Department of War
Post Quantum Cryptography Strategy

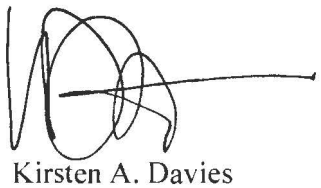
APR 0 1 2026

FOREWORD

The Department's capacity to achieve national objectives and fulfill its defense mission requirements are firmly rooted in our ability to protect war fighting systems from intrusion, to maintain confidence in data, to safeguard critical communications from adversaries, and to protect systems from adversarial control. The cryptographic system components we have deployed to secure critical mission functions are at risk due to advancements in adversarial capabilities to exploit quantum computing.

To ensure mission success in the face of quantum threats, I am announcing the Department of War (DoW) Post Quantum Cryptography (PQC) Strategy. This strategy outlines deliberate and actionable objectives we must achieve to migrate our war fighting capability (and supporting systems) to ensure continued mission readiness. This includes increasing our capacity to leverage industry capabilities by introducing processes for swift commercial solution vetting and streamlining testing and evaluation. Combining industry capabilities with enhanced DoW coordination for PQC lays the groundwork for expedited hardening against quantum threats and a strategic path for migration to PQC.

This critical PQC migration is not without challenges. Nearly every deployed military asset will be affected in some way, adversaries will continue to probe for weaknesses, and costs will be incurred. But with deliberate and careful planning, guided by this strategy, I am confident the DoW will meet this challenge and provide confidence to our warfighters that the systems they trust with their lives will be secure and available when it counts.



Kirsten A. Davies

Table of Contents

Strategic Intent

The Department of War (DoW) Post Quantum Cryptography (PQC) strategy outlines a framework for the DoW to plan, produce, and deploy a new generation of post quantum cryptographic technologies that will enable long term DoW mission success and provide assured communications in the face of ever evolving and capable adversaries. The PQC transition is necessary to ensure resilient warfighter communications, to address potential disruptions during conflict, and protect command and control (C2) systems domestically and globally.

To prepare warfighting systems and for a future battle space enabled by Cryptographically Relevant Quantum Computers (CRQC) the Department must achieve strategic goals with deliberate, effective, and efficient actions. Specifically, the DoW must:

- Fully understand the most consequential challenges and vulnerabilities of legacy cryptographic systems on mission relevant timelines and their scope of use.
- Design, build, and deploy new classes of High Assurance End Cryptographic Units (HA-ECU) and embedded cryptographic modules.
- Identify ways to leverage agile and interoperable commercial technologies to the greatest extent possible while increasing security and functionality.
- Align authorities, responsibilities, and funding streams to smooth the execution of Department wide modernizations.
- Integrate and streamline device certification and system authorization processes.
- Prioritize modernization efforts based on mission criticality, ease of system migration, and impacts.
- Prepare and implement adaptive and autonomous defense-in-depth mitigation and response strategies, including cryptographic agility, for an unpredictable quantum future state, to include new processes for testing, distributing, and installing critical cryptographic updates and patches.
- Assess cryptographic security and functionality for defense-specific system needs.

Moreover, **no later than December 31**, **2030**, all DoW systems must support PQC or be phased out, and no later than **December 31**, **2031**, all DoW systems must use PQC, unless otherwise noted. For PQC, National Security Systems (NSS) must support Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).

To achieve these strategic goals this strategy defines an overall vision that *all DoW NSS and all non-NSSs employ interoperable, agile, secure, and post quantum cryptographic systems* and provides five major lines-of-effort (LOEs) to enable this vision:

- **LOE 1: Optimize DoW Governance** to provide guidance/oversight and to inform responsible stakeholders, address policy limitations, and allocate resources efficiently, and ensure continued support for warfighter security and functionality needs.
- **LOE 2: Baseline Inventory and Plan** the migration of cryptographic technologies used in DoW Systems.
- **LOE 3: Develop and Analyze** CRQC resistant algorithms, protocols, and solutions to support the migration to PQC.

- **LOE 4: Integrate Commercial Solutions** that utilize approved and secure National Institute of Standards and Technology (NIST) and National Security Agency (NSA) post quantum algorithms within DoW systems (including weapon platforms) while meeting stringent warfighting requirements.
- **LOE 5: Deploy Quantum Resistant Devices** and update and replace cryptography (both for High Assurance and Information Technology (IT) infrastructure), including hardening DoW weapon systems and supporting IT networks, while meeting stringent warfighting requirements.

The Post Quantum Cryptography Strategy details a critical and essential step in the modernization of the DoW Information Network (DoWIN) and therefore supports a multitude of DoW strategies. For the purposes of this strategy, the terms Post Quantum, Quantum Resistant, Quantum Resilient, Quantum Safe, and Quantum Secure should be considered as analogous. Figure 1 highlights how the PQC strategy fits in the broader range of DoW Strategies.

Figure 1: Post Quantum Cryptography Strategy Relationships

Quantum Computing: Existential Threat

Cryptography is a foundational mission enabler across nearly all DoW systems. From the authorization and deployment of nuclear weapons to the execution of coordinated maneuvers with mission partners, insecure communications pose an existential threat to DoW missions.

