SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

GOVERNMENT & DEFENSE EXTENSION

National Security Systems, Federal Agencies, Defense Industrial Base, and Allied Interoperability Providers – *sector-specific challenges and framework adaptations*

Version 3.0 – September 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

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

COPYRIGHT AND LICENSE

DISCLAIMER

This framework 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. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of PQC as of September 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions; movement between editions is published through the PQC Migration Brief.

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, remains an Initial Public Draft at the date of this edition; the deprecation and disallowance dates it proposes are cited as anchors and re-checked at each release. Federal agencies and their contractors should reference the final version when it publishes.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent document	The Applied Quantum PQC Migration Framework – Universal – v3.0 (September 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 v3.0 and its 8-phase lifecycle; working knowledge of CNSA 2.0 and CNSSP 15, NSM-10, Executive Order 14412 and OMB M-26-15, the NIST SP 800-series, and government/defense security architectures and accreditation processes
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.
Status	Version 3.0 - published September 2026

VERSION HISTORY

Version	Date	Changes
2.0	June 2026	Major version. Three methodological changes: (1) two-track migration model separating key exchange (HNDL) and signature/PKI (TNFL) as parallel tracks; (2) PKI architecture fork with definitive position on Merkle Tree Certificates for public Web PKI; (3) FIPS 140-3 validation gap as hard deployment constraint with environment classification. New Program Foundation sections: SOC Implementation (five detection use cases, four incident response playbooks, five tabletop exercises, three-horizon quantum CTI model), GRC Implementation (17-indicator cascading KRI framework, risk appetite statements, regulatory intelligence process, audit and assurance, GRC-SOC handoff). Expanded Program Foundations: Governance (program leadership, board oversight, three lines of defense), Crypto-Agility (five-dimensional operational discipline with four-year implementation roadmap), Skills & Team Structure (team sizing, build/borrow/buy framework, crypto champion program). Also added: cost estimation methodology, NIST CSWP 39 crypto-agility alignment, 2026–2030 regulatory deadline convergence analysis, multinational hybrid navigation framework, deployment ecosystem status data, algorithm pipeline update (9 additional signature candidates, FN-DSA/HQC status, CNSA 2.0 requirements), objection-handling appendix (Appendix F). All sector extensions updated to v2.0.
2.1	June 2026	Targeted update. Activity 3.3 sequencing harmonized with the two-track model; explicit position on hybrid/composite signatures; algorithm-specific vulnerability weighting added to Phase 3 risk scoring (ECC/RSA quantum resource analysis); SP 800-208 hash-based signatures foregrounded as the deploy-now component of Track B. New: Activity 2.5 (Secure the CBOM and Program Artifacts), Migration Verification & Program Closure section, identity and authentication stack in Track B scope. Added: reference program economics (0.2c), confidentiality-horizon method (1.1), evidence dossier as

Version	Date	Changes
		litigation defense, M&A due diligence, procurement model-language references, additional common failures and benefit arguments. Web PQC adoption datapoint corrected to F5 Labs mid-2025 attribution. Companion book (Quantum Ready) cross-references added. Also added: data-at-rest decision framework (5.6); AI-assisted migration position (5.7) with a Phase 1 tool category; counterparty coordination (7.6); cloud shared responsibility and SaaS (7.7); Accelerated Execution Profile (4.7); risk-weighted coverage KPI; algorithm sovereignty and standards fragmentation; crisis communications and industry information sharing (GRC); skills matrix; role-based reading paths and right-sizing profiles; Appendix G (framework crosswalk); Appendix H (protocol coverage matrix).
3.0	September 2026	Major version, published with Universal v3.0. Crypto-agility as the program's method read for accredited estates: the agility window includes the RMF change process, a pre-approved change class for algorithm and parameter-set changes, "migrated with agility debt" as the expected recorded state for Type 1, platform and satellite entries, and closure at zero unaccepted agility debt. Evidence grades and an enumerated denominator on the sector inventory tracks; the Phase 2 minimum record with the Applied Quantum CBOM Profile as informative carriage; firmness grades and the certificate-authority questions in Phase 7; delivery state in the priority tiers; the maturity supplement on the Universal's 0 to 5 scale; four agility KPIs. Regulatory rebuild: CNSSP 15 milestones (January 1, 2027; December 31, 2030; December 31, 2031) replace the prior date summary as the binding NSS schedule, with the advisory's per-category chart (2030 and 2033, no category at 2035) recorded inside them by its provenance; SLH-DSA removed from the CNSA 2.0 algorithm list; Challenge 11 retitled Concurrent NSS and Civilian Federal Mandates and rewritten on Executive Order 14412, OMB M-26-15 and the Department of War PQC Strategy, each obligation stated once as directed rulemaking; the directed FAR rule and the CBOM guidance mandate placed; the regulatory map restructured with status and enforcement-tier columns and the national rosters replaced by the Global PQC Migration Clock pointer; the CMMC Phase 2 suspension of July 13, 2026 recorded with its instrument chain, the Chief Information Officer's memorandum and Class Deviation 2026-O0025 through

Version	Date	Changes
		Revision 3 of September 3, 2026, and with the CMMC Program rule and DFARS 252.204-7021 stated as unamended. Corrections: the HNDL statement restated as inference with the CISA/NSA/NIST and AIVD statements quoted at their own strength; the FIPS validation-gap subsection rewritten to the per-product rule (CMVP #5247); NCSC UK guidance date corrected to March 2025; NIST PIV working drafts of June 2026 recorded without an issuance date. Requirements register generated as Appendix J. About block aligned to the Universal.

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 government and defense-specific guidance: national security systems under CNSA 2.0 and CNSSP 15, federal civilian systems under Executive Order 14412 and OMB M-26-15, the Defense Industrial Base, and coalition and allied interoperability. 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.

WHAT'S NEW IN V3.0

Version 3.0 of the Government & Defense Extension publishes with Universal Framework v3.0 (September 2026). Crypto-agility is the program's organizing method and measured end state, and this extension reads that ruling for accredited estates: the agility window includes the RMF change process, algorithm and parameter-set changes need a pre-approved change class, "migrated with agility debt" is the expected recorded state for Type 1, platform and satellite entries, and closure requires zero unaccepted agility debt with every remaining entry funded or under a SteerCo-signed exception. Regulatory content states the mechanism and the sector's own instruments with status and enforcement tier; the national rosters are in the Universal's Regulatory Timeline Context and on the Global PQC Migration Clock page.

The sector's regulatory picture changed more than any other's. Challenge 11 is retitled Concurrent NSS and Civilian Federal Mandates and rewritten from two speeds to two concurrent mandate chains: CNSA 2.0 through CNSSP 15 for national security systems (new acquisitions from January 1, 2027; phase-out by December 31, 2030; mandated use by December 31, 2031, with the advisory's per-category chart, 2030 and 2033, inside that schedule), and Executive Order 14412 (June 22, 2026) with OMB M-26-15 (June 24, 2026) for federal high value assets and high-impact systems, with a migration plan due from every civilian agency; the Department of War PQC Strategy (released June 23, 2026) binds every DoW system to the same shape. The directed FAR rule for covered contractors is placed in Challenge 6 and the CBOM minimum-elements guidance mandate in Phase 2, each stated once as directed rulemaking. The extension keeps its two anchors, CNSA 2.0 and the civilian mandate, because they are the two mandate chains that set the sector's dates. The "2033 HW"

summary and the SLH-DSA entry in the CNSA 2.0 algorithm list are corrected, and no chart category carries 2035. Challenge 1 and the regulatory map also carry the CMMC Phase 2 suspension of July 13, 2026 and its instrument chain, from the Chief Information Officer's memorandum to Class Deviation 2026-O0025, at Revision 3 of September 3, 2026, which directs contracting officers to remove or revise CMMC requirements in solicitations and contracts; the CMMC Program rule and DFARS 252.204-7021 stand unamended, and the suspension neither creates nor removes a PQC algorithm requirement.

Alignment section and adaptations. The alignment section is rebuilt on v3.0: the validation subsection now states the per-product, per-operation, per-certificate rule, read per operation and carrying the CNSA 2.0 FAQ's verification-only exception for software and firmware signature verification where it applies, with CMVP certificate #5247 (Go Cryptographic Module, Level 1 software, April 2026, ML-KEM-768 and ML-KEM-1024) and #5497 (Crypto4A QASM, Level 3 hardware, August 2026, carrying ML-DSA), and that a Level 3 validation carrying PQC is not by itself NSS acceptability, the HNDL statement is restated as inference with the CISA/NSA/NIST (August 2023) and AIVD (2023, 2024) statements quoted at their own strength, and three subsections are added: the agility criterion and rehearsal under re-accreditation; evidence grades and the coverage denominator on classified estates; vendor dates and questions in accredited supply chains. The phase adaptations mirror the v3.0 method where this extension already adapts the element: the dual-outcome charter and the Crypto-Agility and Cryptographic Record owners (Phase 0), evidence grades and the enumerated denominator (Phase 1), the minimum record and the CBOM guidance mandate (Phase 2), the added factors restated inside Dimensions 1 and 3 with a delivery-state column (Phase 3), gate records with two results and the Re-Baseline Protocol (Phase 4), the rehearsal per wave (Phase 5), the four-field register with entropy references (Phase 6), and the questionnaire order, the certificate-authority questions and the movement between the two mandate chains' algorithm sets (Phase 7). NIST's June 2026 PIV working drafts are recorded in the identity subsection without an issuance date.

Supplements and currency. The maturity supplement is re-based on the Universal's 0 to 5 scale with the Universal's level names, and the KPI supplement gains the four agility KPIs with sector thresholds. Two immediate actions are added: a Crypto-Agility owner and a first rehearsal. Further Reading adds the June 2026 federal instruments, the July 2026 HNDL analysis and the Global PQC Migration Clock. Every regulatory date was re-checked against its primary source in September 2026; the NCSC UK guidance date is corrected to March 2025. Appendix J lists the extension's own requirements.

WHAT'S NEW IN V2.1

Version 2.1 of the Government & Defense Extension is a major alignment release tracking Universal Framework v2.1 (June 2026). Because the extension moves directly from v1.1, it adopts the Universal v2.0 structural foundations and the v2.1 positions in a single release:

Alignment with Universal Framework v2.1. A new alignment section maps the two-track migration model, the FIPS validation gap and the CNSA-mandated environment class, and the Merkle Tree Certificates position onto government and defense estates, followed by six v2.1 position subsections: the CNSA 2.0 divergence from the Universal composite-signature default; algorithm-specific vulnerability weighting across government PKI; the PIV/CAC identity stack in Track B; SP 800-208 as a mandate rather than an option; CBOM protection under classification; and verification, decommissioning, and accreditation evidence. The remaining Universal v2.1 additions are sector-

neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

New and extended challenges. Challenge 11 (Two-Speed Federal Mandates: NSS Hard Gates, Civilian Discretion) addresses the 2026 bifurcation of US federal PQC policy. Challenge 1 gains the January 1, 2027 CNSA 2.0 acquisition gate and the late-2026 compliance sequence (FIPS 140-2 certificates to Historical status, CMMC 2.0 Phase 2). Challenge 9 gains the concrete allied divergence: European hybrid mandates against the NSA standalone position.

Currency updates. The regulatory alignment map and Further Reading reflect the June 2026 state, including the CNSA 2.0 article series published in May 2026. A cross-reference to the companion book, Quantum Ready, was added.

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 Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, 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.org, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

Two sibling Applied Quantum properties carry work this framework cites rather than repeats. The Applied Quantum CBOM Profile, the property taxonomy layered on CycloneDX that Phase 2 cites by minimum version, publishes at CBOMProfile.org. The Cryptographic Concentration Framework, which measures cryptographic concentration beneath the vendor layer and consumes a Profile-conforming CBOM, publishes at CCFramework.org. Both are open under CC BY 4.0 and follow this framework's sector taxonomy.

