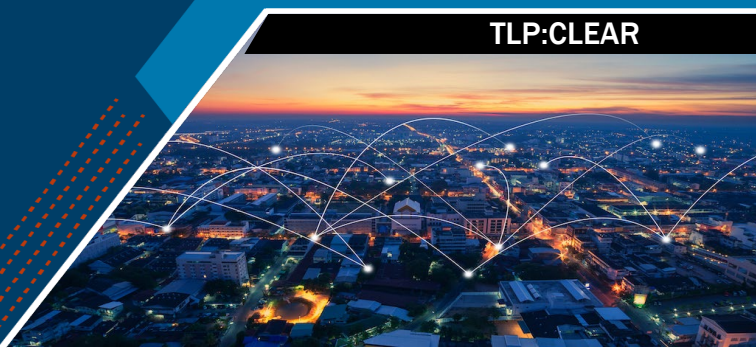
QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY



BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) created this factsheet to inform organizations — especially those that support Critical Infrastructure — about the impacts of quantum capabilities, and to encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap. NIST is working to publish the first set of post-quantum cryptographic (PQC) standards, to be released in 2024, to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today.

WHY PREPARE NOW?

A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors. Early planning is necessary as cyber threat actors could be targeting data today that would still require protection in the future (or in other words, has a long secrecy lifetime), using a catch now, break later or harvest now, decrypt later operation. Many of the cryptographic products, protocols, and services used today that rely on public key algorithms (e.g., Rivest-Shamir-Adleman [RSA], Elliptic Curve Diffie-Hellman [ECDH], and Elliptic Curve Digital Signature Algorithm [ECDSA]) will need to be updated, replaced, or significantly altered to employ quantum-resistant PQC algorithms, to protect against this future threat. Organizations are encouraged to proactively prepare for future migration to products implementing the post-quantum cryptographic standards. This includes engaging with vendors around their quantum-readiness roadmap and actively implementing thoughtful, deliberate measures within their organizations to reduce the risks posed by a CRQC.

ESTABLISH A QUANTUM-READINESS ROADMAP

While the PQC standards are currently in development, the authoring agencies encourage organizations to create a quantum-readiness roadmap by first establishing a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that identify the organization's current reliance on quantum-vulnerable cryptography. Systems and assets with quantum-vulnerable cryptography include those involved in creating and validating digital signatures, which also incorporates software and firmware updates. Having an inventory of quantum-vulnerable systems and assets enables an organization to begin the quantum risk assessment processes, demonstrating the prioritization of migration. Lead by an organization's Information Technology (IT) and Operational Technology (OT) procurement experts, the inventory should include engagements with supply chain vendors to identify technologies that need to migrate from quantum-vulnerable cryptography to PQC.

Organizations are often unaware of the breadth of application and functional dependencies on public-key cryptography that exist within the products, applications, and services widely deployed within their operational environments, leading to a lack of visibility. The project team should lead the creation of such an inventory. The team should also include the organization's cybersecurity and privacy risk managers who can prioritize the assets that would be most impacted by a CRQC, and that would expose the organization to greater risk.

PREPARE A CRYPTOGRAPHIC INVENTORY

- Having an inventory of quantum-vulnerable technology and associated criticality of the data enables an organization to begin planning for risk assessment processes to prioritize its migration to PQC. This cryptographic inventory will:
  - Help an organization become quantum-ready — a state where a CRQC is not a threat,
  - Help an organization prepare a transition to zero trust architecture,
  - Help identify or correlate outside access to datasets, as those are more exposed and at higher risk, and
  - Inform future analysis by identifying what data may be targeted now and decrypted when a CRQC is available.
- Organizations should create a cryptographic inventory that offers visibility into how the organization leverages cryptography in its IT and OT systems. Cryptographic discovery tools should be used to identify quantum-vulnerable algorithms in:
  - Network protocols, used to identify quantum-vulnerable algorithms in network protocols that allow traceability
  - Assets on end user systems and servers, including applications and associated libraries, both within application functionality and for firmware and software updates, and
  - Cryptographic code or dependencies in the continuous integration/continuous delivery development pipeline.

