


# Best Practices for Implementing Quantum-Resistant Security

Gina Scinta
Deputy CTO

Thales Trusted Cyber Technologies

# Thales Trusted Cyber Technologies: Who We Are

## Trusted, U.S. Provider of Cybersecurity Solutions Dedicated to the U.S. Federal Government

**U.S. Support | Cleared Employees | U.S. Manufacturing**

We protect the government's most vital data from the core to the cloud to the edge

We provide unified data protection solutions for:

Encryption

Key Management

Access Control Requirements


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Topics

01

## The Quantum Security Challenge

02

## Quantum Transition Strategy

03

## Industry PQC Activities

04

## Summary


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES **© 2024 THALES. All rights reserved.**

# The Quantum Security Challenge




This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES **© 2024 THALES. All rights reserved.**

# Background and Policy



## Quantum computers will efficiently crack PKI

Without quantum-resistant encryption, ***everything*** that has been transmitted, or will ever be transmitted over a network, ***will be vulnerable*** to eavesdropping and public disclosure



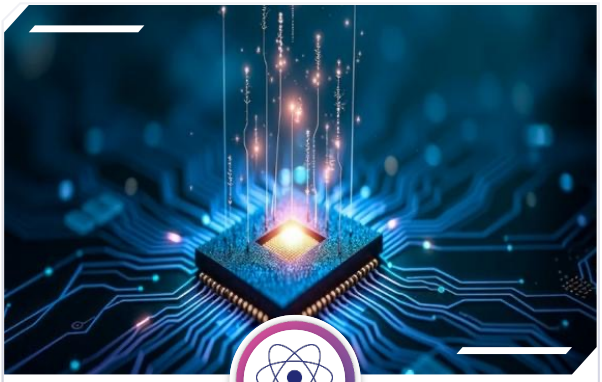
## Harvest Now, Decrypt Later

Intercept classified comms

Expose government secrets

Perform corporate espionage

Access personal information



## Post-Quantum Cryptography (PQC) will maintain our "way of life"

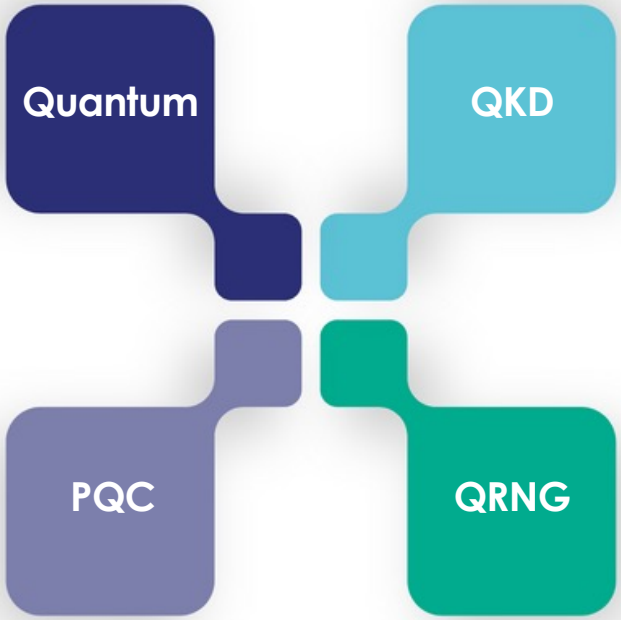
Crypto agile products allow us to use PQC algorithms and keys today


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES **© 2024 THALES. All rights reserved.**

# “Which” Quantum?

## Quantum Computing

Computer that seeks to exploit the properties of quantum mechanics to speed up computing




## Quantum Key Distribution

Use of quantum physics to distribute keys

## Post-Quantum Cryptography (PQC)

Cryptographic systems that are secure against both quantum and classical computers (aka Quantum Resistant Algorithms (QRA))

## Quantum Random Number Generation

Hardware random number generators used to generate nondeterministic randomness



Thales Trusted Cyber Technologies
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.



# Long Lifetime Data Confidentiality Requirements

**Expiration date**

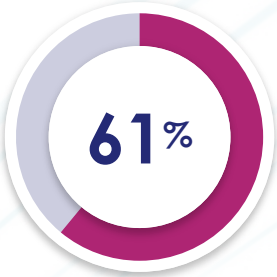
- Hours – temporary credentials
- Months – corporate earnings
- Years – banking information, credit cards
- Decades – trade secrets, classified information
- Lifetime – DNA data, personal information


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

KEY FINDINGS

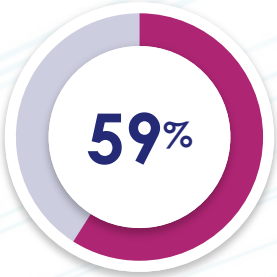
# Future risks are here today

## Quantum concerns shift to the reality of harvest now, decrypt later (HNDL)




Cited as the top concern.

