DOW CIO Memo

Preparing for Migration to Post Quantum Cryptography

November 18, 2025

Overview

Preparing for Migration to Post-Quantum Cryptography is a DoW-wide memorandum issued by the Department of War Chief Information Officer on November 18, 2025. It establishes a structured framework for **transitioning DoW systems**, **networks**, and **platforms to quantum-resistant cryptographic solutions** in response to emerging quantum computing threats. The memorandum directs DoW Components – including Military Departments, Combatant Commands, and Defense Agencies - to inventory existing cryptographic implementations, designate PQC leads, and plan for the phased replacement of quantum-vulnerable encryption across information systems, National Security Systems, cloud environments, operational technology, and weapons platforms. It emphasizes centralized governance through the DoW CIO to ensure consistent, standards-based adoption of post-quantum cryptography.

The memorandum aligns DoW cryptographic modernization efforts with NIST and CNSS standards and sets enforceable timelines requiring the **phase-out of legacy cryptographic mechanisms by 2030**, with limited extensions for select systems. Together with existing federal cybersecurity and cryptographic policies, the memorandum establishes the foundation for DoW-wide cryptographic agility, long-term cyber resilience, and secure communications in the post-quantum era.

Framework

The memorandum establishes clear expectations for how cryptographic risk is managed across the DoW enterprise. Organizations are required to maintain accurate awareness of cryptographic dependencies, coordinate all post-quantum cryptography (PQC) activities through designated points of contact, and obtain appropriate approval before initiating PQC testing, evaluation, or acquisition efforts. The memo reinforces disciplined implementation by restricting unapproved technologies, requiring ongoing coordination with the DoW CIO, and ensuring that cryptographic changes are documented, reviewed, and aligned with approved security and interoperability standards.

What Does This Mean for Government?

The Department of War will face new mandates to:

- Maintain visibility into cryptographic implementations across systems, networks, and platforms.
- Designate accountable leads to coordinate post-quantum cryptography planning and reporting.
- Centralize approval of post-quantum cryptography testing, acquisition, and deployment activities.
- Plan for the phased replacement of quantum-vulnerable cryptographic mechanisms within established timelines.

The memorandum represents a significant step in formalizing cryptographic modernization, making post-quantum readiness a core requirement for protecting government systems and communications.

What Does This Mean for Industry?

For contractors, integrators, and vendors supporting the DoW, the memorandum requires them to:

- Support NIST and CNSS-approved post quantum cryptography.
- Provide crypto-agile solutions that can transition away from quantum-vulnerable encryption.
- Align PQC testing and implementation with DoW CIO approval processes.
- Treat post-quantum readiness as a core requirement for future DoW engagements.

The memorandum establishes post-quantum cryptography as an expected capability for vendors supporting DoW systems.

Timeline

The following timeline summarizes key requirements, responsibilities, and milestones established by the memorandum to guide the Department's transition to PQC.

Requirement	Key Dates	Details & Responsible Entity
Halt unapproved PQC testing, evaluation, acquisition, or deployment	**Effective Immediately**	All DoW Components must coordinate any PQC-related activity with and obtain approval from the DoW CIO PQC Directorate; activities must cease immediately if security concerns arise
Conduct comprehensive cryptographic inventory	**Ongoing**	DoW Components are responsible for inventorying all cryptographic implementations across IT, NSS, cloud, weapons systems, platforms, OT, mobile, IoT, and business systems, including algorithms, protocols, key management, and dependencies.
Coordinate PQC planning and approvals	**Ongoing**	The DoW CIO PQC Directorate serves as the approval authority for PQC testing, evaluations, and migration approaches, ensuring alignment with CNSS and NSA direction.
Designate and report PQC migration leads	**December 8, 2025**	DoW Components (Military Services, Combatant Commands, and Defense Agencies) must identify a primary PQC point of contact responsible for cryptographic inventory, coordination, and reporting and submit contact information to the DoW CIO.
Update PQC points of contact	**Annually by September 30**	DoW Components must maintain and submit updated lists of component and subordinate PQC leads to ensure continuity of oversight and coordination.
Replace pre-shared key (PSK)–based cryptographic solutions	**December 31, 2030**	DoW Components must phase out PSK-based asymmetric and symmetric key establishment in favor of NIST-approved, quantum-resistant cryptographic mechanisms.
Replace symmetric cryptographic protocols	**December 31, 2030**	DoW Components must transition symmetric key establishment, key agreement, and key distribution protocols to PQC-approved approaches, unless an exception is granted.
Extended deadline for CSfC-registered systems	**December 31, 2031**	CSfC-registered systems operated by DoW Components may receive a one-year extension, subject to approval.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.