A peer adversary using a CRQC, (e.g., a computer that can break present day asymmetric cryptography) presents a substantial threat to DoW systems that are protected by current asymmetric (and some symmetric) cryptographic algorithms. The extent to which an adversary can impact the confidentiality, integrity and availability of U.S. systems, missions, and interests can include, but are not limited to:

- Collection and decryption (e.g., through "Harvest Now, Decrypt Later" attacks) of U.S. classified information transmitted over terrestrial, space, Radio Frequency (RF), and other network infrastructure.
- Unfettered access to DoW information systems by breaking current Public Key Infrastructure (PKI) enabled authentication and authorization systems allowing adversaries to impersonate legitimate users.
- Unauthenticated and unauthorized adversarial access that results in adversarial control of DoW systems with the potential for adversarial weaponization of DoW capabilities against the DoW.
- Installation of potentially undetectable malware on DoW weapon system software through compromised software and firmware updates with forged signatures; and
- Access to C2 of warfighting systems in theater, resulting in integrity failures and loss of U.S. information dominance.

Department of War Post Quantum Cryptography Framework

The DoW PQC Framework (Figure 2) defines and organizes five LOEs necessary to achieve the vision of interoperable, agile, secure, and post quantum cryptographic solutions deployed within DoW systems. Each of these LOEs are divided into high-level objectives (detailed in the following pages). The order of the LOEs does not explicitly imply the order in which activities must occur. Many of the time-based objectives will occur simultaneously across the LOEs, with some currently in progress to achieve the vision. This framework seeks to provide a high-level view of those processes necessary to achieve post quantum cryptography.[1]

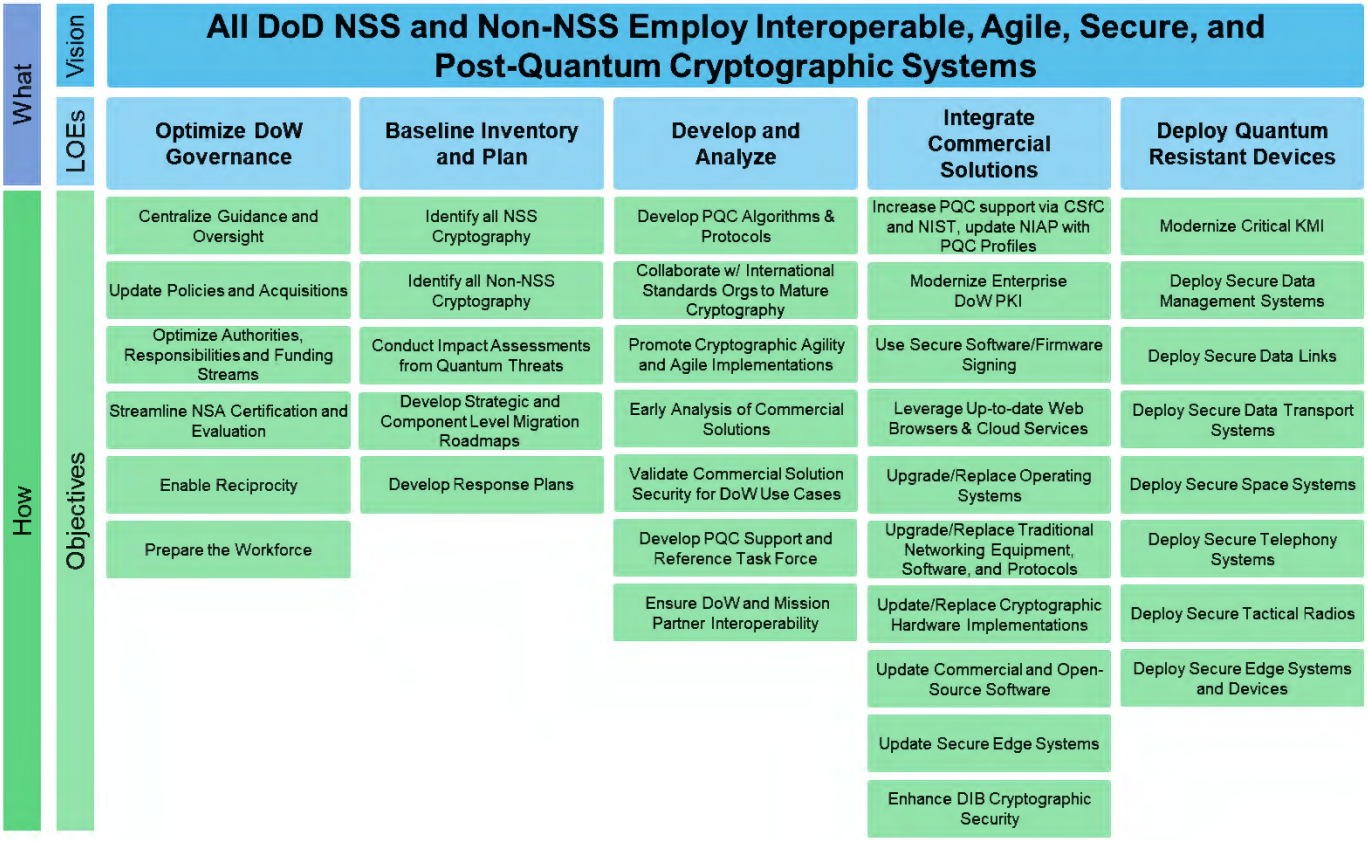


Figure 2: DoW PQC Framework

[1] "Report on Post-Quantum Cryptography" July 2024

Department of War Strategic Path

The DoW PQC Strategic Path (Figure 3) provides a decomposition of the objectives within the LOEs and demonstrates how they interrelate in the context of system development. The complexity, costs, and timing of the resulting acquisition paths are largely based on the category of cryptographic device(s) and the importance of the mission they support. For the purposes of this strategy these categories are: **High Assurance ECU** and **Commercial Solutions**.