This framework is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.com). Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, for the roles and training levels described in Skills & Team Structure.

The PQC Migration Brief (pqcmigrationbrief.com) carries corrections, standards and regulatory movement between editions, and the current jurisdiction roster is maintained on the Global PQC Migration Clock page on PostQuantum.com; the framework itself remains free and ungated.

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. In government and defense the PQC migration is mandated, with dated milestones, by the authorities that define the cryptographic standards, and the requirements are particularly explicit and mission-specific.

Mandatory PQC Timelines Set by the Standards Authorities

The sector's PQC migration deadlines are explicit, mission-specific and set by the standards authorities themselves. CNSA 2.0 (Commercial National Security Algorithm Suite 2.0), published by NSA, requires all national security systems (NSS) to move to quantum-resistant algorithms. CNSSP 15 (updated 2024, published March 2025) makes the schedule binding: new NSS acquisitions CNSA 2.0 compliant from January 1, 2027, equipment and services that cannot support CNSA 2.0 phased out by December 31, 2030, and CNSA 2.0 algorithms mandated for use by December 31, 2031, with the advisory's per-category chart running to 2033 for the last custom and legacy systems, recorded with its own provenance and status (Challenge 1). These requirements are 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, May 4, 2022) directed federal agencies to inventory their cryptographic systems and develop migration plans. OMB M-23-02 (November 18, 2022) required agencies to submit prioritized inventories of quantum-vulnerable systems by May 4, 2023 and annually thereafter until 2035. In June 2026 the civilian

mandate gained dates of its own and a required migration plan per agency (Challenge 11). Similar mandates exist or are emerging in the UK, EU, Australia, Canada, and other Five Eyes and NATO nations.

These policies already supply the executive mandate Phase 0 requires. The implementation phases must satisfy government accreditation and compliance requirements that commercial enterprises do not face, which adds scope and duration to every subsequent phase.

HNDL and the Classification Horizon

Harvest Now, Decrypt Later (HNDL) is an active planning risk in this framework. The basis is the one the Universal states: the means, motive, opportunity and precedent for passive collection are demonstrated. The harvest itself cannot be observed. Finding no trace of it is the expected condition (Two-Track Migration Model; Appendix F). The precedent for this sector is in NSA's own VENONA release: Soviet traffic collected in the 1940s was still being worked when the program closed in 1980.

The agencies that would know are quoted at the strength they used. CISA, NSA and NIST wrote in their joint factsheet of August 21, 2023 that threat actors "could be targeting data today that would still require protection in the future" (Quantum-Readiness: Migration to Post-Quantum Cryptography). The Dutch AIVD, with CWI and TNO, wrote in the second edition of its PQC Migration Handbook that secured data "can be intercepted today and then deciphered with a quantum computer from Q-Day onwards" (AIVD, December 3, 2024; first edition April 2023). Neither statement describes an observed collection program, and this extension does not report one.

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 different from commercial enterprises.

Bifurcated NSS and Non-NSS Environments

Government organizations operate in at least two distinct security domains: national security systems, which the statute defines by mission function as well as by classification and which run at one or more classification levels, and non-NSS federal systems, including systems that handle Controlled Unclassified Information (CUI, which is unclassified) and public-facing systems. Cryptographic requirements, accreditation authorities, vendor bases, and migration timelines vary across domains.

National security systems must follow NSA's CNSA 2.0 through CNSSP 15; non-NSS federal systems follow NIST standards under the civilian mandate (Challenge 11). Which

domain a system is in is settled by the boundary determination Challenge 11 requires. The classification marking alone does not settle it. 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 moved the exposure 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 in Service for 20 to 50 Years

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. The aircraft's 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 whose migration timelines,

approved algorithms (CNSA 2.0 for US/Five Eyes, national algorithms for some European and Asian allies), and classification authorities diverge.

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 parameter sets: ML-KEM-1024 for key establishment; ML-DSA-87 for digital signatures in any use case, including firmware and software signing; LMS and XMSS allowed for signing firmware and software, with LMS SHA-256/192 recommended and the transition preferred to begin with them; AES-256 for symmetric encryption; and SHA-384 or SHA-512 for hashing. HSS and XMSS^MT are not allowed for NSS.

SLH-DSA is not approved for any NSS use, and HashML-DSA is not allowed at present (NSA CNSA 2.0 FAQ, Version 2.1, December 2024). CNSA 2.0 specifies the only algorithms approved for national security systems. The binding schedule is CNSSP 15 (updated 2024, published March 2025): new NSS acquisitions CNSA 2.0 compliant from January 1, 2027; equipment and services that cannot support CNSA 2.0 phased out by December 31, 2030; CNSA 2.0 algorithms mandated for use by December 31, 2031, each unless otherwise noted in the applicable profile.

The per-category chart comes from a different instrument with a different status. NSA's CNSA 2.0 advisory of September 2022 predates the CNSSP 15 update and is guidance. Its chart names 2030 for software and firmware signing and for networking equipment (VPNs and routers). It names 2033 for three groups: web, cloud and operating-system platforms; niche equipment; and custom applications and legacy equipment. No chart category carries 2035.

The chart's 2033 dates fall after CNSSP 15's mandated-use date of December 31, 2031. The chart does not extend the policy. A system's binding date is the CNSSP 15 date or the date its applicable profile notes. The chart date is recorded with its provenance, as the advisory's planning guidance for that category.

A system that misses these dates is out of compliance with the policy on which its authorization is conditioned. The authorizing official records the consequence. The authority to operate (ATO) can be denied or revoked; a new system that cannot meet the acquisition gate is not accredited; disconnection from classified networks is among the available remedies. Unlike commercial compliance frameworks where penalties are financial, the consequence of non-compliance with CNSA 2.0 is that the system may lose its authorization to be used for its mission.

Framework Impact: Phase 0 must anchor the entire program timeline to the CNSSP 15 milestones. Phase 4 must build a roadmap that meets the acquisition gate, the phase-out date and the mandated-use date, with the advisory's per-category dates recorded against each category as guidance and with margin for testing and accreditation.

The nearest gate is procurement, and it is no longer distant. On January 1, 2027, a new acquisition for a National Security System in scope of CNSSP 15 must support CNSA 2.0 algorithms (ML-KEM-1024 key establishment, ML-DSA-87 signatures), unless the applicable profile notes otherwise. The gate runs on the acquisition event, not on the delivery date alone. Record which event the applicable policy or profile attaches the requirement to: the solicitation, the award, or a delivery order placed under an existing vehicle.

A system procured through an event after the gate and delivered without those algorithms is non-compliant on arrival. A delivery under a pre-gate award is read against the terms and profile that bind that contract, and the December 31, 2030 phase-out and December 31, 2031 mandated-use dates reach it regardless, so no system is grandfathered out of the schedule as a whole. Two other late-2026 dates were expected to compound the gate. One has passed and one is suspended.

On September 21, 2026, NIST moved every remaining FIPS 140-2 certificate to the Historical list; CMVP supports the purchase and use of those modules for existing systems, and their exclusion from procurement for new federal systems follows from agency and contractual policy, as the validation subsection states. CMMC 2.0 Phase 2, which was to begin third-party assessment of most Level 2 defense contractors on November 10, 2026 with FIPS-validated cryptography as a prerequisite, was suspended by the Department of War on July 13, 2026, with pending and future implementation milestones held in abeyance until further notice.

The instrument is the Department of War Chief Information Officer's memorandum "Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements," dated July 13, 2026, which:

- permits requiring activities to include CMMC Level 1 (Self) or Level 2 (Self) assessments in all procurement requests and requirement documents;
- requires baseline compliance with NIST SP 800-171 Rev 2 in accordance with the clause at DFARS 252.204-7012;

- suspends the November 2026 CMMC Phase 2 transition;
- requires program managers and requiring activities to initiate amendments to active solicitations and provide them to the cognizant contracting officer;
- requires contracting officers to issue the corresponding solicitation amendments as soon as practicable;
- for existing contracts that carry these requirements, requires contracting officers to remove them by modification before the next option period is exercised or at the next scheduled administrative modification.

The CMMC Reform Task Force's 60-day review of the program expired on September 11, 2026. The task force sent its recommendations to the Department CIO, and they have not published at this edition. The Department's CMMC program page states the current status (DoW CIO CMMC program page).

The instrument that states the direction. The direction reached the acquisition workforce three days after the memorandum, in Class Deviation 2026-O0025, Revision 2 (Office of the Assistant Secretary of War (Acquisition and Sustainment), issued July 16, 2026, effective immediately, revising and superseding Revision 1 of June 29, 2026).

Revision 3, issued September 3, 2026 by the same office and signed by Principal Director John M. Tenaglia, revises and supersedes Revision 2 and is the current instrument at this edition. Revision 3 repeats the July 13 CMMC direction word for word in the clause's CMMC section, and writes the suspension into the revised DFARS Part 240 text. Its principal new changes are elsewhere, in information security and supply chain security.

Three things about the deviation are worth stating plainly:

- It implements the memorandum and directs contracting officers to collaborate with requiring activities to remove or revise the CMMC requirements in new and existing solicitations and contracts.
- It is not a CMMC instrument. It is the Revolutionary FAR Overhaul deviation for FAR Part 40 and DFARS Part 240, and its principal subject at Revision 2 was a court order on the 1260H treatment of Alibaba entities. The CMMC direction is one of six things it implements.
- It remains in effect until rescinded or incorporated into the FAR, DFARS and DFARS PGI.

What is suspended, and what is not. What is suspended is the Department's exercise of its discretion to designate the higher assessment levels, not the regulation.

- 32 CFR Part 170 is unamended, and no Federal Register document has issued.
- DFARS 252.204-7021 remains in the deviated Part 240 at 240.371-5, so the CMMC Program rule and the clause stand as written.
- During the suspension, requiring activities may designate CMMC Level 1 (Self) and Level 2 (Self), but not Level 2 (C3PAO) or Level 3 (DIBCAC).

- Phase 1 self-assessment, in force since November 10, 2025, continues, as do the DFARS 252.204-7012, NIST SP 800-171 Rev 2 and FAR 52.204-21 obligations.

The deviated text contains them as well. It issues the safeguarding clause at DFARS 252.204-7012 in deviated form, and names SP 800-171 Rev 2 by URL at paragraph (b)(2)(i). The duty to protect CUI and its FIPS-validated-cryptography control are therefore imposed by the clause and not by Department policy alone, and the suspension neither creates nor removes a PQC algorithm requirement.

How to grade it. An unamended rule whose discretionary application is suspended is a different firmness grade from a withdrawn rule. The suspension is now written into a class deviation and not into memoranda alone, which is firmer than memoranda and still short of rulemaking. That is the same distinction this framework draws between directed rulemaking and an issued clause.

A contractor reads the assessment level designated on its own solicitation, and expects the solicitation amendments and contract modifications the deviation directs. This edition does not substitute a replacement date.

Defense acquisition cycles run 18 to 36 months from requirements definition to delivery, which means requirements written today determine compliance status at delivery in 2027 and 2028. Remediation after the fact is not a patch. It is a cryptographic architecture redesign, potentially including new hardware where existing components cannot handle ML-KEM-1024 and ML-DSA-87 sizes.

CHALLENGE 2: CLASSIFIED SYSTEM ACCREDITATION OVERHEAD

A cryptographic change on a classified system is assessed under the authorization process that governs the system (the Risk Management Framework under NIST SP 800-37 for US systems, or the equivalent national process) and ends in a recorded authorization decision. The path depends on the change. An algorithm or parameter-set change inside a class the authorizing official has pre-approved is recorded and monitored under the existing authorization; a change that alters the security architecture or affects controls at the boundary needs reassessment of the affected controls before the decision; a change that moves the system's risk beyond what the authorizing official accepted needs a broader reauthorization.

Every cryptographic change must have an impact assessment and a recorded authorization decision. No change forfeits the authorization by itself, and none is exempt from the assessment. Plan 12 to 24 months for a broader reauthorization of a complex system as a planning assumption, replaced by the authority's own figure once the pre-approved change class is negotiated (Phase 4).

