

The MIL Corporation

Post Quantum Cryptography (PQC)



Understanding How Quantum Affects National Security

Advancements in quantum computing is accelerating at a pace that poses a real national security challenge. These emerging technologies have the potential to break classical encryption, putting federal systems and long-lived critical infrastructure at risk. Organizations cannot afford to wait—quantum disruption is not a distant threat.

The MIL Corporation (MIL) positioned itself to help clients understand this rapidly evolving landscape and prepare strategically for the emerging quantum era.

Planning First: A Proactive, Data Driven Strategy

MIL emphasizes planning over reacting. We leverage detailed data analysis to prioritize your assets, reduce uncertainty, and guide decision-making. Our phased, proactive approach is designed to:

- » Reduce operational downtime and operational disruption
- » Strengthen security and readiness.
- » Provide data informed risk prioritization
- » Creates clear, actionable migration roadmaps
- » Provides modular, a la carte services, tailored to your needs (not expensive, bundled solutions)

Readiness as a Lifecycle

PQC readiness is not a one-time initiative—standards, threats, and technologies will continue to evolve. MIL provides continuous support through every phase of your journey, staying fully engaged through updates, maintenance, and long-term system evolution. Our lifecycle-based support includes:

- » Ongoing assessments
- » Maintenance, tuning, and system modernization
- » Continuous governance and PQC support
- » Workforce education and training

Compliance & Governance

PQC compliance mandates are already here. MIL ensures your organization understands and meets these evolving requirements with clarity and confidence:

- » **Executive Order 14028:** Requirements for secure cryptographic standards and transition planning
- » **NSA/CISA CNSA 2.0 guidance:** PQC planning starting in 2022; full adoption by 2030 for NSS systems
- » **NIST PQC standards (2024):** Five finalized algorithms

A La Carte Post Quantum Cryptography (PQC) Services

MIL's PQC capabilities are modular and scalable. You choose exactly what you need:

- » Cryptographic Bill of Materials (CBOM) creation
- » Cryptographic risk assessments and prioritization
- » Roadmap development and modernization planning
- » System hardening, mitigation, and algorithm upgrades
- » Implementation across network, application (COTS and custom), and platform layers
- » Red/Blue team crypto validation & integrity testing
- » Continuous governance & support
- » Education and workforce development

Partner Ecosystem

MIL acts as the integration and risk mitigation partner, supported by a robust ecosystem of PQC vendors. This ecosystem ensures your organization receives best of breed, scalable, compliant PQC solutions, such as:

- » PQC automation & CBOM generation tools
- » AI driven vulnerability scanning
- » Offensive testing capabilities
- » FedRAMP Moderate solutions with path to FedRAMP High
- » Hardware, PKI, cert, and cryptographic modernization partners

MIL's Expertise & Commitment

- » Decades of mission focused federal support
- » Deep cybersecurity and modernization expertise
- » Strong partner network for end-to-end PQC readiness
- » Commitment to guiding organizations through the entire lifecycle of quantum risk mitigation and transition

Contact us.

Yolanda Reid, Vice President | yolanda.reid@milcorp.com