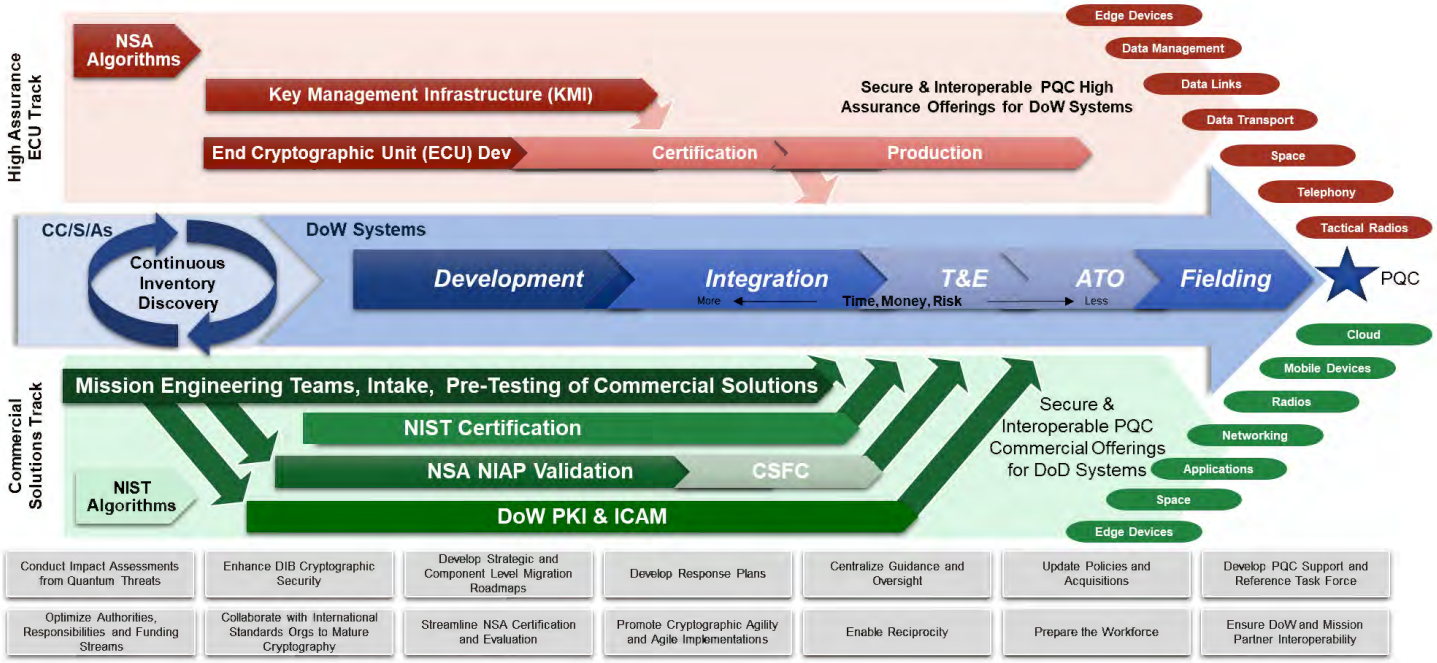


Figure 3: DoW PQC Strategic Path

High Assurance ECU Track

The High Assurance ECU Track is informed by the Cryptographic Modernization 2 (CM2) Initial Capability Document and related road maps. The High Assurance ECU Track organizes the relevant ECUs by function type (e.g., Data Links) and outlines two different acquisition methodologies: Special Purpose and General Purpose. All ECUs are dependent on the NSA Key Management Infrastructure (KMI). Additionally, all High Assurance Devices must be certified by the NSA, with the NSA assuming the risk when device is used in accordance with the Operational Security Doctrine.

Commercial Solutions Track

The Commercial Solutions Track is largely dependent on the commercial adoption and integration of NIST PQC Algorithms within commodity IT leveraged by DoW Systems. This applies to Low and Medium Assurance as well as High Assurance systems made available through the Commercial Solution for Classified (CSfC) Program. The complexity and cost of introducing updated commercial commodity IT will depend on

the nature of the system. For example, for systems within the commercial cloud, the transition will largely be transparent; for complicated weapon systems and other systems-of-systems, modernizing commercial IT is likely to take a significant amount of time and be costly. Many of these systems within this track will be dependent upon/enabled by the DoW PKI.

Essential Requirements of PQC Migration

Deployment of PQC must encompass all areas where CRQC-vulnerable cryptography is currently used, from DoW weapons systems and enterprise software to edge devices and critical infrastructure. As such, high order characteristics of a successful migration should be understood by all DoW stakeholders. These qualities include:

Maintain Warfighting Capability

Mission capability and capacity should not be sacrificed during the migration.

Vulnerability Deprecation

Quantum resistance is not achieved when PQC is rolled out but when quantum-vulnerable solutions are deprecated. Therefore, a mission thread is only quantum resistant when there is no use of vulnerable algorithms or protocols in the protection of critical data across the entire data pathway and lifecycle. This includes supply chains, development, at-rest, and in transit.

Do Not Introduce New Security Risks

During the migration, planners should be careful not to introduce other new technical security risks while mitigating quantum risks. General security risks to avoid introducing include new entities or network points with access to keying material or introduction of longer key lifespans. Solutions that lack PQC authentication (i.e., migration of confidentiality only) will not be considered fully PQC. Rigorous analysis of PQC solutions and assessment of potential threat model changes for the integrated systems are critical prior to deployment.