The accreditation pipeline will become a bottleneck as hundreds or thousands of systems bring cryptographic changes to it in the same years, whichever path each

change follows. 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, for each system, which authorization path its cryptographic changes follow (pre-approved change class, reassessment, or reauthorization) and the time each path takes. Phase 6 must prepare accreditation documentation packages in parallel with technical migration. Engage accreditation authorities early to negotiate a pre-approved change class for algorithm and parameter-set changes and expedited handling for changes that need reassessment or reauthorization.

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 and hardest-to-migrate 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 approved by NSA as Type 1 products. Four assurance mechanisms appear in this sector and each has its own authority and scope: Type 1 approval is NSA's certification of a product to protect classified information; Commercial Solutions for Classified (CSfC) is NSA's program for layered commercial products, whose components are commercial products evaluated by NIAP and listed against a capability package; NIAP Common Criteria evaluation tests a commercial product against a protection profile; and FIPS 140-3 validation is the CMVP's validation of a cryptographic module.

None substitutes for another, and the record for each device names which of them it holds. Replacing or upgrading a Type 1 module requires coordination with the weapons system program office, the module vendor, NSA as the approving authority, 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. A satellite already in orbit is not a fixed HNDL exposure by virtue of being in orbit, and classical cryptography is not one algorithm class: what the space link actually uses decides. Inventory it before scoring it. Record the cipher that protects the link and how its keys are established and provisioned. Record separately what authenticates the link and what verifies payload firmware.

Record whether the payload's software or protocol stack can be updated on orbit. Where the link depends on vulnerable public-key establishment, recorded traffic has HNDL exposure for the full period of its confidentiality obligation. That exposure is fixed for the satellite's remaining life only where no available software or protocol change removes the dependency. Where confidentiality depends on symmetric protection with pre-provisioned keys, Shor does not reach it, and the classical signature, authentication and firmware-verifier dependencies are carried separately on the signature track rather than treated as covered.

A PQC gateway at the ground station cannot protect the space leg on its own: the link between the ground station and the payload is protected by PQC only if the payload can participate in the exchange. Draw each link separately. The terrestrial segment from the ground station into the network migrates with Track A. The space segment stays on the

cryptography the inventory found unless the payload's protocol and update capability admit a PQC layer over it.

That residual segment is recorded as exposed in the verification record, or the risk is accepted for the satellite's remaining operational life with the acceptance recorded (Activity 7.4).

Framework Impact: Phase 1 must inventory all satellite and space system cryptographic implementations. Phase 4 must separate in-orbit systems, scored on the space-link protection and update capability the inventory found, from future-launch systems specified as PQC from launch. 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 encrypt stored data, data in transit (VPNs, TLS) and data in processing (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 (a prime contractor and a small machine shop can hold the same CUI under the same clause), the cost burden on small businesses, and the challenge of enforcing cryptographic standards through contract mechanisms. CMMC and DFARS 252.204-7012 set cybersecurity requirements, but neither yet includes PQC-specific provisions.

The lever has changed since the June 2026 edition. Executive Order 14412 (June 22, 2026) directs the Federal Acquisition Regulatory Council to publish, within 180 days, a proposed rule requiring covered contractors to comply by December 31, 2030 with NIST's FIPS, including the FIPS that incorporate PQC algorithms (section 6(c); White House text; Federal Register Vol. 91 No. 121).

The direction is rulemaking, not a rule: no covered-contractor definition, threshold or contract clause exists until the FAR Council publishes. The proposed rule had not been published at this edition, so it creates no obligation and enters planning only as a signal. Covered contractors can read a directed rule with a date as notice of what procurement is expected to require. It does not bind them, and a published proposed rule would not bind them either.

Existing contract terms continue to govern on their own terms until a final rule takes effect with a defined scope and effective date. The signal is still usable: a prime that writes ML-KEM and ML-DSA support, the agility questions and firmness-graded dates into its subcontracts now is ahead of the clause, without waiting for its final text. The

contractor the rule reaches is the one that reads CNSA 2.0 as an obligation for national security systems only.

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 (STANAG 4774/4778 for metadata binding, KMI/KMS for key management) depend on the signature and key-establishment algorithm set beneath them, and PQC changes that set. NATO's Quantum Technologies Strategy (summary published January 2024) commits the Alliance to transitioning its cryptographic systems to quantum-safe cryptography through its committees and bodies (NATO official text). No PQC standardization agreement is identified in the public record at this edition, so coalition planning uses dual-stack windows and the counterparty pattern (Activity 7.6) in the absence of a NATO date. 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 far larger than classical certificates. An ML-DSA-87 certificate carries a 2,592-byte public key and, where its issuer signs with ML-DSA-87, a 4,627-byte signature (FIPS 204), against 256 bytes for each of the two elements in an RSA-

2048 certificate, so each certificate grows by several kilobytes and a chain by a multiple of that. 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 algorithms developed or evaluated nationally 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.

The divergence is now concrete. Germany's BSI and France's ANSSI recommend hybrid constructions in their guidance, framed as recommendations rather than as a general obligation on German or French organizations; ANSSI requires hybridization for a product seeking its security visa, at the phase-2 evaluation. Both accept a broader algorithm menu than CNSA 2.0, including FrodoKEM and SLH-DSA in European guidance, while NSA specifies standalone lattice algorithms at the highest parameter sets and does not approve SLH-DSA for any NSS use.

Australia's ASD guidance ceases traditional asymmetric cryptography in Australian Government systems by 2030, and China's SM national-algorithm series is expected to extend into domestic PQC selections independently of the NIST suite. Read each deployment against the exact national or procurement profile that binds it rather than against a national position in general (Universal Appendix D). The consequence for

coalition operations, multinational programs, and any agency procuring from allied suppliers: divergent cryptographic postures must run concurrently, which makes crypto-agility across algorithm families and postures an architectural requirement.

The Universal Framework's Algorithm Sovereignty and Standards Fragmentation section and this extension's alignment subsection on the CNSA 2.0 divergence carry the planning consequences.

The program keeps an applicability record per system. A national-position roster is stale on the day it is printed. The accreditation package and the vendor questionnaire need the per-system record. For each system the record states which regime binds it (CNSA 2.0 through CNSSP 15; a partner nation's national algorithm mandate; both, for a coalition gateway), the algorithm families and parameter sets that regime requires, the NIAP protection profile or CSfC capability package version the deployment claims, and the date each entry was verified against its source.

The Universal's non-standardized-algorithm rule treats a national algorithm mandated under a documented regime as standardized by an equivalent authority for the purposes of approved-mode use, and this record is the documentation the rule asks for (Activity 7.3). The current roster of national positions is maintained on the Global PQC Migration Clock page.

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.

CHALLENGE 11: CONCURRENT NSS AND CIVILIAN FEDERAL MANDATES

US federal PQC policy is governed by two concurrent mandate chains, each with its own dates. National Security Systems remain bound to CNSA 2.0 through a governance chain that operates independently of the executive orders aimed at civilian agencies (NSD-42, NSM-8, NSM-10, CNSSP 15), with its milestones stated in Challenge 1. Federal civilian systems that are high value assets or high-impact systems, excluding NSS, are bound by Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (June 22, 2026): PQC for key establishment by December 31, 2030, PQC for digital signatures by December 31, 2031, a PQC migration lead in each agency who reports to the CIO and owns the cryptographic inventory and the migration plan, and a plan submitted to OMB and the National Cyber Director (sections 2(h), 4(a) and 4(b); White House text; Federal Register Vol. 91 No. 121).

OMB Memorandum M-26-15, Execution of the Migration to Post-Quantum Cryptography (June 24, 2026), which does not apply to NSS, sets the plan's deadline at 120 days from the memorandum's own date, October 22, 2026 (the clock runs from June 24, not from the order's June 22). The memorandum phases the work as Strategy, Planning and Discovery (2026–2027), Pilots and Early Migration (2027–2028), Prioritized Migration (2028–2030, covering key establishment for high value assets and high-impact systems), Signature Migration (2031) and Full Migration (2035), with the objective of mitigating as much quantum risk as feasible by December 31, 2030.

The memorandum also requires the plan to align with NIST IR 8547, to name the discovery methods and automated tools behind the inventory, and to have a plan for a crypto-agile architecture with the algorithm choice held in configuration rather than compiled into the binary (OMB M-26-15). Agency discretion is confined to systems below the high-impact threshold.

The Department of War's PQC Strategy (released June 23, 2026) binds every DoW system, NSS and non-NSS, to one shape: support PQC or be phased out by December 31, 2030 and use PQC by December 31, 2031, unless otherwise noted, with CNSA 2.0 as the NSS baseline and five lines of effort from governance to device deployment (DoW PQC Strategy). The companion order of the same day, Executive Order 14413 on quantum innovation, sets no migration obligation.

The June 2026 edition drew a valid distinction, now with a corrected premise: the two mandate chains differ in authority, algorithm set and accreditation regime. Both have dates. Defense Industrial Base suppliers, agencies operating mixed estates, and shared-service providers may face both regimes at once, per system and per contract. A system inside an NSS authorization boundary, or a component of one, meets the CNSA 2.0 requirements regardless of what the civilian posture permits; serving a government customer, handling CUI, or connecting to a national security system does not bring an enterprise's other systems under CNSA 2.0, and the boundary determination below is

what decides. A civilian system that is a high value asset or a high-impact system meets the executive order's dates.

Framework Impact: Phase 0 must record a system-boundary determination for every system: whether it is a national security system under the statutory definition (44 U.S.C. §3552(b)(6), which reaches a system by its function – intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment integral to a weapon or weapons system, or the direct fulfillment of military or intelligence missions, excluding routine administrative and business applications – as well as by the classification of the information it holds), the authority that governs it, the profile that applies, and the contract flow-down that imposes the requirement, with civilian federal, NSS, CUI-contractor and commercial systems kept as separate populations.

Classification alone does not decide it. Budget, sequencing and accountability follow from that determination. Phase 4 milestones anchor to the stricter applicable mandate; planning to the NSS dates is the defensible default for a system whose determination is NSS or unresolved, and the civilian mandate's separate key-establishment and signature dates place the two tracks on the mandate's own shape (Two-Track Migration Model in the alignment section). Phase 7 applies the January 2027 acquisition gate to every active solicitation now. Systems specified today deliver into the post-gate regime.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V3.0

Universal Framework v3.0 (September 2026) is a major version. Readiness against dated obligations is the mandate; crypto-agility is the method. The PQC migration is the first exercise of a standing capability to change cryptography on a planned date. V3.0 introduces four groups of changes. This section and the phase adaptations state how each group applies to government and defense.

- **Method.** The charter states two outcomes together (Phase 0). Ten workstreams separate Discovery, a project with an end, from the Cryptographic Record, a permanent capability with a named owner. Crypto-Agility is funded as a workstream from Year 1 (Activity 0.3). Every migration gate and wave exit applies the agility criterion (Activities 4.6 and 5.4), every wave includes an algorithm-change rehearsal (Activity 5.2), Phase 3 produces an agility-debt register, and the program closes only on the closure proof: zero unaccepted agility debt and a rehearsed second algorithm change per track inside the agility window (Migration Verification & Program Closure).

In accredited estates the program office carries these elements through the accreditation process. The subsections on the agility criterion and on verification state the effect on the window, the recorded states and the closure proof.

- **Records and evidence.** Every discovery finding is recorded with an evidence grade, E1 to E5, and coverage is measured against an estate enumerated before discovery ran, with a signed accepted-gaps register at gate G1 → G2 (Activity 1.2). The CBOM record is the framework's own minimum record (Activity 2.1). The Applied Quantum CBOM Profile, v1.0-RC or later, is cited as informative carriage and never required. Questions of concentration are cross-referenced to the Cryptographic Concentration Framework. No document in the set computes a concentration figure.
- **Vendor governance.** Every vendor date is graded for firmness (committed, forecast, announced, unknown). The questionnaire opens with the two agility questions and

the firmness question; certificate authorities answer four further questions. No non-standardized public-key algorithm enters approved-mode use, with the sovereignty carve-out this sector relies on. Provider roadmaps are read under Activity 7.7. Counterparties that cannot be contractually compelled follow Activity 7.6 (Activities 7.2, 7.3 and 7.5 to 7.7).