## Organizations are moving to mitigate quantum risk

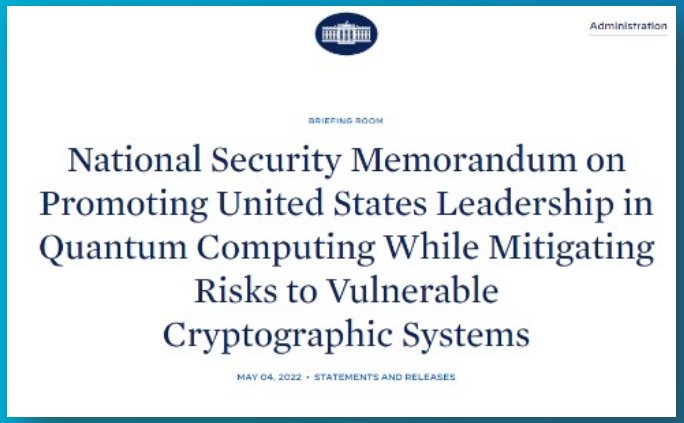



Are prototyping and evaluating Post-Quantum Cryptographic (PQC) algorithms.

# White House National Security Memo 10, dated May 4, 2022

"America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow."

"Central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards."


Administration

BRIEFING ROOM

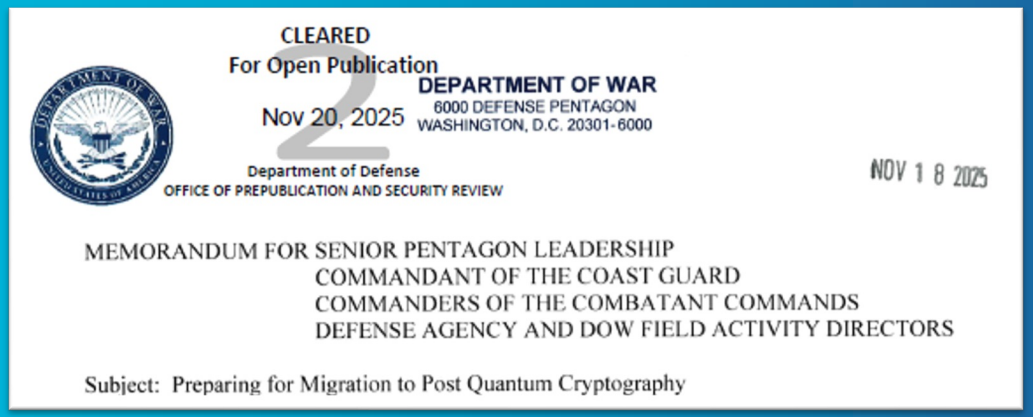
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

# Department of War Memo, dated November 20, 2025
# Preparing for Migration to Post Quantum Cryptography

"…imperative to identify and inventory any type of cryptography used in all DoW information systems including, … national security systems (NSS), non-NSS, business systems, weapons systems, cloud computing systems, and operational technology, regardless of classification, location, connection, type, purpose or use."

[DoW PQC "engagements"] "must submit relevant artifacts … to my office immediately. My office will review the artifacts and determine if there are risks, unmitigated security considerations, or use restrictions that need to be addressed prior to acquisition or PQC engagement."



CLEARED
For Open Publication
Nov 20, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DEPARTMENT OF WAR
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NOV 18 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

Subject: Preparing for Migration to Post Quantum Cryptography


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# GSA Post Quantum Cryptography Buyer's Guide, dated June 2025

**The Post-Quantum Cryptography (PQC) Buyer's Guide for federal agencies is a resource designed to assist agencies in their efforts to prepare systems to protect sensitive data from potential attacks by future quantum computers.**

**PQC Use Case: Quantum PQC and Zero Trust Architecture (ZTA)**

Implementation of both ZTA and PQC requires ***trusted identity, access and encryption using continuous monitoring.***

