NIST post-quantum cryptography standards: Key questions and actions for implementation

Organizations will now have what they need to start encrypting their information systems for post-quantum-based attacks. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) finalized its proposed principal set of encryption algorithms, issuing the first US standards for post-quantum cryptography.

The practice of cryptography is critical for safeguarding sensitive data and communication between information systems, and these new standards reflect the latest evolution in the field. Encryption enables data in transit or at rest to be essentially "locked" by complex mathematical equations only to be unlocked by a solution "key." This concept is known as public-key cryptology, whereby a public key is paired with a private key to create a complete cryptologic function. Effective encryption algorithms can reduce the risk of malicious actors gaining unauthorized access to underlying data.

Complex algorithms can be solved with enough computational horsepower. However, current computer models lack the computing power necessary to overcome the most prevalent cryptologic standards in a timely manner. With the rise of quantum computing, that's no longer the case.

Quantum computation leverages quantum mechanics – a revolutionary approach. The encryption in use today to guard everything from their emails to private information may soon be vulnerable to malicious actors who gain quantum computing capabilities.

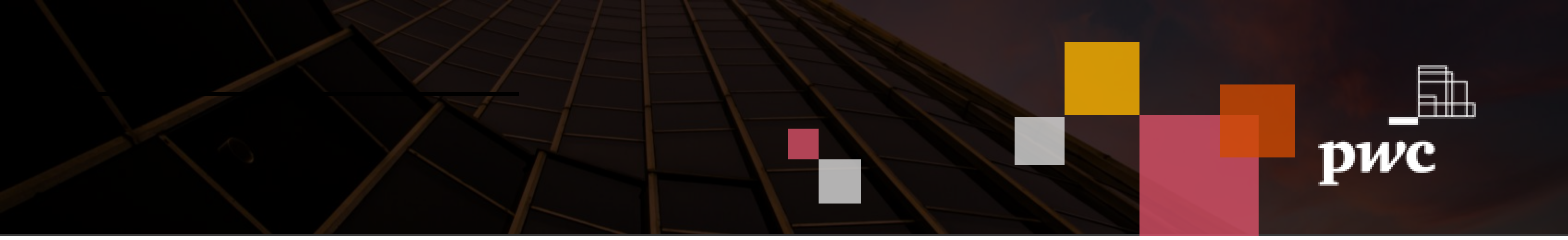
The proposed NIST standards help address that concern and are aimed at helping government and organizations prepare for a post-quantum computing era.

NIST encryption standards at a glance

This month, NIST released **three post-quantum cryptography (PQC) standards** to strengthen modern public-key cryptography infrastructure for the quantum era.

- ML-KEM (derived from CRYSTALS-Kyber) is a **key encapsulation mechanism** selected for general encryption, such as accessing secured websites.
- ML-DSA (derived from CRYSTALS-Dilithium) is a **lattice-based algorithm** for general-purpose digital signature protocols.
- SLH-DSA (derived from SPHINCS+) is a **stateless hash-based** digital signature scheme.

Along with the encryption algorithms' code, the standards released by NIST include instructions on how to implement them into products and encryption systems, and their intended uses.



The path to implementation

With the release of the standards, NIST is encouraging companies to begin implementation. As NIST explained in its official announcement, integrating these algorithms into systems should happen now because full integration and the process of implementation is going to take time. On top of that, threat actors are already moving to gain computing capabilities to expose secrets and vulnerabilities across systems.

In response, many companies have started down the path of implementation by preparing for these standards and can now move ahead with confidence to better safeguard their organizations.

Questions to consider as you plan for implementation:

1. **Are we protecting our data for "harvest now, decrypt later" attacks?**

   Cryptographic processes and migrations can take years to complete. In the meantime, threat actors are getting a head start by stealing data and storing it until they can use a quantum computer to decrypt and gain access. Current data protection practices and risk controls need to account for post-quantum cryptography, and security leaders need to transition to the new NIST standards for the most critical resources.

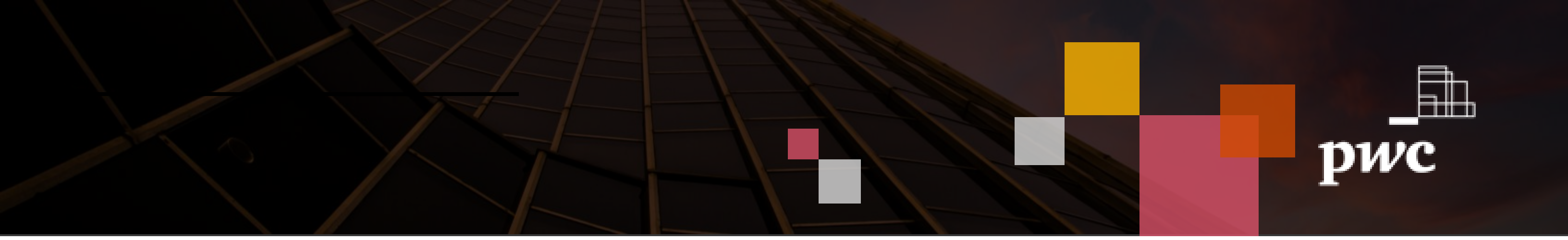
2. **Have we considered our third-party relationships and the impacts on post-quantum cryptography?**

   Even with these new encryption algorithms being available, organizations will need to understand all their data and system dependencies, and that includes outside the organization. The process for aligning with third-party vendors is an essential step to overcome blind spots and requires an understanding of what data a third party holds on to, its data life-cycle management process, its current cryptologic standards and its plans for PQC, and any plans to update its service-level agreements.

3. **Are we prepared to meet regulatory requirements?**

   The expectation is that regulators will start to ask how organizations are approaching NIST encryption standards as part of their post-quantum security protocols and practices. Along with NIST, CISA and ISO/IEC have already started to account for stronger cryptography standards. And for organizations that work with federal agencies, securing cryptography against current and future quantum threats is essential.

   With NIST laying out its standards for encrypting sensitive information in anticipation of quantum-led attacks, organizations should have the tools they need to either get started or update their quantum transformation plans immediately.



Actions to take:

1. **Conduct an inventory of your most critical data for immediate and later-stage attacks**

   Identify your most sensitive and critical data and prioritize for migration to the new NIST standards. Assess the risk of your critical data being targets for “stored now, decrypted later” attacks and consider integrating more robust storage methods, security controls and risk controls.

2. **Assess which systems depend on cryptography and prioritize PQC integration**

   Initiate a cryptologic discovery effort to inventory all systems handling data at rest and in transit. Develop processes to keep an up-to-date system of record for cryptologic infrastructure in the organization and create a transformation plan aligned to the new NIST standards.

3. **Identify those systems that are not able to handle PQC algorithms and plan for quantum-resistant alternatives**

   Determine where and why you’re using public cryptography that can’t transition to the new standards and mark those systems as quantum vulnerable. Develop a plan to risk-accept or begin a timeline to move data to a NIST-compliant storage solution, in line with your organization’s risk appetite and policies.

Bottom line

Quantum computing may be here sooner than some organizations might be anticipating. Companies that are already factoring in post-quantum security practices as part of their overarching cybersecurity strategy are well-positioned to meet the challenges head on.

Contact us

Matt Gorham
Cyber & Privacy Innovation Institute Leader, PwC
matt.gorham@pwc.com

Shawn Lonergan, Ph.D.
Partner, Technology & Operational Resilience, Cyber, Risk & Regulatory, PwC
shawn.lonergan@pwc.com

Amol Chaudhari
Director, Cyber, Risk & Regulatory, PwC
amol.chaudhari@pwc.com