- **Corrections and currency.** Two positions were corrected in the open at v3.0. HNDL is stated as inference from demonstrated capability rather than as observed harvesting, and the v2.0 statement that no validated module offered approved PQC services was false when published (CMVP certificate #5247, April 2026). This extension states both corrections, in the HNDL section and in the validation subsection. The Universal's standards currency is September 2026, and this extension's dates are re-checked to the same month.

The remaining Universal positions apply as written, with two notes carried forward: the counterparty coordination pattern in Activity 7.6 is the general case of coalition and allied interoperability (Challenge 7), applied with the diplomatic and alliance channel standing in for the commercial relationship owner; and the cloud shared-responsibility treatment in Activity 7.7 applies inside sovereign and accredited cloud regions exactly as it does in commercial cloud, with accreditation-program attestations feeding the vendor register and boundary verification still meaning observed algorithm negotiation at the network layer.

Two-Track Migration Model in Government and Defense

Track A (Confidentiality / Key Exchange): TLS on public-facing citizen services, agency VPN and IPsec estates, links between agencies and sites, and cross-domain transport. This track addresses HNDL against the canonical adversary: nation-state collection programs with indefinite patience and decades-long classification horizons. CNSA 2.0's network-equipment dates (support and prefer by 2026, exclusive use by 2030) put Track A on the most aggressive infrastructure schedule in any sector.

Track B (Integrity / Signatures / PKI): software and firmware signing (already under CNSA 2.0 mandate), PIV/CAC credential signatures, Federal PKI hierarchies, weapons system and cross-domain solution signatures, and signed records whose validity must survive for decades. The CNSA 2.0 category milestones effectively assign deadlines per track; map each system's category before sequencing. The federal civilian mandate now sets separate dates of its own for key establishment and for signatures (Challenge 11), which places the two tracks on the mandate's own shape: an agency planning to the mandate plans in this framework's native form.

Validation Decided Per Product in FIPS-Required and CNSA-Mandated Classes

The Universal Framework's Deployment Environment Classification places most of the government estate in its two most constrained classes, FIPS-required and CNSA 2.0-mandated. It decides validation per product, per operation and per certificate, independently of the calendar.

PQC enters production in these classes through a module whose FIPS 140-3 certificate lists the operation as an approved service, with one exception the CNSA 2.0 FAQ states.

Read the requirement per operation. Key generation, signing and key establishment are read against the module's approved services. For software and firmware signature verification-only implementations, the FAQ accepts CAVP algorithm validation in the case it states, without a module certificate covering that operation. The signing side stays on the stricter rule. Each deployment records which operation it performs before it decides which evidence it needs.

As of September 2026 the CMVP validated-modules list includes post-quantum operations as approved services in software and in hardware, and the two certificates this framework cites are not interchangeable evidence.

Property	Certificate #5247	Certificate #5497
Module	Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC)	QASM Cryptographic Module (Crypto4A Technologies, hardware version QASM 1.1, firmware 5.0.1.158)
Type and level	FIPS 140-3 Level 1 software module	FIPS 140-3 Level 3 multi-chip standalone hardware module
Dates	Validated April 27, 2026; updated July 7, 2026	Initially validated August 19, 2026; updated August 21, 2026; sunset date August 18, 2031
ML-KEM	KeyGen and EncapDecap, which covers encapsulation and decapsulation, at ML-KEM-768 and ML-KEM-1024 only, not ML-KEM-512	KeyGen and EncapDecap at ML-KEM-512, -768 and -1024
ML-DSA	None	KeyGen, SigGen and SigVer at ML-DSA-44, -65 and -87

Property	Certificate #5247	Certificate #5497
Other approved algorithms	Not applicable	SLH-DSA across all twelve parameter sets, and LMS

Two qualifications from #5497's Security Policy apply to every citation of it. The first is that §2.7 states that the module does not establish SSPs using an approved KEM, and instead exposes ML-KEM functionality for an external application to use as part of an approved KEM. The second is that HSS key generation, signing and verification are vendor-affirmed, not CAVP-tested.

Every ML-DSA statement in this extension is evidenced by #5497 alone. A module that lists PQC only among its non-approved services does not count, and the planning rule runs per product and not per calendar.

For each deployment, record:

- the governing requirement
- the module and version
- the certificate number and status
- the approved services the certificate lists
- the required security level
- the tested operating environment

Then confirm that the intended cryptographic operation is covered, and set the production date per system from the certificate that covers its operation.

A FIPS 140-3 Level 3 validation carrying post-quantum algorithms is not by itself acceptability for a national security system. Certificate #5497 demonstrates the gap. Its firmware update service verifies with ECDSA and with HSS, and CNSA 2.0 does not allow HSS for NSS. In the FIPS-required class the certificate settles the validation question. In the CNSA 2.0-mandated class the algorithm set the certificate covers is read against the CNSA 2.0 profile that binds the system, and the assurance mechanism the system's authority requires (Challenge 4) is a separate question from both.

Two dates bind these classes harder here than elsewhere, one past and one ahead. On September 21, 2026, the CMVP moved every remaining FIPS 140-2 certificate to the Historical list, the date stated in the maintained prose of NIST's FIPS 140-3 Transition Effort page (its transition-schedule table, stamped 2021, prints September 22, 2026). CMVP states a permission for those modules, not a prohibition. It supports their purchase and use for existing systems and notes that the selection of FIPS 140-3 modules may be limited for several years.

CMVP recommends that purchasers consider every module on the validated-modules search page regardless of whether it was validated against FIPS 140-2 or FIPS 140-3.

The exclusion of a Historical module from procurement for a new system follows from that scoping to existing systems and from agency and contractual policy, not from a CMVP prohibition. Every in-flight solicitation is checked against the policy that binds it, and whether an existing deployment on a Historical certificate may continue is decided separately under the applicable agency or contractual risk policy.

On January 1, 2027, new NSS acquisitions must be CNSA 2.0 compliant (Challenge 1). Pilot and staging work runs now in unrestricted enclaves (development, test and unclassified research networks). Engineering readiness must not be the constraint on the certificate date. The documented-risk-acceptance route open to commercial FIPS-aware deployments has far narrower room inside NSS, where CNSSP 15 compliance is not the agency's to waive. Where an accreditation authority accepts an interim posture, the acceptance is recorded with the module, its certificate status and the date on which the posture ends.

Merkle Tree Certificates and Public-Facing Services

The Universal position on Merkle Tree Certificates concerns the public Web PKI, and it applies to government exactly at the boundary where government meets the public: citizen-facing web services whose certificates chain to public roots will follow the browser vendors' fork, on their schedule. The Federal PKI and agency-internal hierarchies are private PKIs the government controls. They follow CNSA 2.0 dates and are unaffected by the MTC trajectory. Plan the two estates separately and do not let either schedule masquerade as the other.

Hybrid and Composite Signatures Under CNSA 2.0

The Universal Framework's default (Activity 5.2) is composite or dual signatures, with solo ML-DSA recorded as a risk decision. CNSA 2.0 points the other way: standalone ML-DSA-87 is the specified endpoint for NSS, with hybrid constructions tolerated transitionally for key establishment in protocols that cannot yet operate without classical algorithms, and CNSA 2.0 algorithms present and preferred even then. For NSS and CNSA-bound systems, the Universal default is therefore overridden by mandate. Record it as a mandated divergence.

For non-NSS government systems and the commercial side of DIB estates, the Universal composite default stands. Multinational and coalition programs must satisfy both postures at once. European partners mandate hybrid (Challenge 9). The crypto-agility architecture must serve both without forking the codebase.

Algorithm Weighting Across Government PKI and Legacy Suites

The Universal position that quantum attack cost tracks key size, not classical strength (Activity 3.1), applies directly to government estates. ECDSA P-256 and P-384 are everywhere (PIV/CAC credentials, Suite B-era deployments, TLS), and they must not be

sequenced later than RSA systems on the assumption that elliptic curves are the stronger cryptography. At equal mission sensitivity, ECC-protected systems are sequenced at least as early as RSA-protected ones. Combined with classification horizons that run to fifty years, the weighting analysis and the confidentiality-horizon method (Universal Activity 1.1) jointly determine Phase 3 ordering for government data.

PIV, CAC, and Federation as Track B

The Universal's identity and authentication scope in Track B is, in government, the credential estate itself: PIV and CAC signature operations, derived credentials on mobile devices, PKINIT in Active Directory-heavy enclaves, ICAM federation token signing, and FIDO2 deployments now rolling out across agencies. All of it is Track B. Most of it terminates in card and token hardware, and the credential wave has three separately planned parts: card and token stock with the applet capability to hold ML-DSA keys and certificates; issuance and reissuance through the card management systems, at the issuers' throughput; and reader and middleware compatibility on every relying system, which changes as software on its own schedule.

Inventory the credential estate as its own track, and plan reissuance and re-enrollment alongside the PKI migration that underpins it. On June 12, 2026 NIST released initial working drafts of SP 800-73-6 (Parts 1 and 2) and SP 800-78-6 that add ML-DSA and ML-KEM to the PIV specifications under a dual-stack model: existing classical keys and data objects stay, and new key references, certificate containers and data objects carry the PQC credentials (NIST, PQC Updates to the PIV Standards).

The drafts name no closing comment date and no issuance date for PQC PIV credentials; OMB M-26-15 separately directs GSA to convene an inter-agency working group on FICAM modernization for PQC. Plan the credential wave against the dual-stack model, record the issuance date as unknown until a card issuer commits to one, and grade it under Activity 7.5 when it arrives.

SP 800-208 Signing Under the CNSA 2.0 Schedule

In the Universal Framework, SP 800-208 stateful hash-based signatures are the deploy-now component of Track B, under the conditions of section 8 of that publication: key and signature generation inside a hardware module with at least Level 3 physical security, no export of the private key in any form, and signing state managed inside the module, with backup, replication and failover designs that cannot reuse a state. A deployment that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

State safety is an acceptance item evidenced inside the conforming implementation, not an inference from "HSM-backed" or "controlled ceremony": the supported parameter sets, exhaustion monitoring, atomic state handling, and tested backup, replication, crash-recovery and concurrent-signing behavior. The validated LMS implementation

this framework can evidence is CMVP certificate #5497, whose CAVP entry covers one parameter set, LMS_SHA256_M24_H5 with LMOTS_SHA256_N24_W2, while the module's own security-function table lists more.

XMSS support is materially rarer than LMS, and the CMVP search form offers no filter for either scheme, so the validated population cannot be enumerated and no broader claim is made in either direction. The deploying organization verifies parameter-set coverage on the specific certificate rather than inferring it from the algorithm's presence, and a signer for NSS also reads its parameter set against the CNSA 2.0 profile. HSS and XMSS^MT are not allowed for NSS.

In government the signing category is on a schedule: CNSA 2.0's per-category chart sets software and firmware signing to support and prefer CNSA 2.0 algorithms by 2025 and to use them exclusively by 2030, and for that category CNSA 2.0 allows LMS and XMSS, with LMS SHA-256/192 recommended and the transition preferred to begin with them, and approves ML-DSA-87 for all signature use cases including firmware and software signing (NSA CNSA 2.0 FAQ, Version 2.1, December 2024). The signing module's certificate reference, the parameter sets its certificate covers, and its entropy validation go in the Phase 6 register.

