Post Quantum Cryptography Strategy

June 23, 2026

Overview

Released on June 23, 2026, the Department of War (DoW) Post-Quantum Cryptography (PQC) Strategy establishes a department-wide plan to secure military communications, data, and command-and-control systems against future quantum-enabled threats. The strategy recognizes quantum computing as a significant risk to current cryptographic protections and outlines an accelerated transition to quantum-resistant encryption across defense systems.

Aligned with Executive Order 14409, the strategy sets clear modernization goals requiring high-impact systems to adopt PQC by 2030 and full implementation across the Department by 2031. It emphasizes maintaining operational readiness while upgrading cryptographic infrastructure, ensuring warfighting capabilities remain secure and uninterrupted during the transition.

Framework

The DoW PQC Strategy establishes a comprehensive framework for migrating defense systems to quantum-resistant cryptography, centered on long-term resilience, operational continuity, and mission assurance. It prioritizes replacing vulnerable cryptographic systems while avoiding disruptions to critical military functions and ensuring interoperability across platforms and partners.

Core elements include identifying vulnerabilities in existing cryptographic systems, developing and deploying new high-assurance cryptographic technologies, and integrating commercial solutions where appropriate to accelerate adoption. The framework also emphasizes crypto-agility, enabling systems to adapt quickly to evolving threats and future algorithm updates.

To operationalize this transition, the strategy is structured around **five key Lines of Effort (LOEs)**:

- Governance and Oversight – centralizing guidance and improving coordination across the Department.
- Inventory and Planning – identifying cryptographic assets and prioritizing systems for migration.
- Technology Development – advancing and testing quantum-resistant algorithms and solutions.
- Industry Integration – leveraging commercial technologies and strengthening partnerships.
- Deployment and Fielding – implementing PQC across warfighting systems and infrastructure.

Together, these efforts create a structured, enterprise-wide approach to ensuring all defense systems transition to secure, interoperable, and quantum-resilient cryptography.

What Does This Mean for the Department of War?

For the Department of War, the strategy drives a **full-scale modernization effort** across all mission systems and networks.

DoW components are expected to:

- Support the Conduct comprehensive inventories of cryptographic systems across both National Security Systems (NSS) and non-NSS environments.
- Identify and prioritize mission-critical systems vulnerable to quantum threats.
- Develop and execute migration plans to transition to PQC while maintaining operational capability.
- Deploy high-assurance cryptographic devices and upgrade existing infrastructure.
- Implement crypto-agility and defense-in-depth strategies to adapt to evolving threats.

Overall, the strategy positions PQC adoption as a **mission-critical requirement**, ensuring that warfighting systems remain secure, resilient, and operational in a future quantum-enabled threat environment.

What Does This Mean for Industry?

For the Defense Industrial Base (DIB), technology vendors, and contractors, the strategy signals **significant demand for quantum-resistant solutions** and deeper collaboration with the Department.

Key takeaways for vendors:

- Increased demand for PQC-enabled products aligned with NIST and NSA standards.
- Greater opportunities to provide commercial-off-the-shelf (COTS) solutions that can be integrated into defense systems.
- Preparation for upcoming federal acquisition and compliance requirements related to quantum-resistant cryptography.
- Expanded collaboration with DoW to accelerate testing, certification, and deployment of secure technologies.
- Increased focus on interoperability, scalability, and secure supply chains supporting defense missions.

For industry partners, the strategy reinforces a long-term shift toward **quantum-resilient cybersecurity** solutions, positioning PQC as a foundational requirement for future defense systems and technologies.

Timeline

Deadline	Provisions	Requirements
December 31, 2030	Initial PQC Transition	All DoW systems must support post-quantum cryptography (PQC) or be phased out if they cannot be updated.
December 31, 2030	Deprecation of Vulnerable Cryptography	All systems using quantum-vulnerable cryptographic algorithms or protocols must be removed or replaced.
December 31, 2031	Full PQC Implementation	All DoW systems must use PQC for all cryptographic functions unless otherwise noted.

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.