Concrete examples of technologies introducing technical security risks that should not be used as security solutions for quantum resistance include quantum communication technologies, such as quantum key distribution (QKD) and quantum networking, solutions combining QKD with other cryptographic key establishment, or non-local quantum randomness generation. While such quantum communication technologies may offer other functional properties, they will not be used as a means for achieving security for confidentiality, data or entity authentication, key distribution, or non-local randomness generation.

Furthermore, solutions using CRQC-vulnerable cryptographic algorithms with longer key sizes will not be considered fully quantum resistant. Any such solutions that cannot be updated to PQC algorithms will be phased out and replaced **not later than December 31, 2030**, unless otherwise

noted. PQC is required for all cryptographic uses **not later than December 31, 2031**, unless otherwise noted.

For non-High Assurance use cases, the following approaches will not be considered fully quantum resistant: symmetric key establishment protocols, symmetric key agreement protocols, symmetric key distribution protocols, and/or use of cryptographic pre-shared keys (PSK) for quantum resistance (when not provisioned through NSA KMI for High Assurance devices). Any such solutions will be phased out **not later than December 31, 2030**, unless otherwise noted, and Components will not test, pilot, use, or procure commercial solutions of these types for quantum resistance. Use cases where symmetric key distribution protocols have been in use prior to 2010 are exempt from this requirement as not introducing new risks. However, upgrading to asymmetric PQC algorithm-based key establishment should be investigated. Uses of PQC proxy solutions instead of upgrading to PQC **will** be avoided.

Migration Variants

During migration, planner should consider PQC integration options:

- **In-place migration**: Quantum vulnerable cryptography will be replaced with PQC components within a system. This approach generally offers cost savings and minimal system disruption. PQC variants of existent cryptographic approaches may not always be capable of supporting operational models and functional needs, necessitating alternative technical PQC approaches. Interoperability needs must be considered in all migration cases.
- **Re-platform**: Changing a platform solution or adding new cryptography providers to an existing system. This results in a new or upgraded system that offers PQC and is generally necessary for cryptographic hardware components.
- **Retire the service**: A service end-of-life date may be set for withdrawing a system from use entirely by the migration deadline, as an alternative to migrating it.

Line of Effort 1: Optimize DoW Governance

The DoW must plan, organize, and govern to enable full PQC transition within deadlines.

Why it Matters: Governance remains a challenge for the DoW where PQC is not immune. Current mechanisms are based on traditional processes for routine development and integration of cryptographic technology. Changes in governance and oversight is essential in streamlining and accelerating migration to PQC.

How to Measure: Amendment to current guidance accelerates PQC compliance to meet established timelines. Changes to policy are identified and adopted. Approval and integration rates of PQC solutions increases to meet NSM-10 deadlines.

Objective	Overview
Centralize Guidance and Oversight	DoW **will** create a centralized governance and oversight body and work with existing DoW Components and services to provide recommendations and Department-wide guidance for PQC migration. This will support maintaining compliance with PQC migration roadmaps and timelines, enable the DoW to maintain visibility, facilitate the development of appropriate technical and funding support to Components, and ensure mission driven migration to PQC.
Update Policies and Acquisitions	The DoW **will** review existing Departmental policies and acquisition authorities to determine where efficiencies are needed to accelerate the migration to PQC. Additionally, the DoW and its Components **will** update acquisition processes to streamline testing and deployment capabilities.
Optimize Authorities, Responsibilities, and Funding Streams	The DoW **will** work to address limitations and inefficiencies within authorities, responsibilities, and funding-streams.

Streamline NSA Certification and Evaluation	The DoW, in collaboration with the NSA, **will** identify and adopt strategies for prioritizing among and streamlining the NSA cryptographic evaluation and certification for DoW-relevant solutions. Additionally, the DoW will streamline intake and approval tracking across NSS and non-NSS. This will enable critical solutions to be fielded at the speed of relevance necessary to mitigate risk and keep pace with innovation.
Enable Reciprocity	The DoW Components **will** leverage reciprocity from similar systems and implementations to assist in the timely deployments, reduce costs and accreditation overhead, and ease the overall burden on the workforce. DoW Components will share the responsibility of building and using joint requirements, rather than duplicating services, certification, or testing.
Prepare the Workforce	The DoW **will** create and distribute training and materials to prepare the workforce for development of PQC understanding and system migration to PQC.

Line of Effort 2: Baseline Inventory and Plan

DoW planners and systems owners must identify **all** cryptography in use in both NSS and non-NSS, which of those are quantum-vulnerable, what systems rely on a security feature(s) dependent on CRQC-vulnerable cryptography, and their organizations' exposure to the ongoing CRQC threat. Furthermore, planners must prioritize modernization efforts based on risk, mission threads, data pipelines, and assess the impact of the CRQC threats to systems and data.

Why it Matters: To effectively plan for the PQC migration and mitigate the quantum risk, it is necessary to understand where cryptographic systems are in use and all cryptography across the DoW. Per NSM-10 and M-23-02 "Migrating to Post Quantum Cryptography," the use of cryptography in NSS and non-NSS must be inventoried and reported.[2] This applies to all assurance levels. Centralized inventories will enable the DoW to properly track enterprise level migration status and ensure that all gaps are covered in the planning processes.[3] Inventory will assist DoW Components identify and prioritize systems for migration and monitor and track their status of migration.