Securing the CBOM Against Nation-State Collection

Universal Activity 2.5 treats the CBOM as a high-value intelligence target. In government the case is not hypothetical: an aggregated CBOM with risk scores is a nation-state collection priority, and portions of it may themselves require classification or CUI handling once aggregated. Apply Activity 2.5 at its highest setting: need-to-know partitioning by enclave, access logging, and SOC/SIEM integration designed inside the accreditation boundary from the initial architecture. Before the CBOM is assembled, the information security officer determines at what point the assembled inventory exceeds the classification of its parts.

Verification, Decommissioning, and Accreditation Evidence

The Universal's Migration Verification & Program Closure section defines the evidence standard for declaring a system migrated and the closure proof for ending the program. In government that evidence has a second customer, the accreditation process. Closure artifacts (observed negotiation evidence, negative tests showing classical-only negotiation refused, destruction certificates for classical key material, configuration lockdown records, rehearsal records with their segment timings) feed RMF packages and ATO maintenance directly, so generate them in accreditation-consumable form from the start.

Closure requires a verification disposition for every Tier-1 and Tier-2 service in one of four states (migrated; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; retired), the rehearsed second algorithm

change per track inside the agility window as the next subsection reads it for accredited systems, and the agility-debt register at zero unaccepted debt: every remaining entry carries a funded treatment with a date or a SteerCo-signed exception.

In this sector the dated treatments and the signed exceptions will outnumber the closed entries at closure. Type 1, HAIPE, platform and satellite entries close on device, depot and launch schedules. An entry under a SteerCo-signed exception recorded in the accreditation package is accepted debt. An entry with no signature is unaccepted debt and blocks closure. Where coalition or cross-domain counterparts lag, verification at shared boundaries follows the counterparty pattern (Activity 7.6): observed negotiation, dual-stack windows, and documented residual-risk acceptance for connections that cannot yet close.

The Agility Criterion, Rehearsal, and Re-accreditation

The Universal's agility criterion counts a system as migrated only when four conditions hold: the negotiated outcome is observed in production traffic; classical-only negotiation is refused where policy requires it, with the refusal tested; the algorithm can be changed by configuration without a code change or a rebuild; and the change has been rehearsed in staging with the rollback exercised (Activity 4.6). On accredited systems the third and fourth conditions meet the RMF change process: changing the approved algorithm set is a security-relevant change on most authorization boundaries.

The rehearsed change includes the impact analysis, the authorizing official's decision and the continuous-monitoring record. This extension therefore reads the agility window for an accredited system as the 48-hour assessment plus a change window that includes the RMF change process. The Universal's ten-business-day default applies only where the authorizing official has pre-approved a change class covering algorithm and parameter-set changes.

Record the window per authorization boundary, and negotiate that change class before the first rehearsal. A rehearsal that waits for a full re-authorization measures the accreditation pipeline and not the system.

"Migrated with agility debt" will be the common recorded state in this sector. Type 1 and CSfC-listed modules change algorithms with a certified device or firmware release, not a configuration; weapons-platform cryptography changes at depot; HAIPE and Type 1 encryptors change on the National Manager's schedule. Each such system passes the protection result at its gate and has an agility-debt entry whose closure date is the device, firmware, depot or launch event that removes the debt. The register entry names the event, its owner and its firmness grade (Activity 7.5), so the roadmap shows the closure date for each debt entry.

Evidence Grades and Coverage on Classified Estates

Every discovery finding is recorded with one of five evidence grades: E1 runtime observed, E2 binary confirmed, E3 inventory declared, E4 vendor attested, E5 inferred (Activity 1.2). Classified estates produce more E4 and E5 than any other sector. Type 1 and CSfC modules are closed to binary analysis, and passive monitoring inside an accreditation boundary needs its own authorization. The grade is recorded with the finding and is never raised by the sensitivity of the system: a Tier-1 classified backbone whose PQC status is known only from a vendor questionnaire is E4 until an authorized active test or observed negotiation raises it.

The coverage denominator is enumerated before discovery runs, from the registers the accreditation process already maintains: the NSS registry, the FISMA system inventory, system security plans and authorization boundaries, the platform program offices' configuration baselines, and the contract register for the DIB track. "All systems in the NSS registry and the FISMA inventory" is a denominator; "what the tools found" is not.

The accepted-gaps register at G1 → G2 records the classified enclaves, weapons platforms and coalition segments that discovery did not reach, with the reason and the closure date, signed by the Discovery lead, countersigned by the CISO and accepted by the SteerCo. A gap that exists because access was refused is escalated under the discovery access pre-authorization in the charter (Activity 0.4).

Vendor Dates and Questions in Accredited Supply Chains

Every roadmap date a vendor, a certification program or a counterparty supplies has a firmness grade, committed, forecast, announced or unknown (Activity 7.5), and Phase 3 scores the firmness grade independently of the calendar date. In this sector the grade applies to dates the government does not set for itself: a Type 1 device's certification date, an NIAP protection profile revision, a FIPS 140-3 certificate's expected issue date, a CSfC component's listing date, an ally's migration milestone.

A certification date from a program office is forecast until the certificate issues. The questionnaire opens with the two agility questions and the firmness question (Activity 7.2). A product whose algorithms change only with a new certified release turns every future algorithm change into a procurement, and CNSA 2.0 will not be the last algorithm set an NSS runs. Certificate authorities, including the Federal PKI operators, the DoD PKI issuers and the external CAs the DIB uses, answer the four CA questions.

The non-standardized-algorithm rule (Activity 7.3) excludes from approved-mode use any public-key algorithm not standardized by NIST or an equivalent national authority. Its sovereignty carve-out records a national algorithm together with the documented regime that mandates it, which is the applicability record Challenge 9 specifies.

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, Executive Order 14412 and OMB M-26-15 for civilian agencies, the DoW PQC Strategy for defense components, national directives elsewhere). 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.

The charter states both outcomes together, as the Universal requires: readiness against the mandate that binds each part of the estate (Challenge 11), and crypto-agility proven by a rehearsed algorithm change on Tier-1 systems inside the agility window as the accreditation boundary defines it. The second outcome is the one policy does not supply. The mandates name algorithms and dates and are silent on the capability to change them again. OMB M-26-15 now asks every civilian agency plan for a crypto-agile architecture. The charter is where the agency says what that means in its estate.

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. Name the Crypto-Agility workstream lead and the Cryptographic Record owner from day one, separately from the Discovery lead (Activity 0.3). Discovery ends and the record does not.

The Crypto-Agility lead is the owner of the agility-debt register that the Type 1, platform and satellite estate will fill. For civilian agencies the PQC migration lead named under Executive Order 14412 is the natural Quantum Readiness Program Manager, and the PMO's plan is the migration plan OMB M-26-15 requires (Challenge 11). For defense organizations, align the PMO with the centralized governance the DoW PQC Strategy establishes and with the existing weapons system program offices. Those offices put PQC migration into the 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, FedRAMP cloud services, 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.

Every finding on these tracks is recorded with its evidence grade (E1 to E5, Activity 1.2). The classified, weapons-platform and CDS tracks will run largely on E4 vendor attestation and E5 inference until an authorized active test or module documentation raises them, and the grade is reported with every coverage figure. The denominator for each track is enumerated before discovery runs: the NSS registry and the FISMA system inventory for the first two tracks, the CDS accreditation records, the platform program offices' configuration baselines, the certificate authorities' issuance records and card populations, and the contract register for the DIB track. What the denominator contains

and discovery did not reach goes to the accepted-gaps register signed at G1 → G2 (the alignment section's evidence subsection).

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.

The record is the framework's own minimum record (Activity 2.1), expressed as plain CycloneDX 1.7 or, where an agency adopts it, as Applied Quantum CBOM Profile properties at v1.0-RC or later. The Profile is informative carriage and is not required. Executive Order 14412 section 5(d) directs CISA, coordinating with NIST, to publish public guidance on the minimum elements of a cryptographic bill of materials within 270 days of June 22, 2026, so by March 19, 2027 (White House text; Federal Register Vol. 91 No. 121). The direction compels no CBOM production and says nothing yet about content.

A CBOM built to the minimum record now carries the fields such guidance is likeliest to name, and the record is reviewed against the guidance when it publishes, with the differences recorded in the Version History rather than absorbed. OMB M-26-15 separately expects each civilian agency plan to name the discovery methods and automated tools behind its inventory and to maintain a central CBOM populated from them.

Phase 3 – Risk Scoring & Prioritization

Adapted Risk Scoring

The Universal's four dimensions apply as ratified by the SteerCo (Activity 3.1), Dimensions 1 to 4: HNDL risk; TNFL risk, with verifier updatability as a factor; migration feasibility; regulatory and compliance pressure. Government scoring adds two factors, each stated as a factor inside an existing dimension rather than as a fifth dimension, so the composite arithmetic of Activity 3.2 applies unchanged:

Factor	Dimension	Weight	Scoring
Data classification	Dimension 1 – HNDL	High	TOP SECRET =

Factor	Dimension	Weight	Scoring
level	risk		Critical, and any level with SCI or special-access compartmentation = Critical (SCI is a compartmentation and control framework applied at a level, not a level of its own); SECRET = High; CUI = Medium (CUI is unclassified; aggregation keeps it above Low); unclassified public data = Low. The classification period sets the confidentiality horizon that the dimension's horizon factor reads
Accreditation complexity	Dimension 3 – Migration feasibility	Medium	Cross-domain dependencies or multiple interconnected authorization boundaries = Hard; a single boundary with a pre-approved change class = Medium; an unrestricted or FIPS-aware enclave = Easy

Dimension 2's verifier-updatability factor is Critical for most Type 1 devices, tactical data links and satellite payloads, whose verifiers change with a certified device or a launch. These entries populate the agility-debt register as the alignment section describes. Dimension 4 reads the enforcement tier of the instrument that binds the entry (Regulatory Alignment Map): tier 1 for the CNSA 2.0 acquisition gate and the CMMC

cryptography control, tier 3 for the executive order's dates and tier 4 for NCSC UK's milestones.

Dimension 1's accessibility factor is scored against a state-level collector, so a flow that crosses a carrier, a commercial satellite link or a coalition boundary scores as partner-facing at least. The tier is assigned by the ordered test of Activity 3.2 from Dimensions 1, 2 and 4 alone; Dimension 3, including the accreditation-complexity factor above, and the delivery state place no entry in a tier, and they reach the program through sequencing inside the tier and through the roadmap.

Delivery state is recorded per entry with the four values available, dependent, blocked and unknown (Activity 3.2). A Type 1 module awaiting a certified PQC release is dependent or blocked. It keeps the tier the ordered test gives it and appears on the roadmap against the National Manager's release date with that date's firmness grade.

Government Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	Classified network backbone (TLS/IPsec), cross-domain solutions, intelligence collection/processing systems, satellite ground stations; weapons system and tactical data-link communications on Type 1 devices, including legacy platforms whose cryptography cannot be upgraded; coalition interoperability gateways; Federal PKI and DoD PKI roots and enterprise-wide trust anchors	Placed by the ordered test of Activity 3.2: Dimension 1 Critical on a carrier-, satellite- or partner-facing flow against a state-level collector; or Dimension 2 Critical, where verifiers change only with a certified device, a depot visit or a launch, or where the entry is a root or an enterprise-wide trust anchor; or Dimension 4 Critical under the CNSA 2.0 acquisition gate. Mandatory CNSA 2.0 compliance.	Available for TLS and IPsec on commercial platforms; dependent or blocked for CDS, Type 1 and platform paths, shown against the certified release, depot or retirement date with its firmness grade; a blocked entry runs under the double-encryption layer of Activity 7.4 (a PQC-protected outer layer over the classical device where the link topology admits one) or under that activity's documented residual-risk acceptance with a re-evaluation date

Priority	System Category	Rationale	Typical Delivery State
Tier 2	Command and control networks inside a single accreditation boundary, end-entity PKI and identity infrastructure (PIV/CAC credential estate, derived credentials, ICAM federation), federal high value assets and high-impact systems bound by the executive order's 2030 and 2031 dates	Dimension 1 Critical or High with accessibility below partner-facing; or Dimension 2 High, where verifiers are updatable and the verification period is under 15 years; or Dimension 4 High under a mandatory deadline within 5 years.	Dependent on device certification, card issuance and issuer schedules; a blocked entry keeps this tier
Tier 3	Unclassified federal networks and FedRAMP cloud services below the high-impact threshold, CUI-handling contractor systems, administrative IT	Any applicable risk dimension (1, 2 or 4) Medium or above. Lower classification sensitivity. Can use commercial PQC products. NIST-governed; a contractor system moves to Tier 2 on Dimension 4's contractual-requirement factor once a contract requires PQC, and on its deadline factor once the directed FAR rule is final with a date within 5 years.	Available; dependent where a FedRAMP provider's roadmap sets the date
Tier 4	Archived systems and low-sensitivity public-facing services whose every applicable risk	Every applicable risk dimension Low. Monitor; apply compensating controls; migrate	Blocked entries are shown in the tier the ordered test gives them, not in this one

Priority	System Category	Rationale	Typical Delivery State
	dimension is Low	when feasible. A blocked migration does not place an entry here, and a legacy platform whose cryptography cannot be upgraded is tiered on its risk under Tier 1 or Tier 2 with delivery state blocked.	

