



CLEARED
For Open Publication

Nov 20, 2025

DEPARTMENT OF WAR
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

NOV 18 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

Subject: Preparing for Migration to Post Quantum Cryptography

Advancements of Quantum Information Science (QIS) and cryptanalytically relevant quantum computers requires expedited migration to quantum-resistant cryptography to safeguard the Departments' information systems, communications, and personnel. The migration to post quantum cryptography (PQC) must not only be planned and executed with deliberate urgency to maintain warfighter lethality and information dominance in the DoW global ecosystem, but also strategically coordinated. To achieve this level of coordination, we must identify PQC migration points of contact for information sharing and create processes for streamlining intake and prioritization of PQC solutions to support certification activities and timelines.

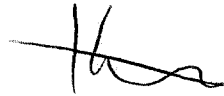
To assess risk and track PQC migration, it is imperative to identify and inventory any type of cryptography used in all DoW information systems including, but not limited to, national security systems (NSS), non-NSS, business systems, weapons systems, cloud computing capabilities, mobile devices, physical access control systems, internet of things, unmanned systems, and operational technology, regardless of classification, location, connection, type, purpose, or use. DoW CIO will be releasing a DoW-wide task to identify, inventory, and report all cryptography used in any type of system as an initial step outlined in the DoW PQC Strategy mandated by Office of Management and Budget Memorandum 23-02, "Migrating to Post-Quantum Cryptography," Nov 18, 2022.

In preparation for the release and execution of the DoW PQC Strategy and the scale of coordination required for PQC migration, it is essential to identify key personnel, Department-wide within every DoW Component, who will be responsible for migration to post quantum cryptography and associated coordination. These leads will be responsible for cryptographic inventory, PQC coordination on migration with the DoW CIO PQC Directorate, PQC acquisition requirements within the Component, quantum-attack risk management plans, coordination with other related Component leads for PQC, dissemination of PQC information, and tracking of all tests, evaluation, and PQC readiness efforts relevant to the component's systems. The contact information for PQC migration leads in each subordinate organization within all Components (name, title/role, email, phone, local group/dept./org, DoW Component (e.g., Navy NAVSEA), location (i.e., base, post, camp, station, ship)) must be collected by the Component lead and provided to my point of contact below within 20 days of date of this Memorandum. Each DoW Component will maintain lists of subordinate points of contact and provide an updated list to my point of contact below by September 30, annually. Points of contact will be responsible for coordinating with the DoW CIO PQC Directorate on cryptographic migration. Coordinated work across NSA, DoW PKI, and DISA with the DoW CIO PQC Directorate also continues to support consistent and streamlined guidance.

DoW Components currently, or in the future, testing, developing, evaluating, piloting, researching, investing in, prototyping, demonstrating, implementing, integrating, or any planned or actual acquisition, hereinafter referred to as “engagement”, of PQC or PQC related technologies (i.e., discovery, inventory, migration, enablement, etc.) must submit relevant artifacts (i.e., test plans, test results, acquisition artifacts, risk mitigations, etc.) to my office immediately. My office will review the artifacts and determine if there are risks, unmitigated security considerations, or use restrictions that need to be addressed prior to acquisition or PQC engagement. All identified issues must be addressed and verified as mitigated by my office prior to acquisition or engagement. Systems with security or interoperability considerations which cannot be mitigated, do not have a sufficient mitigation plan, or are not mitigated based on the use environment, as assessed by my office, will be removed from PQC engagement and use by the relevant Component(s) immediately.

The attachment includes requirements and security considerations regarding PQC and PQC-related technologies which DoW Components must follow to ensure consistent and coordinated approach to PQC migration. The requirements in the attachment are effective immediately. This Memorandum and attachment do not change or supersede existing authorities or responsibilities of the National Manager. As stated above, we must strategically streamline and execute while maintaining close collaboration to ensure interoperability, reduce duplication, and optimize fiscal investments.