How to Measure: Planners should consider: percent of DoW systems using cryptography with reported details, Service Components reporting inventory, number/type/location of implementations, and known adversary collection events.

Objective	Overview
Identify All NSS Cryptography	DoW Components **will** identify and report to DoW CIO and the NSA all High Assurance, CSfC, Cryptographic High Value Product (CHVP), and Medium and Low Assurance cryptographic capabilities within their NSSs[4], including within NSS that integrate PKI and NSS such as cloud services. This inventory should include vulnerability assessment where applicable. Additionally, the DoW should investigate the potential use of automated cryptography discovery and inventory (ACDI) tools to support inventory efforts where appropriate.

[2] NSM-10 Sec 3(c)(xi)

[3] Quantum-Readiness: Migration to Post-Quantum Cryptography, Cybersecurity Infrastructure Security Agency, National Security Agency, National Institute of Standards and Technology, August 21, 2023

[4] NSM-10 Sec3 (c)(xi)

Identify all Non-NSS Cryptography	DoW Components **will** identify and report to DoW CIO all cryptographic capabilities present within non-NSSs[5], including Defense Industrial Base (DIB) systems that hold/process DoW data. Processes and tools for efficiency and automation should be considered where appropriate. Inventory should include vulnerability assessments where applicable.
Conduct Impact Assessments from Quantum Threats	For identified CRQC vulnerable systems, DoW Components **should** estimate the potential adversarial collection and decryption of associated traffic and the short/long term impact of that data being known by adversaries, as well as impact of adversarial capability to own or control systems and data through authenticity vulnerabilities. DoW Components should consider engaging DoW intel and threat expertise while executing this objective (e.g., NSA). This information is critical to establishing migration prioritization plans.[6]
Develop Strategic and Component Level Migration Roadmaps	DoW Components **will** leverage DoW guidance and strategy documents as well as NSA deprecation guidance on CRQC-vulnerable cryptography to create roadmaps for PQC migration. Roadmaps should be tailorable to individual Components, account for strategic system prioritizations and be maintained/updated during the migration. Early cryptographic solution analysis, interoperability, and future cryptographic agility should be considered with these roadmaps.
Develop Response Plans	The mission impact assessment estimation of adversarial compromise and impacts (e.g., general security, mission failures, etc.) **should** form the basis for advance response planning to mitigate the risk to DoW missions, personnel, and security. Mission planning alternatives and response plans should be considered and developed as appropriate to enable mission survivability in the case of quantum threat exploitation of vulnerable cryptographic systems.

[5] Formerly known as Type 2, 3, & 4 cryptographic products

[6] Derived from NSM-10 – identified area for additional understanding

Line of Effort 3: Develop and Analyze

DoW Components must ensure that secure algorithms & protocols are developed and analyzed for use in the DoW, including engaging with international standards bodies on protocol standards and ensuring commercial technologies properly implement those standards. Resulting products and solutions should also be analyzed for security and functionality needs within warfighting use cases, and systems must be assessed for suitability and cost of in-place migration, re-platforming, or retirement of service.

Why it Matters: If DoW equities are not represented within international standards bodies or active in suitability and system needs assessments for commercial solutions, then migration to PQC will not be possible without significant risks to security, functionality, and interoperability.

How to Measure: Planners should consider engagement with international standards bodies and modern standardization methods, security vetting of cryptography-enabled solutions, functionality testing of commercial solutions, and use case determination for suitability of in-place migration, re-platforming, or retirement of service.

Objective	Overview
Develop CRQC Algorithms and Protocols	NIST and the NSA **will** develop and publish certified post quantum algorithms that will be implemented in cryptographic products within the DoW. Additionally, the DoW and NSA will develop PQC protocols, as needed, that can incorporate PQC algorithms and introduce designs to international standards bodies as appropriate.
Collaborate with International Standards Organizations to Mature Cryptography	The DoW and NSA **will** collaborate with standards organizations for standardization of relevant protocols, variants, and novel approaches that incorporate PQC algorithms to enable open source and widely used communication and security standards. Additionally, the DoW should engage with standards organizations on use case needs to ensure that functionality considerations of DoW systems are accounted for in protocol development and profiles. This includes participation in the North Atlantic Treaty Organization (NATO) standards body, Internet Engineering Task Force (IETF), and similar organizations to ensure interoperability.

Promote Cryptographic Agility and Agile Implementations	The DoW and DIB **will** investigate agile cryptographic implementations. Agile solutions will enhance the DoW's ability to respond to future cryptographic threats and reduce the cost, time, and effort needed to update or migrate to new cryptographic algorithms and protocols moving forward. This may include implementation of multiple algorithm and protocol options beyond defaults and should include pathways for updating and replacing algorithms and protocols swiftly, as required. The DoW **must** ensure enablement of cryptographic agility does not introduce new vulnerabilities.
Early Analysis of Commercial Solutions	The DoW **will** position itself to ensure early, preliminary analysis of commercial and DoW developed cryptography-enabled solutions to ensure that they meet security requirements and PQC needs. Early analysis of cryptography-enabled solutions will enhance the DoW's ability to assess solution viability quickly and centralize intake of potential solutions that meet security requirements, conserving DoW and NSA resources to prioritized solutions based on mission need.
Validate Commercial Solution Security for DoW Use Cases	The DoW **will** validate the cryptography-enabled solutions' security within the context of the specific use case needs and threat model, including commercial and DoW solutions. This includes not only that solutions utilize approved PQC algorithms and have passed early analysis while also meeting the security and functional needs of the intended use case. This may include jamming resilience, latency needs, key-compromise resilience, etc. Additionally, the DoW should ensure that implemented solutions do not utilize symmetric key establishment or distribution, PSK-based solutions without PQC asymmetric key establishment derivation, QKD, non-local quantum randomness generation, or quantum networking as a security solution for quantum resistance.
Develop PQC Support and Reference Task Force	The DoW **should** stand up a centralized task force for migration and acquisition support, early analysis, commercial solution review, and use case alignment to ensure support for cases not explicitly clear in guidance, such as in special operations or new DoW systems still in the acquisition process, and to alleviate the risk and costs of mis-assessed acquisitions.
Ensure DoW and Mission Partner Interoperability	Components **will** ensure coordination to mitigate risk in the mission partner environment. The responsible, accountable, consulted and informed (RACI) chart, (Appendix B), provides strategic objectives in which mission partners should be involved.

