity infrastructure, coalition interoperability gateways	High HNDL and TNFL exposure. Platform lifecycle dependencies. Coalition coordination required.
Tier 3	Unclassified federal networks, FedRAMP cloud services, CUI-handling contractor systems, administrative IT	Important but lower classification sensitivity. Can leverage commercial PQC products. NIST-governed.
Tier 4	Legacy weapons platforms (non-upgradable crypto), archived systems, low-sensitivity public-facing services	Apply compensating controls. Plan replacement on platform lifecycle. Lowest migration urgency.

Phase 4 — Roadmap & Governance

CNSA 2.0 Milestone Alignment

The migration roadmap must explicitly align with CNSA 2.0 milestones:

- **By 2027:** Complete cryptographic inventory for all NSS. PQC pilots underway on non-mission-critical systems.
- **By 2030:** All software and firmware cryptographic implementations on NSS migrated to CNSA 2.0 algorithms. Accreditation pipeline cleared for priority systems.
- **By 2033:** All hardware cryptographic modules on NSS upgraded or replaced with PQC-capable devices.

- **By 2035:** Full disallowance of classical asymmetric algorithms on NSS. All remaining systems migrated or decommissioned.

Acquisition Integration

Integrate PQC requirements into all new acquisition programs immediately. Update Request for Proposal (RFP) templates, Statement of Work (SOW) language, and technical evaluation criteria to require CNSA 2.0 compliance or a credible upgrade path. For programs already in acquisition, issue contract modifications to add PQC requirements.

Phase 5 — Pilots & Migration Execution

Government Pilot Sequence

- **Pilot 1 — Unclassified network TLS:** Migrate TLS on unclassified web servers and internal services to hybrid PQC. Low classification risk, high learning value.
- **Pilot 2 — VPN and remote access:** Deploy hybrid PQC IPsec on remote access VPNs for unclassified/CUI networks. Test with commercial PQC-capable VPN products.
- **Pilot 3 — Classified network backbone:** Deploy PQC-TLS/IPsec on a classified network segment in a lab/test environment. Coordinate with accreditation authority for test ATO.
- **Pilot 4 — PKI certificate migration:** Issue PQC certificates from a test CA. Validate smart card (CAC/PIV) compatibility and application integration.
- **Pilot 5 — Coalition interoperability:** Joint pilot with a Five Eyes or NATO ally to test PQC-protected information exchange on a coalition test network.

Phase 6 — Infrastructure Modernization & Performance

Government-Specific Performance Considerations

- **PKI/certificate infrastructure:** Benchmark PQC certificate validation, OCSP response sizes, and directory (LDAP) query performance at government scale (millions of certificates).
- **Smart card/CAC constraints:** Test ML-DSA key and certificate storage on current and next-generation smart card hardware. Coordinate with GSA and card issuers.
- **Tactical network bandwidth:** Model PQC handshake and certificate overhead against tactical link bandwidth (Link 16: 31.6 kbps per timeslot; tactical SATCOM: variable but often constrained).
- **HAIPE and Type 1 encryptors:** Track NSA's PQC-capable HAIPE development timeline. Plan transition for network encryptors across classified WANs.

Phase 7 — Vendor & Supply Chain Governance

Government Vendor Classification

- **Tier A — Mission-critical:** NSA-certified cryptographic module vendors, CDS vendors, HAIPE vendors, satellite encryption providers. Government has direct engagement through NSA/DISA.
- **Tier B — Infrastructure:** Major IT contractors (network, cloud, identity), FedRAMP CSPs, PKI vendors. Engage through contract requirements and FedRAMP PQC guidance.
- **Tier C — DIB cascade:** Defense contractors of all sizes. Drive PQC through CMMC, DFARS, and contract flow-down clauses.

DIB PQC Requirements

- **Contract flow-down:** Add PQC readiness requirements to DFARS clauses for all new and renewed contracts involving classified or CUI data.
- **CMMC evolution:** Advocate for PQC-specific controls in future CMMC versions. Provide guidance and toolkits for small DIB contractors.
- **FedRAMP PQC:** Engage FedRAMP PMO to incorporate PQC requirements into cloud service authorization baselines.

GOVERNMENT & DEFENSE REGULATORY ALIGNMENT MAP

Authority	Requirement	Timeline	Gov/Def Implication
NSA CNSA 2.0	Mandatory PQC algorithms for NSS	2030 SW/FW, 2033 HW, 2035 disallowance	Hard compliance deadline. Loss of ATO for non-compliant systems.
NSM-10 / EO 14028	Federal crypto inventory and migration plans	Ongoing since 2022	Agencies must have inventories and plans. OMB oversight.
NIST SP 800-208	PQC recommendations for federal systems	FIPS 203/204/205 published 2024	Governs unclassified federal systems. Basis for FedRAMP PQC.
NIST IR 8547	Transition to PQC standards	Draft 2024; final expected 2025–2026	Deprecation/disallowance timelines for classical algorithms on federal systems.
CMMC / DFARS	DIB cybersecurity certification	CMMC 2.0 rolling out; PQC TBD	Will eventually require PQC for CUI protection. Early mover advantage for contractors.
NATO STANAG	Allied cryptographic interoperability	Under review for PQC	Affects coalition operations. Multi-year NATO standardization process.

UK NCSC	PQC guidance for government systems	Guidance published 2024; updates ongoing	Aligns with but may differ from US CNSA 2.0 in algorithm specifics.
EU/ENISA	PQC recommendations for member states	Multiple publications; ongoing	Affects EU defense cooperation and dual-use systems.