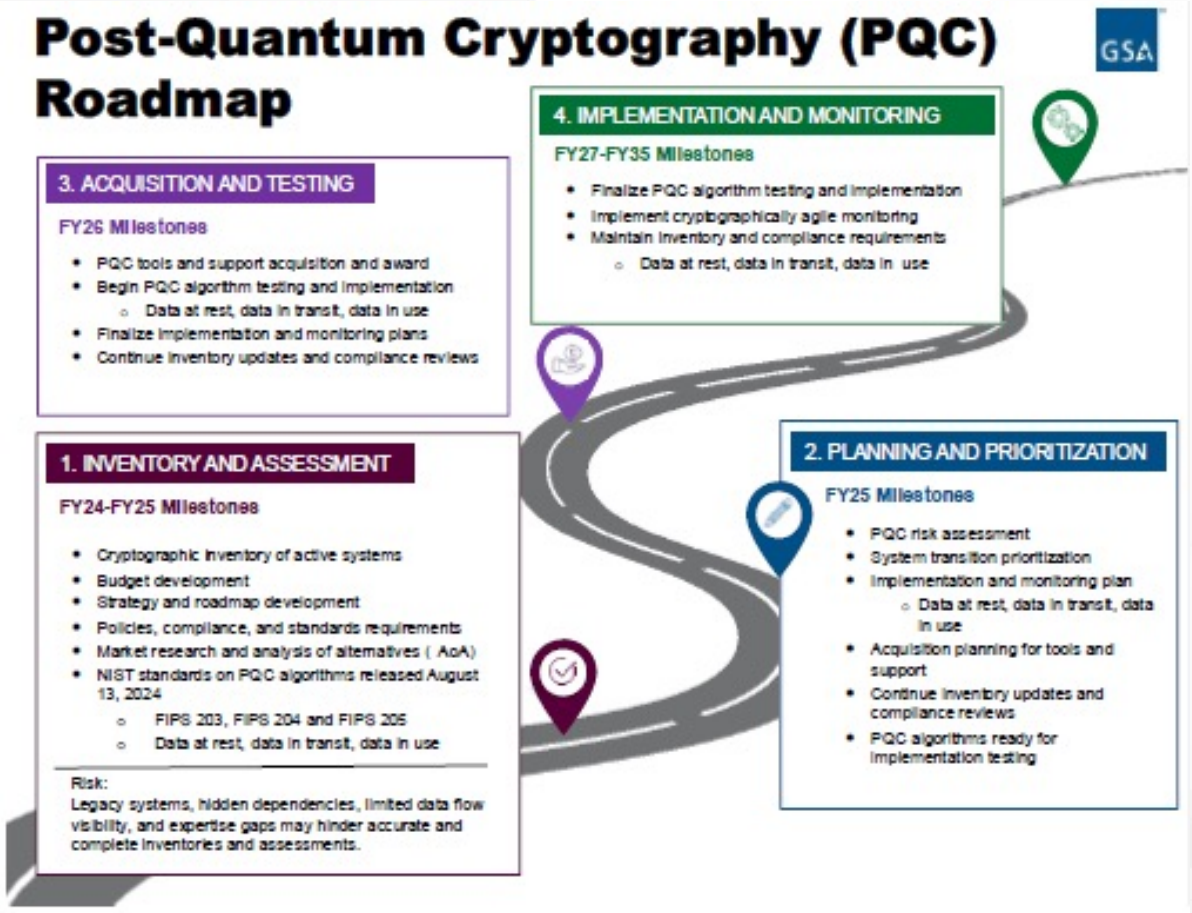
Cryptography, including PQC algorithms, offer a foundation for ZTA, and building systems with ***crypto agility*** in mind are designed to incorporate new protocols without requiring significant change to system infrastructure.





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# GSA PQC Buyer's Guide Roadmap






Thales Trusted Cyber Technologies
nent may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All ri

THALES

# National Cybersecurity Strategy, dated March 6, 2026

**The National Cybersecurity Strategy outlines priorities for ensuring that America remains unrivaled in cyberspace**

Accelerate modernization, defensibility, and resilience of federal information systems by ***implementing cybersecurity best practices, post-quantum cryptography, zero-trust architecture and cloud transition***.

Adopt AI-powered cybersecurity solutions to defend networks and deter intrusions at scale.





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Executive Order 14412: Securing The Nation Against Advanced Cryptographic Attacks, dated June 22, 2026

"The advent of large-scale quantum computers…will pose a significant threat to widely used cryptographic security systems…the United States must take steps to strengthen cryptographic protections for the Nation's sensitive data, critical infrastructure, and digital economy"

"It is the policy of the United States to safeguard national security and maintain technological leadership by responsibly and effectively executing the transition of Federal information systems to NIST-approved FIPS for PQC…"