The Department of War lead for PQC and point of contact for this memorandum is Dr. Britta Hale. Dr. Hale and the PQC Directorate can be reached at osd.pentagon.dod-cio.mesg.dcio-cs-pqc@mail.mil.



Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of War

Attachment:
As stated

Nov 20, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Subject: Preparing for Migration to Post Quantum Cryptography

1. DoW Components will:
 - a. Comply with the requirements in this Memorandum and attachment. New PQC requirements, PQC approval, migration, and use processes, and updated information will be maintained at <https://cybersecurityks.osd.mil/DoDcs/pqc> to ensure expedited dissemination, improve coordination, and consistent messaging in one authoritative location.
 - b. Inform and provide artifacts to Director, DoW CIO PQC, of current or future plans to test, evaluate, pilot, invest in, use, or acquire any PQC-enabling or PQC-related technology (i.e., discovery and inventory tools, migration, enablement, cryptographic security solutions, etc.), including technologies described as quantum resistant or quantum resilient.
 - c. Provide Director, DoW CIO PQC, any related artifacts or technology descriptions, or obtain any further descriptions as may be required to inform cryptographic use authorization.
 - d. Obtain cryptographic intake approval, as issued by Director, DoW CIO PQC, before testing, evaluating, piloting, investing in, using, or acquire any PQC-enabling or PQC-related technology, including technologies described as quantum resistant or quantum resilient.
 - e. Obtain cryptographic deployment approval, as issued by Director, DoW CIO PQC (and informed by Intelligence Community, National Institute of Standards and Technology (NIST), and National Security Agency certification outcomes), before deployment of any PQC-enabling or PQC-related technology, including technologies described as quantum resistant or quantum resilient.
 - f. Cease tests, pilots, functional or performance evaluations, investment, acquisition, obligation, or use of the technology immediately if security issues are identified by the Director, DoW CIO PQC, and coordinate with the Director, DoW CIO PQC for remediation or alternatives.

The above requirements are in addition to requirements issued by the Committee on National Security Systems (CNSS), CNSS Policy #15, "Use of Public Standards for Secure Information Sharing," December 2024, and Chairman of the Joint Chiefs of Staff Instruction 6510.02, "Cryptographic Modernization Planning," Aug 16, 2022.

2. DoW Components will not test, evaluate, pilot, use, or procure the following technologies or capabilities for the purposes of providing confidentiality, authenticity, or integrity in DoW networks and communications:

ATTACHMENT

- a. Quantum Confidentiality or Keying Technologies. Examples of these include but are not limited to quantum key distribution (QKD); solutions combining QKD with other cryptographic key establishment; quantum communications or networking; non-local quantum randomness generation; or non-FIPS random number generation. While such quantum communication technologies may offer other functional properties, they shall not be used as a means for achieving security for confidentiality, data or entity authentication, key distribution, or non-local randomness generation. Such solutions shall not be used unless provided exception by the point of contact above.
3. DoW Components will phase out and replace all of the following types of cryptographic solutions:
 - a. Use of cryptographic pre-shared keys (PSK) for providing quantum resistance in solutions where the PSK is not provisioned through NSA KMI for Type 1 devices. These solutions will be phased out and replaced with solutions using NIST-approved (respectively, CNSA 2.0-listed for National Security Systems) asymmetric PQC algorithms for key establishment no later than December 31, 2030, unless otherwise directed or provided exception by the point of contact above.

Additionally, DoW Components will not test, pilot, use, or procure commercial PSK-based solutions for quantum resistance effective immediately.

- b. Symmetric key establishment protocols, symmetric key agreement protocols, and symmetric key distribution protocols. These solutions shall be phased out and replaced no later than December 31, 2030 (or no later than December 31, 2031, for solutions currently registered with NSA CSfC), unless otherwise directed or provided exception by the point of contact above.

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.

Additionally, DoW Components will not test, pilot, use, or procure commercial solutions of this type (i. e., symmetric key establishment protocols, symmetric key agreement protocols, and symmetric key distribution protocols) for quantum resistance effective immediately.