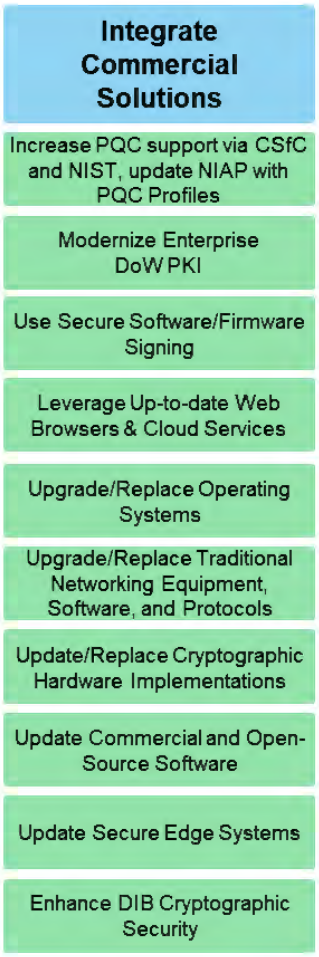
Line of Effort 4: Integrate Commercial Solutions

The DoW Components must work to update and integrate PQC compliant commercial products and solutions into mission systems**,** contract requirements, and acquisition decisions aligned with this strategy.

Why it Matters: DoW systems and missions are highly reliant on commercial products and services. Commercial products and services process and transport non-public, sensitive, and potentially classified DoW information, including in weapon systems. Coordination with commercial vendors and requirements integration in open-source software are essential to ensure that PQC requirements are adopted across the DoWIN in commodity IT as well as in edge systems reliant on cryptography.

Systems with controlled software baselines (e.g., weapon systems) will require deliberate planning and integration testing.

How to Measure: For DoW to understand this LOE's progress, planners should track vendor roll-out of PQC compliant software and services; industry security analysis status on solutions; Component pre-testing of commercial solutions; Component-level tracking of program of action and milestones (POA&M) associated with system upgrades and modernizations. Meanwhile they should ensure interoperability of systems in accordance with mission needs, security assessments, functional suitability, and approval of commercial PQC solutions prior to acquisitions and implementation.



Objective	Overview
Increase PQC support via CSfC and NIST, and Update NIAP with PQC Profiles	DIB Partners will continue to develop a variety of post quantum commercial-off-the-shelf (COTS) solutions supporting Top Secret, Secret, and Unclassified uses (e.g., network devices, firewalls, mobile devices, and government-off-the-shelf (GOTS) products) certified through the CSfC program and NIST accreditation, that DoW Components acquire and integrate. National Information Assurance Partnership (NIAP) evaluation **will** be streamlined and enhanced through suitable guidance, integration of PQC, and development of end-to-end encryption protection profiles.
Modernize Enterprise DoW PKI	DoW PKI support of NIST algorithms is a critical enabler for a variety of asymmetric cryptographic based systems. DISA and the DoW Components **will** ensure DoW PKI (at all classification levels) is upgraded in line with the availability of commercial PQC solutions.

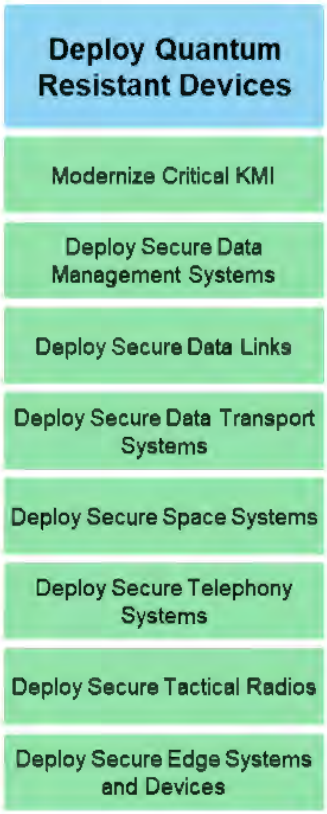
Use Secure Software/Firmware Signing	Software and firmware signing, used to secure DoW software supply chains, **will** be updated to PQC algorithms (e.g., tool, applet, hardware, or firmware upgrades). Inventories of software signing tools and firmware signing dependencies is necessary to understand which vendors must be reviewed, supported, or updated for PQC-readiness and the timeline for mitigation or replacement.
Leverage Up-to-date Web Browsers and Cloud Services	DoW Components **will** use PQC compliant web-browsers and cloud services. For modern DoW IT systems leveraging cloud services, ensuring up-to-date web browsers that support PQC algorithms is an important step. However, full PQC compliance is dependent on the DoW PKI and cloud services also implementing and using compliant algorithms for PQC confidentiality and authenticity of data. DoW networks will be tested to ensure that intermediate devices (e.g., firewalls, traffic inspection solutions) do not allow downgrading of protocols to non-PQC algorithms.
Upgrade/Replace Operating Systems	DoW Components **will** use PQC ready operating systems. Leveraging up-to-date operating systems is a significant step in DoW's PQC efforts. Upgrading enterprise and niche DoW systems' (e.g., weapon systems) underlying operating systems is likely to require careful planning and integration testing to ensure related COTS and GOTS software within these environments continue to operate.
Upgrade/Replace Traditional Networking Equipment, Software, and Protocols	DoW Components **will** use PQC ready networking. Traditional networking equipment, software, and protocols (e.g., routers, firewalls, proxies, switches) connect significant portions of the DoWIN and **must** be updated to PQC algorithms, protocols, and certificates to protect communications. The deployment of PQC-ready networking equipment, software, and protocols will provide a significant layer of security for DoW systems and help create wide-spread quantum security in conjunction with other PQC readiness efforts or as an intermediate mitigation for systems with longer timelines. This includes both data in transit and data at rest. To be interoperable, networking equipment must mutually support PQC algorithms as well as PQC networking protocols. Proxy solutions for PQC should be avoided with a focus instead on actual network upgrades to PQC.