Phase 4 – Roadmap & Governance

Algorithm-specific weighting. Apply the Universal Framework's vulnerability weighting (Activity 3.1) in government scoring: quantum attack cost tracks key size rather than classical strength, so ECDSA P-256/P-384 estates (PIV/CAC, Suite B-era systems) are weighted at least as urgent as RSA-2048 at equal mission sensitivity. See the alignment section's Algorithm Weighting subsection.

CNSA 2.0 Milestone Alignment

The migration roadmap must align explicitly with the CNSSP 15 milestones, with the advisory's per-category dates recorded against them by their provenance and status (Challenge 1):

- **By January 1, 2027:** Every new NSS acquisition CNSA 2.0 compliant on delivery. Cryptographic inventory complete for all NSS with evidence grades. PQC pilots underway in unrestricted enclaves.
- **By 2030:** Software and firmware signing and networking equipment (VPNs, routers) on CNSA 2.0 exclusively (per-category chart). By December 31, 2030, equipment and services that cannot support CNSA 2.0 phased out (CNSSP 15). Accreditation pipeline cleared for priority systems; agility debt on Type 1 and platform entries carried with dated closure events.
- **By December 31, 2031:** CNSA 2.0 algorithms mandated for use on NSS, unless a profile notes otherwise (CNSSP 15).
- **By 2033:** Web, cloud and operating-system platforms, niche equipment, and custom applications and legacy equipment on CNSA 2.0 exclusively, replaced or decommissioned (advisory per-category chart. These dates fall after the CNSSP 15

mandated-use date, so the binding date for these categories is CNSSP 15's or the applicable profile's, Challenge 1).

- **2035:** Not a CNSA 2.0 chart date. 2035 is NSM-10's overall mitigation goal and the Full Migration phase of OMB M-26-15, which does not apply to NSS (Challenge 11). An NSS roadmap plans to the CNSSP 15 dates, with the chart's 2030 and 2033 dates recorded against their categories as guidance.

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.

Gates, Recorded States, and Re-baselining

From gate G5 → G6 onward, and at every wave exit, the agility criterion of Activity 4.6 decides what counts as migrated, and every gate record shows two results as separate fields: the protection result (which functions and boundaries are verified, which remain exposed) and the agility result (which change was rehearsed, through which mechanism, in what elapsed time, with which constraints). A system that passes on protection and fails the configuration or rehearsal conditions is recorded as migrated with agility debt, with a closure date in the Phase 3 register; in this sector that record will name a certified release, a depot visit or a launch as the closure event.

The Re-Baseline Protocol (Activity 4.8) applies with its triggers extended to the dates this program does not own: a certified PQC device or firmware release slipping past the bridging capacity recorded in Activity 7.4, a CMVP or NIAP date moving, a coalition partner missing a committed interoperability window, or a platform sustainment schedule changing. Each opens a re-baseline review at the next SteerCo, and the minute is filed to the evidence dossier and to the accreditation package. A date the accreditation authority owns is moved only with that authority.

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 against the dual-stack model of NIST's June 2026 PIV working drafts, and application integration. Record the issuance date for production credentials as unknown until the card issuer commits to one.
- **Pilot 5 – Coalition interoperability:** Run with a Five Eyes or NATO ally to test PQC-protected information exchange on a coalition test network.

Rehearsal per Wave and the Wave-Exit Criterion

Every wave includes an algorithm-change rehearsal in staging on at least one system in the wave (Activity 5.2). The natural rehearsals in this sector are the changes the mandates will require: a parameter-set change from ML-KEM-768 to ML-KEM-1024 on a key-establishment path, which is the move a system makes when its boundary determination changes to NSS (Challenge 11); a hybrid-to-standalone switch on a signing path, which is the CNSA 2.0 endpoint; and a certificate-signature-algorithm change on an internal issuer.

The rehearsal is timed across assessment, decision, change and verification, with the decision segment including the authorizing official's decision under the pre-approved change class, and the four elapsed times feed the rehearsed time-to-change KPI (KPI Supplement). For accredited enclaves the rehearsal runs on the test ATO environment of Pilot 3 before it runs anywhere accredited. Every wave exit applies the agility criterion: negotiated outcome observed, classical-only refused and tested where policy requires it, algorithm changeable by configuration, change rehearsed with rollback. A system that fails the last two exits the wave as migrated with agility debt, and the wave-exit record shows the protection and agility results for every system in the wave (Activity 5.4).

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 each tactical link's bandwidth in the waveform and mode it runs (Link 16, Link 22, tactical SATCOM), taking the figure from the link's own specification for that mode; tactical SATCOM is 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.

HSM, KMS, and Encryptor Register

The Activity 6.2 register records four fields per module, separately: the visible platform (the product as procured), the supplier's canonical firmware family, the manufacturer of origin, and the certificate reference. For FIPS-validated modules the reference is the FIPS 140-3 certificate with its approved-services list and status; for Type 1 and CSfC components it is the NSA certification or the CSfC component listing, and KMI-provisioned key material is recorded with its source.

For every module that generates PQC keys with a long lifetime, the register also records the Entropy Source Validation certificate or the ENT designation, with the operating envelope the validation covers. Two products under two names can be one firmware family. A cloud KMS inside a sovereign or accredited region is a dependency boundary rather than a manufacturer. The boundary-verification rule of Activity 7.7 applies to those rows.

Where an institution measures cryptographic concentration beneath these vendors, the instrument is the Cryptographic Concentration Framework. This extension records the fields and computes no figure.

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.

Questionnaire Order, Certificate Authorities, and the Concurrent Mandates

The questionnaire of Activity 7.2 opens with the two agility questions (algorithms changeable by configuration; verifiers and trust stores updatable in the field) and the firmness question. Every date it returns is graded committed, forecast, announced or unknown before it enters the roadmap. The dates in the three vendor tiers above are graded the same way, and a Tier A certification date is forecast until the certificate issues.

The four certificate-authority questions go to the Federal PKI operators, the DoD PKI issuers and the external CAs the DIB relies on. An issuer that cannot issue ML-DSA or composite certificates on the roadmap's dates gates every Track B migration behind it (Activity 3.3). Any product whose quantum-safe claim depends on a proprietary or pre-standard algorithm, which is common in tactical, satellite and secure-voice offerings, gets the one-afternoon test of Activity 7.3 before it is evaluated further, and the sovereignty carve-out of that rule applies only to a national algorithm recorded in the Challenge 9 applicability record.

CNSA 2.0 prescribes ML-KEM-1024 and ML-DSA-87, with LMS and XMSS allowed for firmware and software signing, and the civilian mandate accepts any NIST-standardized parameter set. A system that serves both, or that moves from one to the other when its boundary determination changes, moves between the two algorithm sets by configuration under the pre-approved change class as a recorded change inside the existing authorization. A product that answers yes to both agility questions, with a rehearsal completed under the RMF change process, moves between the two mandate chains as a recorded configuration change. A product that answers no moves between them as a procurement.

DIB PQC Requirements

- **Contract flow-down:** Write PQC requirements (ML-KEM and ML-DSA support, the two agility questions, firmness-graded dates) into new and renewed contracts involving classified or CUI data now, ahead of the directed FAR rule (Challenge 6).
- **CMMC evolution:** The Department of War's PQC Strategy states that CMMC will be updated to include PQC requirements and that the Department's external certificate authorities will move to PQC certificates (Line of Effort 4). Until a revision publishes, CMMC Level 2's FIPS-validated-cryptography control (SC.L2-3.13.11) is the enforceable cryptographic requirement for CUI, through DFARS 252.204-7012, NIST SP 800-171 Rev 2 and the Phase 1 self-assessment that remain in force. The third-party assessment Phase 2 was to begin on November 10, 2026 is suspended by the Department of War Chief Information Officer's memorandum of July 13, 2026 and carried into acquisition by Class Deviation 2026-O0025 (Challenge 1).

The CMMC Program rule and DFARS 252.204-7021 stand unamended, and requiring activities may designate Level 1 (Self) and Level 2 (Self) but not Level 2 (C3PAO) or Level 3 (DIBCAC) during the suspension. A contractor reads the assessment level designated on its own solicitation and expects the solicitation amendments and contract modifications the deviation directs. Provide guidance and toolkits for small DIB contractors.

- **Vulnerability disclosure:** Executive Order 14412 section 6(d) directs a proposed FAR rule within 270 days of the order requiring covered contractors' vulnerability disclosure programs to accept reports of cryptographic vulnerabilities, including

missing encryption and the use of non-FIPS algorithms. Align DIB vulnerability-disclosure language with it now.

- **FedRAMP PQC:** OMB M-26-15 assigns CISA and the Department of War, with GSA, the lead on PQC migration for FedRAMP-authorized cloud services and for SaaS, PaaS and IaaS used at more than one agency. Delineate PQC responsibilities with each provider under the shared responsibility model (Activity 7.7), and treat a provider's published roadmap date as forecast until it is contractual.

GOVERNMENT & DEFENSE REGULATORY ALIGNMENT MAP

The rows below are the sector's own instruments as of September 2026, each with its status and with the enforcement tier the Universal's Regulatory & Standards Alignment Map assigns (tier 1, market access; tier 2, supervisory directive with a named enforcer; tier 3, binding government mandate with an audit trail; tier 4, authoritative guidance; tier 5, advisory). The national rosters the Universal already lists (NCSC UK, the EU coordinated roadmap, Australia, Canada) are not repeated here: they are in the Universal's Regulatory Timeline Context and, kept current between editions, on the Global PQC Migration Clock page. Every date is re-checked against its instrument at each release, and readers verify status and applicability for their own systems before planning against a row.