GOVERNMENT & DEFENSE MATURITY MODEL SUPPLEMENT

Level	Universal Indicator	Gov/Def-Specific Indicator
Level 1: Aware	Executive sponsorship; quantum risk acknowledged	CIO/CISO directive issued. CNSA 2.0 compliance gap identified. Quantum PMO established. OMB reporting initiated.
Level 2: Assessed	Inventory complete for priority systems; CBOM initiated	NSS cryptographic inventory complete (per NSM-10). CDS and weapons platform crypto modules cataloged. PKI scope assessed. DIB exposure mapped.
Level 3: Planning	Risk-scored roadmap approved; pilots designed	CNSA 2.0 milestone-aligned roadmap approved. Accreditation authority pre-engaged. Acquisition PQC requirements integrated. Coalition coordination initiated.
Level 4: Migrating	Hybrid PQC in production; CBOM maintained	Tier 1 classified systems migrating. Unclassified networks on PQC. PKI migration underway. Coalition PQC interoperability tested.
Level 5: Resilient	Crypto-agile; all crypto remediated	Full CNSA 2.0 compliance. All NSS on PQC. DIB PQC verified. Coalition interoperability achieved. Legacy platforms compensated or decommissioned.

GOVERNMENT & DEFENSE KPI SUPPLEMENT

Leadership-Level KPIs (Quarterly)

- **CNSA 2.0 compliance trajectory:** Percentage of NSS systems on track for 2030/2033/2035 milestones, by system category.
- **HNDL exposure reduction:** Percentage of classified network traffic protected by PQC or hybrid cryptography.
- **Accreditation pipeline:** Number of systems in PQC re-accreditation queue, average processing time, and projected completion date.
- **DIB PQC readiness:** Percentage of Tier 1 contractors with documented PQC migration plans or demonstrated PQC capability.
- **Coalition alignment:** Status of bilateral/NATO PQC interoperability testing and standards coordination.

Operational KPIs (Monthly)

- **Cryptographic inventory completeness:** Percentage of NSS and federal systems with completed cryptographic inventory (per OMB requirements).
- **CBOM coverage:** Percentage of priority systems with completed CBOM at appropriate classification level.
- **PQC pilot progress:** Pilot phases completed vs. planned, with accreditation status for each.
- **PKI migration:** Number of certificates migrated to PQC / total certificates. Smart card PQC compatibility test results.
- **Acquisition compliance:** Percentage of new RFPs/SOWs containing CNSA 2.0 / PQC requirements.

RECOMMENDED IMMEDIATE ACTIONS

- **1. Establish a Quantum Migration PMO with cross-domain authority.** Staff with both classified and unclassified program managers. Anchor the program plan to CNSA 2.0 milestones.
- **2. Complete the NSM-10 cryptographic inventory if not already done.** This is a federal mandate. Prioritize NSS and CUI-handling systems. Use the inventory to identify CNSA 2.0 compliance gaps.
- **3. Update all acquisition templates immediately.** Add CNSA 2.0 compliance requirements to RFPs, SOWs, and technical evaluation criteria for all new procurements. Issue contract modifications for active programs.
- **4. Engage your accreditation authority on PQC re-authorization.** Discuss streamlined re-accreditation pathways for PQC-specific changes. Model the accreditation pipeline capacity needed for your system portfolio.
- **5. Launch unclassified network PQC pilots.** Deploy hybrid PQC TLS on unclassified web services and VPNs. This builds organizational competency, validates tools, and generates accreditation evidence — all without classified system risk.
- **6. Inventory weapons platform cryptographic modules.** For each major platform (aircraft, ships, satellites, tactical systems): what crypto modules are installed, who manufactures them, can they be upgraded, and what is the vendor's PQC timeline?
- **7. Initiate DIB PQC engagement.** Brief your top-10 contractors on PQC expectations. Issue PQC readiness questionnaires. Begin developing DFARS/CMMC PQC flow-down language.
- **8. Coordinate with allies.** Engage Five Eyes cryptographic coordination channels and NATO standards bodies on PQC interoperability. Propose joint PQC testing on coalition test networks.

FURTHER READING

- **Harvest Now, Decrypt Later (HNDL) Risk** — https://postquantum.com/post-quantum/harvest-now-decrypt-later-hndl/
- **Trust Now, Forge Later (TNFL) — The Overlooked Quantum Threat** — https://postquantum.com/post-quantum/trust-now-forge-later/
- **What is the Quantum Threat? A Guide for C-Suite Executives and Boards** — https://postquantum.com/leadership/quantum-threat-executives-board/
- **Post-Quantum Negligence: Legal Risks of Failing to Prepare** — https://postquantum.com/post-quantum/legal-risks-quantum/
- **Mosca's Theorem and Post-Quantum Readiness** — https://postquantum.com/post-quantum/moscas-theorem/
- **Hybrid Cryptography for the Post-Quantum Era** — https://postquantum.com/post-quantum/hybrid-cryptography-pqc/
- **Introduction to Crypto-Agility** — https://postquantum.com/post-quantum/introduction-crypto-agility/
- **PQC Is Necessary, But Not Sufficient** — https://postquantum.com/post-quantum/pqc-not-everything/
- **Engaging and Managing Vendors for Quantum Readiness** — https://postquantum.com/post-quantum/vendors-quantum-readiness/
- **Common Failures in a Quantum Readiness Program** — https://postquantum.com/post-quantum/common-failures-quantum-readiness/
- **Infrastructure Challenges of Dropping In PQC** — https://postquantum.com/post-quantum/infrastructure-challenges-pqc/

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles — including regional and global leadership positions — at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators — including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com