Update/Replace Cryptographic Hardware Implementations	DoW Components **will** use PQC supportable hardware and associated implementations, including firmware. The DoW relies on widely used commercial solutions that deploy their own hardware implementations (e.g., Trusted Platform Module (TPM) and Hardware Security Module (HSM)). The replacement of these hardware implementations with systems and solutions that utilize PQC is necessary to secure and protect the DoWIN. Post quantum data-at-rest solutions must also be utilized to ensure that data stored across the DoW is protected through PQC.
Update Commercial and Open-Source Software	A significant portion of DoW systems rely on commercial and open-source software. The DoW **will** ensure that all commercial and open-source software used, which includes cryptographic elements, is upgraded to PQC.
Update Secure Edge Systems	DoW Components **will** update, replace, or remove from use edge systems that are utilizing CRQC-vulnerable cryptography across the DoW to ensure continued mission effectiveness and security in all systems, including, but not limited to, unmanned systems, space systems, and sensor grids.
Enhance DIB Cryptographic Security	To ensure the security of DoW information hosted on DIB systems, the DoW **will** ensure that the DIB migrates to PQC across the enterprise. The DoW will also collaborate with DIB[7] partners to ensure interoperability during the migration to PQC. This includes PQC protection on access control, zero trust (ZT), and software development platforms. The DoW will update the Cybersecurity Maturity Model Certification (CMMC) to include requirements for PQC and update external certificate authorities to utilize PQC certificates.

[7] Defense Industrial Base Cybersecurity Strategy 2024

Line of Effort 5: Deploy Quantum Resistant Devices

DoW must certify, pre-test, build (or update), test, integrate, deploy, and maintain a variety of quantum resistant devices and platforms across the entire DoW NSS and non-NSS inventory. It must also deprecate and remove from use all legacy devices and platforms that cannot support PQC.



Why it Matters: DoW critical mission systems, weapon platforms, and IT infrastructures employ a large variety of devices with embedded cryptography. Migrating these devices will be a significant challenge for DoW Components. Specifically, the acquisition process can be long and complicated, while the type and number to be built and deployed is significant. The deployment of new PQC High Assurance and commercial devices is critical to enable the DoW to maintain pace with the threat landscape.

How to Measure: Planners should consider: # *Type of ECU*, # to be built, # to be updated, ECU production capacity and rate, ECU integration lead time for each ECU, estimated year of elimination of the CRQC risk for each ECU within the objective categories below.

Objective	Overview
Modernize Critical KMI	The NSA **will** adapt the KMI (for High Assurance devices only) for PQC algorithms while ensuring it maintains interoperability requirements and scales key production to meet DoW Component needs.
Deploy Secure Data Management Systems	The DoW and its Components **will** build or acquire post quantum data management systems that ensure data stored across the DoW is protected by PQC. Where applicable, the DoW will include additional modernization tasks during the upgrade process.
Deploy Secure Data Links	The DoW and its Components **will** update ECUs to support secure data links (e.g., common data link, tactical data link, identification friend or foe) to PQC. Changes **must** also meet interoperability requirements.
Deploy Secure Data Transport Systems	DoW Components **will** upgrade the systems at the transport layer (e.g., inline network encryptors, High Assurance internet protocol encryptors, high speed encryptors, and link/trunk encryptor family) to utilize PQC to ensure data-in-transit is protected by PQC.

Deploy Secure Space Systems	DoW Components operating or utilizing space systems (e.g., telemetry, tracking and control, ground operating equipment, and aerospace vehicle equipment) **will** implement PQC within to-be-deployed systems and upgrade all currently deployed systems capable of supporting PQC. Components must seek to address issues with interoperability and cryptographic vulnerabilities associated with previously deployed space systems or retire the system prior to the migration deadline.
Deploy Secure Telephony Systems	The DoW and its Components **will** upgrade or replace secure telephony systems (e.g., systems supporting secure communications interoperability protocol) to support PQC, ensuring classified voice communications remain secure against CRQCs. Upgraded telephony systems must continue to meet interoperability standards within the DoW and among mission partners and foreign allies.
Deploy Secure Tactical Radios	The DoW and its Components **will** upgrade or replace tactical radios (e.g., single band, multi-band, single channel, multiple channel and specialty equipment) across the DoW to support PQC for secure communications, interoperability, and mission success in support of the warfighter. The refresh process should minimize interruption of warfighting capabilities while ensuring improvements to security and, where applicable, enhancements of functional capabilities.
Deploy Secure Edge Systems and Devices	The DoW and its Components **will** upgrade, replace, or remove from use all High Assurance edge systems and devices that are utilizing CRQC-vulnerable cryptography across the DoW to ensure continued mission effectiveness and security.