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
CNSSP 15 (updated 2024, published March 2025) with NSA CNSA 2.0	CNSA 2.0 algorithms on NSS: acquisition gate, phase-out, mandated use. January 1, 2027; December 31, 2030; December 31, 2031. The advisory's per-category chart (2030 and 2033) is guidance recorded with its provenance (Challenge 1)	Binding for NSS (tier 1 at the acquisition gate; tier 3 thereafter)	Denial or revocation of ATO available to the authorizing official for non-compliance; a new system that cannot meet the gate is not accredited; every in-flight solicitation checked against the gate

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
NSM-10 (May 4, 2022) and OMB M-23-02 (November 18, 2022)	Prioritized inventory of quantum-vulnerable systems, excluding NSS, submitted to ONCD and CISA. First inventory May 4, 2023; annually until 2035	In force; the inventory feeds the M-26-15 plan (tier 3)	The inventory is the enumerated denominator of the civilian program's coverage figures
Executive Order 14412 (June 22, 2026) and OMB M-26-15 (June 24, 2026)	PQC on federal high value assets and high-impact systems, excluding NSS; a PQC migration lead per agency; a migration plan to OMB and ONCD; a five-phase schedule to 2035. The key-establishment and signature dates and the plan deadline as stated in Challenge 11	In force; plans due October 22, 2026 (tier 3)	The civilian mandate; its separate key-establishment and signature dates are the two-track model in mandate form
Executive Order 14412 section 6(c): directed FAR rulemaking	Covered contractors to comply with NIST FIPS, including the PQC FIPS, by the date stated in Challenge 6. Proposed rule due within 180 days of the order, by December 19, 2026	Directed rulemaking; no proposed rule published at this edition (tier 1 once a final rule is in force)	Reaches contractors who read CNSA 2.0 as an NSS-only obligation; primes write subcontract requirements now
Executive Order 14412 section 5(d): CBOM minimum-elements guidance	CISA, coordinating with NIST, publishes public guidance on the minimum elements of a cryptographic bill of materials. Due by	Directed guidance; compels no CBOM production (tier 4 when published)	The Phase 2 minimum record is reviewed against it when it publishes

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
	March 19, 2027		
Department of War PQC Strategy (released June 23, 2026)	All DoW systems support PQC or are phased out; all DoW systems use PQC; NSS on CNSA 2.0; five lines of effort; CMMC to be updated for PQC. The support-or-phase-out and use dates as stated in Challenge 11	Department CIO guidance in force (tier 3 within the Department)	Binds NSS and non-NSS DoW systems to one shape; DIB cryptographic security is a named line of effort
NIST FIPS 203, 204 and 205; NIST SP 800-208	Standardized PQC algorithms (ML-KEM, ML-DSA, SLH-DSA) and stateful hash-based signatures (LMS/XMSS). FIPS 203–205 published August 13, 2024; SP 800-208 published October 2020	Final (tier 4; binding where CNSA 2.0, the executive order or a contract cites them)	The algorithm set for unclassified federal systems; SP 800-208 is the deploy-now signing component under its section 8 conditions
NIST IR 8547	Deprecation of quantum-vulnerable public-key algorithms after 2030 and disallowance after 2035	Initial Public Draft (November 2024); still a draft at this edition (tier 4)	M-26-15 requires agency plans to align with it; the reference other instruments cite
DFARS CMMC rule (48 CFR; published September 10, 2025; effective November 10, 2025)	CMMC status as a condition of award; Level 2 requires FIPS-validated cryptography for CUI (SC.L2-3.13.11). Phase 1 self-assessment November 10, 2025, in force; the	In force as codified; the discretionary designation of Level 2 (C3PAO) and Level 3 (DIBCAC) suspended by memorandum and implemented by class deviation, a different firmness grade from	The sector's market-access example: a contractor without a validated module for its CUI systems cannot be awarded covered work; a contractor reads the assessment level designated on its

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
	advancement to Phase 2 (Level 2 C3PAO and Level 3 DIBCAC assessments, originally November 10, 2026) suspended July 13, 2026 by the Department of War Chief Information Officer's memorandum "Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements," with a CMMC Reform Task Force review of 60 days that expired September 11, 2026 and whose recommendations have not published, and carried into acquisition by Class Deviation 2026-O0025 (Revision 1 of June 29, 2026; Revision 2 of July 16, 2026; Revision 3 of September 3, 2026, current at this edition), which directs contracting officers to remove or revise the CMMC requirements in new and existing solicitations and contracts and remains in effect until	a withdrawn rule (tier 1)	own solicitation and expects the solicitation amendments and contract modifications the deviation directs

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
	rescinded or incorporated into the FAR, DFARS and DFARS PGI; 32 CFR Part 170 unamended and no Federal Register document issued; DFARS 252.204-7012 and 252.204-7021 continue, 252.204-7021 in the deviated Part 240 at 240.371-5, with NIST SP 800-171 Rev 2 and FAR 52.204-21 (DoW CIO CMMC program page)		
NIST CMVP: FIPS 140-2 certificates to the Historical list	Every remaining FIPS 140-2 certificate moved to the Historical list; CMVP supports purchase and use of those modules for existing systems and recommends that purchasers consider modules validated against either standard. September 21, 2026, per the maintained prose of the transition page (its 2021 transition-schedule table prints September 22, 2026)	Past event at this edition (FIPS 140-3 Transition Effort); exclusion from new procurement follows from agency and contractual policy (tier 1 for new procurement)	Compounds the January 2027 acquisition gate; validated PQC services are counted per product (alignment section)
NATO Quantum Technologies Strategy (summary	Alliance transition to quantum-safe cryptography through	Strategy (tier 5); no PQC standardization agreement identified	Coalition interoperability planned on dual-

Instrument	Requirement and Dates	Status at This Edition (Enforcement Tier)	Gov/Def Implication
published January 2024)	NATO committees and bodies. No date published	in the public record at this edition	stack windows and the counterparty pattern (Activity 7.6) in the absence of a NATO date

GOVERNMENT & DEFENSE MATURITY MODEL SUPPLEMENT

The levels, names and descriptions are the Universal's single 0 to 5 scale (Maturity Levels), used by the enterprise model and every per-phase table alike. The sector indicators refine them. The closure criterion reads the same scale.

Level	Universal Name and Description	Gov/Def-Specific Indicator
0	Unaware: no organizational awareness of quantum cryptographic risk; no activities planned or underway	No sector indicator
1	Aware: quantum risk acknowledged at leadership level; initial education conducted; no formal program	CIO/CISO directive issued. Which mandate binds which part of the estate (CNSA 2.0, the civilian mandate, both) identified.
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Quantum PMO established with a Crypto-Agility lead and a Cryptographic Record owner named. PQC migration lead named and the migration plan submitted (civilian agencies). NSS cryptographic inventory underway with evidence grades and an enumerated

Level	Universal Name and Description	Gov/Def-Specific Indicator
		denominator. CDS and weapons platform crypto modules being catalogued. DIB exposure mapped.
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Roadmap aligned to the CNSSP 15 milestones approved. Accreditation authority pre-engaged, with a pre-approved change class for algorithm and parameter-set changes negotiated or in negotiation. Acquisition PQC requirements integrated. Coalition coordination initiated. Agility-debt register produced for the Type 1, platform and satellite estate with dated closure events.
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured	Tier-1 classified systems pass the protection result at their gates; each that fails the configuration or rehearsal conditions is recorded as migrated with agility debt against a dated closure event. Unclassified networks on PQC. PKI migration underway. Coalition PQC interoperability tested. An algorithm change rehearsed on at least one Tier-1 system inside the agility window the authorization boundary defines.
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and	CNSSP 15 milestones met; all NSS on CNSA 2.0. DIB PQC verified. Coalition interoperability achieved. Legacy platforms

Level	Universal Name and Description	Gov/Def-Specific Indicator
	posture management operational	compensated or decommissioned. A rehearsed second algorithm change per track inside the agility window, and the agility-debt register at zero unaccepted debt: every remaining Type 1, platform and satellite entry under a funded treatment with a date or a SteerCo-signed exception.

GOVERNMENT & DEFENSE KPI SUPPLEMENT

Leadership-Level KPIs (Quarterly)

- **CNSA 2.0 compliance trajectory:** Percentage of NSS on track for the CNSSP 15 milestones (the January 1, 2027 acquisition gate, the December 31, 2030 phase-out and the December 31, 2031 mandated use) and for the advisory's per-category dates, 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:** Phases completed against planned, with the accreditation status of each pilot.
- **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.

Agility KPIs (CISO cascade, monthly; summarized to leadership under the Agility KPI)

The four agility KPIs of the Universal's Metrics, KPIs & Reporting section, with the sector's measurement and thresholds.

KPI	Government and Defense Measurement	Threshold
Configuration-driven share	Percentage of Tier-1 systems (classified backbone, CDS, intelligence systems, ground stations) whose key-establishment and signature algorithms change by configuration, verified by rehearsal inside the authorization boundary; Type 1 and CSfC entries reported on a separate line as certified-release-bound	Target by year from the roadmap's agility milestones (Activity 4.2); a year missed by more than 10 points triggers Crypto-Agility workstream review
Rehearsed time-to-change	Elapsed time across assessment, decision (including the authorizing official's decision under the pre-approved change class), change and verification on the most recent rehearsal, per track and per authorization boundary	Inside the agility window the boundary defines; a result outside it is a finding, and a decision segment that dominates the total is an accreditation finding rather than an engineering one
Agility-debt burn-down	Entries closed on the Phase 3 register per quarter, with the certified-release, depot and launch events that closed them	Any quarter with no reduction triggers workstream review; before closure every remaining entry carries a funded treatment with a date or a SteerCo-signed exception
New-system agility compliance	Percentage of new solicitations whose RFP, SOW and evaluation criteria include the two agility questions and the firmness question, and percentage of new deployments passing the CI/CD crypto-policy check and the provider-pattern review	Below 95% in any month triggers architecture and acquisition governance review

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, and submit the M-26-15 migration plan where it applies.** This is a federal mandate. Prioritize NSS and CUI-handling systems. Use the inventory to identify CNSA 2.0 compliance gaps. A civilian agency submits its PQC Migration Plan to OMB and ONCD by October 22, 2026 (Challenge 11), naming the discovery methods and tools behind the inventory.
- **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 expedited 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), record the installed crypto modules, their manufacturer, whether they can be upgraded and 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.
- **9. Name owners for Crypto-Agility and for the Cryptographic Record.** Fund both from Year 1, separately from the Discovery lead, and give the agility-debt register for the Type 1, platform and satellite estate to the Crypto-Agility owner, with a closure event and a firmness grade on every entry.

- **10. Schedule the first algorithm-change rehearsal.** Run it on an unclassified Tier-1 candidate in staging within the first two waves and time the four segments. Use the result as evidence when requesting that the accreditation authority pre-approve a change class for algorithm and parameter-set changes.

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/

CNSA 2.0: The Complete Guide to NSA's Post-Quantum Requirements – https://postquantum.com/cnsa-2-0/complete-guide/ – Full treatment of the algorithm suite, category milestones, and governance chain.

The 2027 Procurement Gate: Why CNSA 2.0 Compliance Starts Now – https://postquantum.com/cnsa-2-0/2027-procurement-gate/ – The January 2027 acquisition requirement and the late-2026 compliance sequence.

CNSA 2.0 vs. the World: Navigating Diverging Global PQC Requirements – https://postquantum.com/cnsa-2-0/global-pqc-requirements/ – The allied divergence on hybrid, algorithm menus, and parameters.

CNSA 2.0 for the Defense Industrial Base – https://postquantum.com/cnsa-2-0/defense-contractors/ – What the mandate means for DIB suppliers and CMMC-bound contractors.

US Federal PQC Mandate After June 2026: Complete Guide – https://postquantum.com/post-quantum/us-federal-pqc-mandate-2026/ – What applies to whom, by when and under which authority after the June 2026 orders.

OMB M-26-15: Federal PQC Migration Playbook Explained – https://postquantum.com/security-pqc/omb-m-26-15-pqc-migration/ – The five-phase schedule and the plan-submission requirements for civilian agencies.

DoW PQC Strategy: The Defense Half of the EO Mandate – https://postquantum.com/security-pqc/dow-pqc-strategy-eo-14412/ – The department-wide 2030 and 2031 gates and the five lines of effort.

Why HNDL cannot be detected (July 2026 analysis) – https://postquantum.com/post-quantum/cannot-detect-harvest-now-decrypt-later/ – The reasoning behind the framework's HNDL position, for the funding conversation.

The Global PQC Migration Clock – https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/ – The maintained jurisdiction roster that this extension's regulatory map points to.

Quantum Ready (companion book) – https://quantumready.com – The executive and governance dimensions of quantum readiness, complementing this framework's technical methodology.

APPENDIX J: REQUIREMENTS REGISTER

This register is generated from the text of this edition at each build and lists every statement in this extension that uses *must*. The four program-level provisions of the Universal Framework's Normative Convention bind this extension through its parent and are listed in the Universal's Appendix J; they are not repeated here. Every statement below binds inside the section that states it, and a statement that appears here without its section's conditions is read with them. The appendix letter matches the Universal's, so "Appendix J" names the requirements register in every document of the set.

