ZRA
zeichner risk analytics

COMET: CRYPTOGRAPHIC OBJECT MIGRATION EVALUATION TOOL

1. Requirements and Critical Decisions

National security experts warn that quantum computing will, within the next 10-20 years, threaten the cryptography that protects sensitive government information and national security systems, thus posing a significant national security threat to the United States. Between now and then, adversaries may be collecting encrypted data to decrypt later once quantum capabilities are available, making immediate action necessary to secure long-term sensitive information.

In response, the U.S. government has launched a comprehensive strategy to standardize post-quantum cryptography, migrate federal systems to these new standards, and require agencies to inventory and prioritize the protection of vulnerable assets. The National Institute of Standards and Technology has released the first set of post-quantum encryption algorithms, and federal agencies will soon receive specific guidance for adopting these standards, with similar changes expected to influence private sector and international practices.

Federal departments and agencies are required to meet post-quantum cryptography (PQC) migration mandates, including identifying high-value assets and creating cryptographic inventories, but the process is lengthy and complex, with the national PQC strategy still lacking clear objectives, milestones, and performance measures. Recent reports, such as the November 2024 GAO assessment, have highlighted gaps in the government's migration plans and emphasized the need for stronger managerial coordination and more detailed migration strategies.

To address these challenges, ZRA is introducing COMET®, which provides a structured roadmap for agencies to define priorities, set milestones, and align migration strategies with organizational needs through collective leadership. COMET® directs critical resources and activities to provide agencies with tailored deliverables such as leadership facilitation sessions, migration roadmaps, and comprehensive cryptographic inventories. COMET® ensures that agencies meet Congressional and Administration requirements, but also prepare for advancements in quantum computing through decisions and investments that protect their most critical information and assets.

2. Discovery and Assessment

COMET® offers a structured approach for USG entities to guide post-quantum cryptography (PQC) migration, starting with a discovery phase to inform migration posture and progressing through integrated assessments of business processes, threats, and risks.

COMET® maps core business functions by interviewing key personnel, analyzing quantum-specific threat actors and vectors, and integrating these insights to identify high-value assets (HVAs), critical business processes, and major vulnerabilities.

Risk analysis then evaluates the probability and impact of quantum attacks, helping organizations visualize and prioritize areas most in need of migration; COMET® draws on scenarios, and where data is available, the risk posture and probabilities inherent in different use cases.

Based on the risk assessment, COMET® facilitates initial migration decisions to align PQC adoption with organizational priorities, resource allocation, and federal standards.

3. Tools Deployment & IT Asset Discovery

COMET® draws on IT tools to target the most critical IT assets and applications. A range of open source and proprietary tools discover (and validate) IT tools used to fulfill the organization's most consequential business functions. In some cases, organizations have already targeted High Value Assets, critical business processes, or other critical IT assets; in other cases, organizations rely on risk analysis– such as the assessments performed through COMET.®

COMET® will direct an organization to compare their critical functions with their sizable IT asset inventory. Not all IT assets will need to migrate toward post-quantum encryption. Such a strategy would be exorbitantly expensive and result in significant operational impediments. As a result,COMET® is designed to provide a clear set of options based on strategic priorities – ranging from critical business needs to compliance, audit concerns, or other operational needs.

4. Cryptographic Inventory Development

COMET® will enable USG entities to create and maintain a prioritized cryptographic inventory to identify systems vulnerable to quantum attacks and guide the migration to post-quantum cryptography.

Developing this inventory is challenging due to the vast scale, complexity, and dynamic nature of modern IT environments, which include numerous endpoints, cloud services, IoT devices, and legacy applications with diverse and often hidden cryptographic dependencies.

Manual inventory methods are insufficient, so agencies must use automated tools and continuous monitoring to capture real-time changes and ensure comprehensive coverage, especially as cryptographic configurations evolve with software updates and network changes.

A complete inventory must detail all cryptographic assets (software and hardware), the nature and usage of algorithms, data assets with risk assessments, and external dependencies, including supply chain and shadow IT, to support effective risk management and quantum-resistant migration.

5. PQC Readiness and Gap Analysis

To prepare for post-quantum cryptography (PQC) migration, organizations must conduct a thorough readiness assessment and gap analysis, identifying vulnerabilities, dependencies, and resource needs that could impede adoption.

A COMET® readiness assessment involves reviewing findings from the cryptographic inventory and mapping cryptographic assets to PQC standards to identify vulnerable components.

The gap analysis will evaluate the organization in skills, resources, and risk exposure, prioritizing identified gaps to inform migration planning.

6. Migration Roadmap

From the prioritized cryptographic inventory,COMET® will guide entities in layering significant encryption decisions - informing a comprehensive migration roadmap.

COMET® ensures that entities establish security objectives and prioritize migration actions from the cryptographic inventory and risk analysis findings.

Once these objectives and actions are identified, COMET® will guide organizations through the process of evaluating and selecting PQC solutions.

As migration to PQC standards is a costly and time-consuming process, organizations will need to define appropriate resource allocation for performing and managing encryption.

7. Migration Support and Execution

Following roadmap development, COMET® supports organizations in executing migration through phased deployment, integrating hybrid cryptographic solutions to maintain continuity during transitions.

Rigorous testing and validation will ensure PQC implementations meet security and performance requirements, with fallback mechanisms in place to address unforeseen operational disruptions.

COMET® provides active migration support including support with system upgrades, troubleshooting integration challenges, and coordination with cryptographic vendors.

Continuous monitoring of deployed solutions, coupled with adaptive resource allocation, will enable organizations to refine their approach as PQC standards evolve or new quantum threats emerge.