Appendix A: Acronyms

Acronym	Definition
ATO	Authorization to Operate
C2	Command and Control
CHVP	Cryptographic High Value Product
CMMC	Cybersecurity Maturity Model Certification
CNSA	Commercial National Security Algorithms
COTS	Commercial-Off-The-Shelf
CRQC	Cryptographically Relevant Quantum Computer
CSfC	Commercial Solutions for Classified
DIB	Defense Industrial Base
DoW	Department of War
DoWIN	Department of War Information Network
ECU	End Cryptographic Unit
GOTS	Government-Off-The-Shelf
HA-ECU	High Assurance End Cryptographic Unit
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IT	Information Technology
KMI	Key Management Infrastructure
LOE	Lines-of-Effort
NATO	North Atlantic Treaty Organization
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSM	National Security Memorandum
NSS	National Security System
PKI	Public Key Infrastructure
POA&M	Program of Action and Milestones
PSK	Pre-Shared Key
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
RACI	Responsible, Accountable, Consulted, and Informed
RF	Radio Frequency
TLS	Transport Layer Security Protocol
TPM	Trusted Platform Module
ZT	Zero Trust

Appendix B: Responsible, Accountable, Consulted, and Informed Chart

PQC Strategy RACI Chart						
LOE	**Objective**	**DCIO**	**NSA/CSS**	**DoW Components**	**DIB Partners**	**FVEY**
Optimize DoW Governance	Centralize Guidance and Oversight	R	C	I		
	Update Policies and Acquisitions	R	R	R		
	Optimize Authorities, Responsibilities, and Funding Streams	R	C	I		
	Streamline NSA Certification and Evaluation	I	R/A	I		
	Enable Reciprocity	R		I		
	Prepare the Workforce	A		R		A
Baseline Inventory and Plan	Identify all NSS Cryptography	I	A	R	C	R
	Identify all non-NSS Cryptography	A	I	R	C	R
	Conduct Impact Assessments from Quantum Threats	A	R/C	R		
	Develop Strategic and Component Level Roadmaps	R/A	C	R	C	
	Develop Response Plans	A	C	R		
Develop and Analyze	Develop CRQC Resistant Algorithms & Protocols	R/C	R/A			
	Collaborate with International Standards Organizations to Mature Cryptography	R	R	R	R	
	Promote Cryptographic Agility and Agile Implementations	A	C	R	R	
	Early Analysis of Cryptography-Enabled Solutions	R/A	C	R	I	
	Validate Cryptography-enabled Solution Security for DoW Use Cases	R/A	R	I	I	
	Develop PQC Support and Reference Task Force	R	C	I	I	
	Ensure DoW and Mission Partner Interoperability	A	C	R	C	
Integrate Commercial Solutions	Increase PQC support via CSfC and NIST, Update NIAP with PQC Profiles	A	R	I		
	Modernize Enterprise DoW PKI	R/A	C	I		
	Use Secure Software/Firmware Signing	A	C	R	C	R
	Leverage Up-to-date Web Browsers & Cloud Services	A	C	R	C	
	Upgrade/replace Operating Systems	A	C	R	C	
	Upgrade/replace Traditional Networking Equipment, Software, and Protocols	A	C	R	C	R
	Update/Replace Cryptographic Hardware Implementations	A	C	R	C	R
	Update Commercial and Open-Source Software	A	C	R	C	R
	Update Secure Edge Systems	A	C	R	C	R
	Enhance DIB Cryptographic Security	A	C	R	R	
Deploy Quantum Resistant Devices	Modernize Critical KMI	A	R	I		I
	Deploy Secure Data Management Systems	A	C	R		R
	Deploy Secure Data Links	A	C	R		R
	Deploy Secure Data Transport Systems	A	C	R		R
	Deploy Secure Space Systems	A	C	R		
	Deploy Secure Telephony Systems	A	C	R		
	Deploy Secure Tactical Radios	A	C	R		R
	Deploy Secure Edge Devices	A	C	R		R

Key: R = Responsible, A = Accountable, C = Consulted, I = Informed

Appendix C: References

- CNSSP 15, *Use of Public Standards for Secure Information Sharing*, March 2025
- *Cryptographic Modernization 2 (CM2), Initial Capability Document (ICD),* Version 2.0, October 2023, National Security Agency (NSA).
- Defense Industrial Base Cybersecurity Strategy 2024, March 2024, Department of Defense Chief Information Officer.
- M-23-02, Migrating to Post-Quantum Cryptography, November 2022
- National Security Memorandum-10, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, May 2022.
- *NSA|CNSA Suite 2.0 and Quantum Computing FAQ*, December 2024 Ver. 2.1
- Quantum-Readiness: *Migration to Post-Quantum Cryptography*, August 2023, Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf
- Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2019, Through June 30, 2020, December 2020, DoW Office of Inspector General.