Statements in document order

1. *Why Government and Defense Requires a Sector Extension, Mandatory PQC Timelines Set by the Standards Authorities.* The implementation phases must satisfy government accreditation and compliance requirements that commercial enterprises do not face, which adds scope and duration to every subsequent phase.
2. *Why Government and Defense Requires a Sector Extension, Bifurcated NSS and Non-NSS Environments.* National security systems must follow NSA's CNSA 2.0 through CNSSP 15; non-NSS federal systems follow NIST standards under the civilian mandate (Challenge 11).
3. *Why Government and Defense Requires a Sector Extension, Bifurcated NSS and Non-NSS Environments.* PQC migration must be planned and executed separately for each domain, with coordination at the boundaries.
4. *Why Government and Defense Requires a Sector Extension, Defense Industrial Base as Extended Attack Surface.* CMMC (Cybersecurity Maturity Model Certification), DFARS clauses, and FedRAMP requirements must evolve to incorporate PQC.
5. *Why Government and Defense Requires a Sector Extension, Defense Industrial Base as Extended Attack Surface.* 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.
6. *Why Government and Defense Requires a Sector Extension, Weapons Systems in Service for 20 to 50 Years.* The aircraft's cryptographic capabilities must either be quantum-resistant from delivery or upgradable to PQC during its service life.

7. *Why Government and Defense Requires a Sector Extension, Weapons Systems in Service for 20 to 50 Years.* Existing platforms must be assessed for cryptographic upgrade feasibility, with remediation plans integrated into platform sustainment programs.

8. *Why Government and Defense Requires a Sector Extension, Coalition and Allied Interoperability.* PQC migration must be coordinated across allied nations whose migration timelines, approved algorithms (CNSA 2.0 for US/Five Eyes, national algorithms for some European and Asian allies), and classification authorities diverge.

9. *Why Government and Defense Requires a Sector Extension, Coalition and Allied Interoperability.* 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.

10. *Why Government and Defense Requires a Sector Extension, Coalition and Allied Interoperability.* NATO's cryptographic standards bodies must coordinate PQC adoption across 32 member nations.

11. *Industry-Specific Challenges, Challenge 1: CNSA 2.0 Compliance Under Hard Deadlines.* Framework Impact: Phase 0 must anchor the entire program timeline to the CNSSP 15 milestones.

12. *Industry-Specific Challenges, Challenge 1: CNSA 2.0 Compliance Under Hard Deadlines.* Phase 4 must build a roadmap that meets the acquisition gate, the phase-out date and the mandated-use date, with the advisory's per-category dates recorded against each category as guidance and with margin for testing and accreditation.

13. *Industry-Specific Challenges, Challenge 1: CNSA 2.0 Compliance Under Hard Deadlines.* On January 1, 2027, a new acquisition for a National Security System in scope of CNSSP 15 must support CNSA 2.0 algorithms (ML-KEM-1024 key establishment, ML-DSA-87 signatures), unless the applicable profile notes otherwise.

14. *Industry-Specific Challenges, Challenge 2: Classified System Accreditation Overhead.* Every cryptographic change must have an impact assessment and a recorded authorization decision.

15. *Industry-Specific Challenges, Challenge 2: Classified System Accreditation Overhead.* 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.

16. *Industry-Specific Challenges, Challenge 2: Classified System Accreditation Overhead.* Framework Impact: Phase 4 must model, for each system, which

authorization path its cryptographic changes follow (pre-approved change class, reassessment, or reauthorization) and the time each path takes.

17. *Industry-Specific Challenges, Challenge 2: Classified System Accreditation Overhead.* Phase 6 must prepare accreditation documentation packages in parallel with technical migration.

18. *Industry-Specific Challenges, Challenge 3: Cross-Domain Solution Migration.* Framework Impact: Phase 3 must classify CDS as highest-priority and hardest-to-migrate systems.

19. *Industry-Specific Challenges, Challenge 3: Cross-Domain Solution Migration.* Phase 5 must include dedicated CDS PQC pilots in isolated lab environments.

20. *Industry-Specific Challenges, Challenge 3: Cross-Domain Solution Migration.* Phase 7 must engage CDS vendors on PQC roadmaps.

21. *Industry-Specific Challenges, Challenge 4: Weapons System Embedded Cryptography.* Framework Impact: Phase 1 must inventory all Type 1 and CSfC-listed cryptographic modules across weapons platforms.

22. *Industry-Specific Challenges, Challenge 4: Weapons System Embedded Cryptography.* Phase 4 must integrate PQC migration into platform sustainment and modernization schedules.

23. *Industry-Specific Challenges, Challenge 4: Weapons System Embedded Cryptography.* Phase 7 must coordinate with NSA and cryptographic module vendors on next-generation PQC-capable devices.

24. *Industry-Specific Challenges, Challenge 5: Satellite and Space System Constraints.* These systems must be quantum-resistant for their entire orbital lifetime (often 15–20 years).

25. *Industry-Specific Challenges, Challenge 5: Satellite and Space System Constraints.* Satellites currently in design and production must incorporate PQC from launch.

26. *Industry-Specific Challenges, Challenge 5: Satellite and Space System Constraints.* Framework Impact: Phase 1 must inventory all satellite and space system cryptographic implementations.

27. *Industry-Specific Challenges, Challenge 5: Satellite and Space System Constraints.* Phase 4 must separate in-orbit systems, scored on the space-link protection and update capability the inventory found, from future-launch systems specified as PQC from launch.

28. *Industry-Specific Challenges, Challenge 5: Satellite and Space System Constraints.* Phase 7 must coordinate with satellite manufacturers on PQC-by-design requirements.

29. *Industry-Specific Challenges, Challenge 6: Defense Industrial Base Supply Chain Cascade.* Framework Impact: Phase 7 must extend to DIB PQC readiness assessment.

30. *Industry-Specific Challenges, Challenge 6: Defense Industrial Base Supply Chain Cascade.* Phase 3 must score contractor-held data for HNDL exposure.

31. *Industry-Specific Challenges, Challenge 7: Coalition Cryptographic Interoperability.* Framework Impact: Phase 4 must model coalition interoperability requirements.

32. *Industry-Specific Challenges, Challenge 7: Coalition Cryptographic Interoperability.* Phase 5 must include joint testing with key allies.

33. *Industry-Specific Challenges, Challenge 7: Coalition Cryptographic Interoperability.* Phase 7 must include engagement with NATO and bilateral cryptographic standards bodies.

34. *Industry-Specific Challenges, Challenge 8: PKI at Government Scale.* 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.

35. *Industry-Specific Challenges, Challenge 8: PKI at Government Scale.* The DoD CAC (Common Access Card) replacement cycle and PIV card infrastructure must be planned to accommodate PQC certificates and the corresponding key sizes.

36. *Industry-Specific Challenges, Challenge 8: PKI at Government Scale.* Framework Impact: Phase 2 must document all PKI trust hierarchies and certificate counts.

37. *Industry-Specific Challenges, Challenge 8: PKI at Government Scale.* Phase 6 must benchmark PQC certificate performance across identity, authentication, and signature use cases.

38. *Industry-Specific Challenges, Challenge 8: PKI at Government Scale.* Phase 4 must align PKI migration with smart card refresh cycles.

39. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* Organizations operating across multiple jurisdictions must accommodate these variations.

40. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* 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.

41. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* Framework Impact: Phase 0 must map all applicable national cryptographic requirements.

42. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* Phase 5 must architect for multi-algorithm PQC support where sovereign requirements exist.

43. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* Phase 7 must engage with national cryptographic authorities.

44. *Industry-Specific Challenges, Challenge 9: Sovereign Cryptography and National Algorithm Requirements.* The consequence for coalition operations, multinational programs, and any agency procuring from allied suppliers: divergent cryptographic postures must run concurrently, which makes crypto-agility across algorithm families and postures an architectural requirement.

45. *Industry-Specific Challenges, Challenge 10: Tactical and Deployed System Constraints.* Software-defined radios, tactical data links (Link 16/22), and satellite communications terminals all embed cryptographic functions that must eventually support PQC.

46. *Industry-Specific Challenges, Challenge 10: Tactical and Deployed System Constraints.* 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.

47. *Industry-Specific Challenges, Challenge 10: Tactical and Deployed System Constraints.* Framework Impact: Phase 6 must benchmark PQC overhead against tactical bandwidth and latency budgets.

48. *Industry-Specific Challenges, Challenge 10: Tactical and Deployed System Constraints.* Phase 1 must inventory deployed cryptographic equipment.

49. *Industry-Specific Challenges, Challenge 10: Tactical and Deployed System Constraints.* Phase 7 must track NSA/HAIPE PQC device timelines.

50. *Industry-Specific Challenges, Challenge 11: Concurrent NSS and Civilian Federal Mandates.* Framework Impact: Phase 0 must record a system-boundary determination for every system: whether it is a national security system under the statutory definition (44 U.S.C. §3552(b)(6), which reaches a system by its function – intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment integral to a weapon or weapons system, or the direct fulfillment of military or intelligence missions, excluding routine administrative and business applications – as well as by the classification of the information it holds), the authority that governs it, the profile that applies, and the contract flow-down that imposes the requirement, with civilian federal, NSS, CUI-contractor and commercial systems kept as separate populations.

51. *Alignment with Universal Framework v3.0, Two-Track Migration Model in Government and Defense.* Track B (Integrity / Signatures / PKI): software and firmware signing (already under CNSA 2.0 mandate), PIV/CAC credential signatures, Federal PKI hierarchies, weapons system and cross-domain solution signatures, and signed records whose validity must survive for decades.

52. *Alignment with Universal Framework v3.0, Validation Decided Per Product in FIPS-Required and CNSA-Mandated Classes.* On January 1, 2027, new NSS acquisitions must be CNSA 2.0 compliant (Challenge 1).

53. *Alignment with Universal Framework v3.0, Validation Decided Per Product in FIPS-Required and CNSA-Mandated Classes.* Engineering readiness must not be the constraint on the certificate date.

54. *Alignment with Universal Framework v3.0, Hybrid and Composite Signatures Under CNSA 2.0.* Multinational and coalition programs must satisfy both postures at once.

55. *Alignment with Universal Framework v3.0, Hybrid and Composite Signatures Under CNSA 2.0.* The crypto-agility architecture must serve both without forking the codebase.

56. *Alignment with Universal Framework v3.0, Algorithm Weighting Across Government PKI and Legacy Suites.* ECDSA P-256 and P-384 are everywhere (PIV/CAC credentials, Suite B-era deployments, TLS), and they must not be sequenced later than RSA systems on the assumption that elliptic curves are the stronger cryptography.

57. *Alignment with Universal Framework v3.0, SP 800-208 Signing Under the CNSA 2.0 Schedule.* A deployment that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

58. *Phase 2 adaptation, Classification-Aware CBOM.* Government CBOMs must be produced at the appropriate classification level.

59. *Phase 4 adaptation, CNSA 2.0 Milestone Alignment.* The migration roadmap must align explicitly with the CNSSP 15 milestones, with the advisory's per-category dates recorded against them by their provenance and status (Challenge 1):

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the founder and CEO of Applied Quantum, and the founder of Quantum Academy (QuantumAcademy.com). PostQuantum.com is his personal blog. 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, including some exceeding 120,000 discrete migration tasks, for telecoms, financial institutions, and critical infrastructure operators.

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.

QUANTUM READY: THE COMPANION BOOK

Quantum Ready (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic), the book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, and sector narratives. It also gives guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as standards, products and deadlines change, and the book supplies the depth that a methodology document omits by design.

QUANTUM ACADEMY

Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, from executive education on quantum risk to practitioner courses on PQC migration, crypto-agility and cryptographic inventory, for the roles and training levels described in Skills & Team Structure.

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