MODERNIZING ARMY CYBER DEFENSE for the Post-quantum Era

A Case Study on Advancing Quantum Readiness for the Army Endpoint Security Solution

THE CHALLENGE

Legacy Encryption Puts Army Systems at Risk

The Army Endpoint Security Solution (AESS) defends hundreds of thousands of U.S. Army and jJoint endpoints across the world. Its mission depends on secure communications, trusted identities, and resilient cyber operations.

As quantum computing advances, the encryption that protects these systems will eventually become vulnerable. The approach of "Q Day" and post-quantum cryptography (PQC) feels reminiscent of the Y2K problem, but unlike the known countdown in 1999, quantum risk emerges unpredictably. And, adversaries ranging from nation-states to individual threat actors are already collecting encrypted data for future quantum-powered decryption.

Federal mandates such as NSM-10 and the Quantum Computing Cybersecurity Preparedness Act established the urgency for post-quantum readiness. More recently, the Office of Management and Budget (OMB) Memorandum M-23-02 and Department of War (DoW) Chief Information Officer (CIO) guidance have translated that urgency into concrete inventory, assessment, and reporting requirements for national security systems. For AESS, meeting these requirements at scale posed an immediate challenge. Cryptography is woven into every endpoint, application, certificate store, and communication protocol. Much of it is inherited across tools and vendors. Until now, there has been no unified view of what cryptography existed on the enterprise, or how much of it was weak, misconfigured, or at risk.

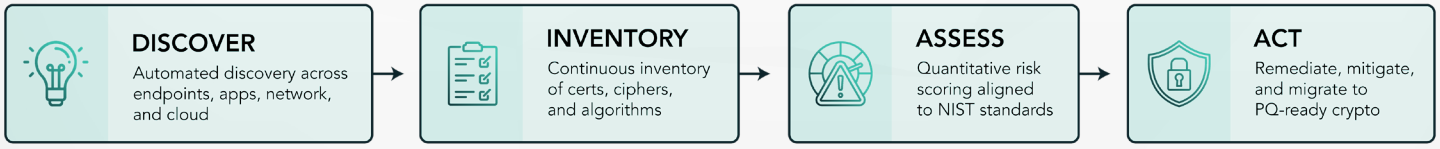
To achieve quantum readiness, AESS needed:

- **Full visibility** into its cryptographic footprint
- **A validated method for discovering risks** that threaten confidentiality, integrity, and availability
- **A scalable approach** to comply with quantum readiness mandates
- **Trusted partners** capable of operating at the speed and size of Army cyber operations

THE SOLUTION

A Phased Approach to Achieving Quantum Readiness

To overcome these challenges, AESS called on two longstanding partners: Everforth™ ECS®, who has delivered AESS as a fully managed platform-as-a-service (PaaS) for nearly a decade, and TYCHON, whose Automated Cryptographic Discovery and Inventory (ACDI) platform is already recognized by the U.S. Government as a leading solution for quantum readiness.



TYCHON performs automated discovery across endpoints, applications, network devices, and cloud environments, continuously monitoring certificates, keys, cipher suites, cryptographic libraries, transport layer security (TLS) configurations, and related dependencies. This creates a defensible cryptographic baseline and a cryptographic bill of materials (CBOM) aligned with the inventory requirements outlined in OMB M-23-02.

To help AESS achieve quantum readiness, Everforth ECS and TYCHON initiated a phased enterprise deployment, beginning with more than 180,000 endpoints (and to expand to all managed endpoints), that provided:

Key capabilities include:

- **Automated cryptographic discovery** of endpoints, applications, protocols and network devices both on-premise and in the cloud.
- **Automated cryptographic inventory** and continuous dynamic detection of algorithms, key lengths, certificates, libraries, ciphersuites and PQC and methods
- **Quantitative risk scoring and visualization** aligned to federal and National Institute of Standards and Technology (NIST) standards; drillable operator and executive dashboards organized by COAMS tags to support Army-wide visibility; and, actionable reporting on both classical and quantum-relevant weaknesses.
- **Remediation and mitigation** of todays cryptographic vulnerabilities and a programmatic approach to migrate to quantum resistant algorithms.

This approach gave AESS the ability to discover risks in near real time and manage quantum readiness as a continuous cybersecurity function. It also established a trusted operational picture to support zero trust, mission resiliency, and compliance requirements.

THE RESULTS

A Foundation for Modernized Army Cryptography

180,000+
endpoints inventoried in initial deployment

100M+
file certificates risk assessed

Within weeks, Army cyber leaders gained unprecedented visibility across a substantial portion of the AESS environment. The ACDI deployment revealed a significant population of weak ciphers, high-risk quantum-susceptible algorithms, and long-lived certificates. More than 100 million file certificates were analyzed and risk assessed. Analysis revealed that a significant portion of ciphers in use were weak, long-lived, or susceptible to future quantum decryption risk, including certificates configured with extraordinarily long validity periods — sometimes extending centuries into the future — making routine review or rotation unlikely without automation.

These insights enabled AESS to:

- **Strengthen** enterprise cyber hygiene
- **Prioritize** remediation across systems and enclaves
- **Improve** readiness for post-quantum cryptography
- **Advance** compliance with national mandates
- **Establish** a reusable framework that supports future modernization

This initial rollout established the foundation for continued expansion across the full AESS scope, including network devices and additional asset classes as the program matures.

LOOKING AHEAD

Ensuring Army Cyber Resilience in the Post-Quantum Era

As manufacturers begin releasing hardware and software that support quantum-resistant algorithms, AESS is positioned to adopt these technologies with confidence. Everforth ECS and TYCHON will continue supporting Army stakeholders with updated risk datasets, migration guidance, and ongoing discovery that strengthens the service's cybersecurity foundation. Future phases will extend the same automated discovery and inventory capabilities to additional asset classes, including network infrastructure, further strengthening Army-wide cryptographic visibility.

AESS now operates with a continuous, enterprise-scale capability to assess, prioritize, and reduce cryptographic risk as quantum threats evolve. With the right partners in place, readiness is no longer a distant goal. It is a capability delivered at enterprise scale and sustained as an ongoing cybersecurity function.