    Note: Discovery tools may not be able to identify embedded cryptography used internally within products, hindering discoverability or documentation. Organizations should ask vendors for lists of embedded cryptography within their products.
- Organizations should include in their inventory when and where quantum-vulnerable cryptography is being leveraged to protect the most sensitive and critical datasets and include estimates on length of protection for these datasets. Organizations should:
  - Correlate cryptographic inventory with inventories available from existing programs, such as Asset Inventory, Identity, Credential, and Access Management, (ICAM), Identity & Access Management (IdAM), Endpoint Detection and Response (EDR), and Continuous Diagnostics and Mitigation (CDM),
  - Understand which systems and protocols are being used to move or access their most sensitive and critical datasets, and
  - Identify quantum-vulnerable cryptography that protects critical processes, especially for Critical Infrastructure.
- Organizations should feed the quantum-vulnerable inventory into their risk assessment process, allowing risk officials to prioritize where to ensure use of PQC as soon as it is available.

DISCUSS POST-QUANTUM ROADMAPS WITH TECHNOLOGY VENDORS

CISA and the authoring agencies encourage organizations to start engaging with their technology vendors to learn about vendors' quantum-readiness roadmaps, including migration. Solidly built roadmaps should describe how vendors plan to migrate to PQC, charting timelines for testing PQC algorithms and integration into products. This applies to both on-premises commercial-off-the-shelf (COTS) and cloud-based products. Ideally, vendors will publish their own PQC roadmap, framing their commitment to implementing post-quantum cryptography. The authoring agencies also urge organizations to proactively plan for necessary changes to existing and future contracts. Considerations should be in place ensuring that new products will be delivered with PQC built-in, and older products will be upgraded with PQC to meet transition timelines.

SUPPLY CHAIN QUANTUM-READINESS

Organizations should develop an understanding of their reliance/dependencies on quantum-vulnerable cryptography in systems and assets, as well as how the vendors in their supply chain will be migrating to PQC. As noted above, understanding your organization's dependencies on quantum-vulnerable cryptography involves discovering where quantum-vulnerable algorithms are used in current IT and OT systems and devices (custom-built or COTS) and in the organization's reliance on cloud services, ensuring that plans will reduce as much quantum risk as feasible and meet the organization's transition strategy.

Organizations should also begin to ask their vendors how they are addressing quantum-readiness and supporting migration to PQC. Additional considerations:

- Prioritization should be given to high impact systems, industrial control systems (ICSs), and systems with long-term confidentiality/secrecy needs.
- If an organization discovers quantum-vulnerable cryptography in its custom-built technologies, it should identify the risk to data or functions that rely on those technologies. The organization could either migrate to PQC within those technologies or develop system security upgrades that mitigate the risk of their continued use. Custom-built products, especially those in older systems, will likely require the most effort to make quantum-resistant.
- For COTS products, engagement with vendors on their PQC roadmap is critical. Migration to PQC should be viewed as an IT/OT modernization effort. An organization's quantum-readiness roadmap should include details of when and how each COTS vendor plans to deliver updates or upgrades to enable the use of PQC, as well as the expected cost associated with migration to PQC.
- For cloud-hosted products, organizations should engage with their cloud service providers to understand the provider's quantum-readiness roadmap. Once PQC standards are available, engagements should evolve to focus on how to enable the use of PQC, for example through configuration changes or application updates.

TECHNOLOGY VENDOR RESPONSIBILITIES

Technology manufacturers and vendors whose products support the use of quantum-vulnerable cryptography should begin planning and testing for integration. CISA, NSA, and NIST encourage vendors to review the NIST-published draft PQC standards, which contain algorithms, with the understanding that final implementation specifics for these algorithms are incomplete. Ensuring that products use post-quantum cryptographic algorithms is emblematic of Secure by Design principles. Vendors should prepare themselves to support PQC as soon as possible after NIST finalizes its standards.