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

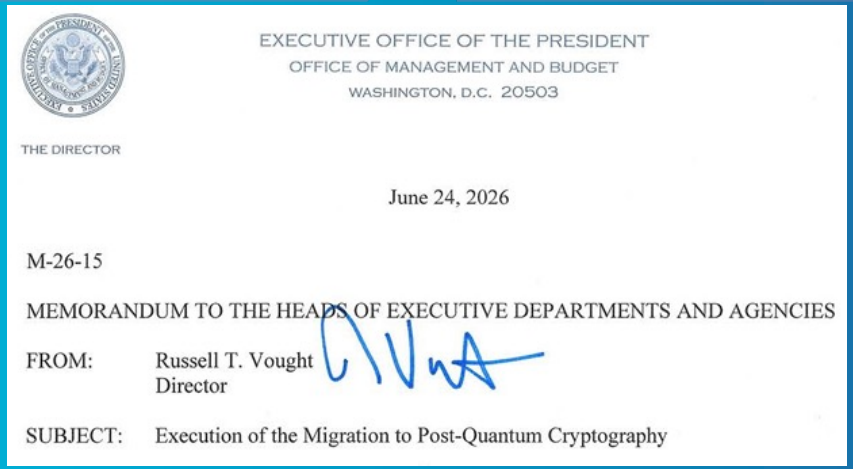
# M-26-15: Execution of the Migration to Post-Quantum Cryptography, dated June 24, 2026

**Memorandum implements the accelerated migration for Federal Government systems to post quantum cryptography as described in EO 14412.**

**It fulfills the OMB's responsibility to issue guidance directing each agency to prioritize critical information technology and develop a PQC migration plan.**

**Within 120 days of this memo, agencies must develop and submit action plan to OMB, and ONCD with a multi-year phased approach to migration.**

**Align plans with NIST Internal Report (IR) 8547, Transition to Post-Quantum Cryptography Standards**



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 24, 2026

M-26-15

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Execution of the Migration to Post-Quantum Cryptography


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Executive Order 14413: Ushering in the Next Frontier of Quantum Innovation, dated June 22, 2026

**Establishes a coordinated national effort to accelerate US leadership in quantum information science and technology (QIST), focusing on quantum computing, sensing, networking, commercialization, and workforce development.**

**Key Objectives:**

- **National Quantum Strategy Update**
- **Quantum Computer for Application Development & Discovery Science (QC-ADDS)**
- **Commercialization & Industry Engagement**
- **Workforce Development**
- **National Security & Counterintelligence**
- **International Collaboration**





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2025 THALES. All rights reserved.

# Industry PQC Challenge Summary



## Education

- End users
- Decision makers



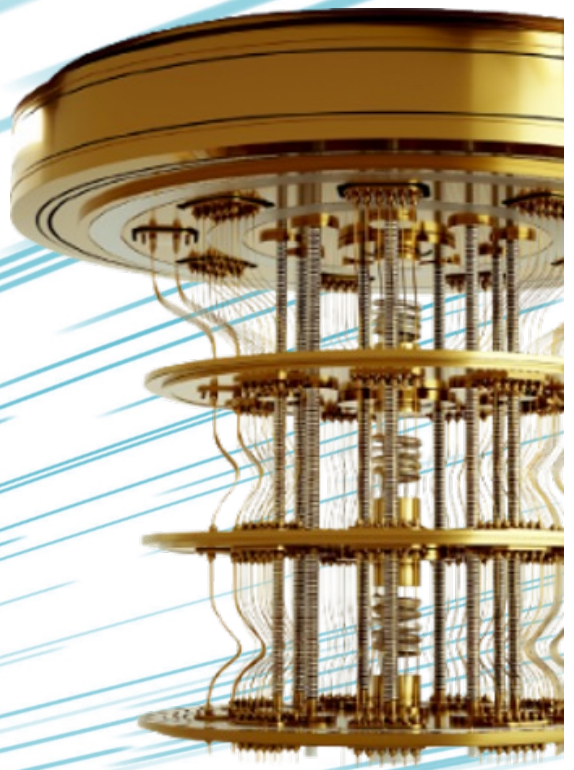
## Standards Maturity

- Algorithms
- Protocols



## Ecosystem Interoperability

- Complementary technology
- Broader ecosystem




This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Quantum Transition Strategy




This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES **© 2024 THALES. All rights reserved.**

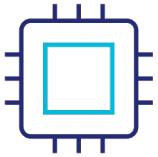
# CISA, NSA and NIST Post-Quantum Cryptography Timeline

## Dated October 2021



**2021-2023**

Inventory and prioritize systems



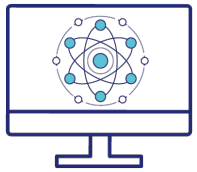
**2024**

NIST post-quantum cryptography standard published



**2024-2030**

Transition of systems to NIST post-quantum cryptography standard



**2030**

Cryptographically relevant quantum computer potentially available


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# EO 14412: Section 4. Accelerating the PQC Transition



**30 Days**

Each Agency to Identify **PQC Migration Lead**

**90 Days**

OMB, CISA & National Cyber Director **issue guidance** requiring each agency to:

Review **inventory** of HVAs and high impact systems, excluding NSS

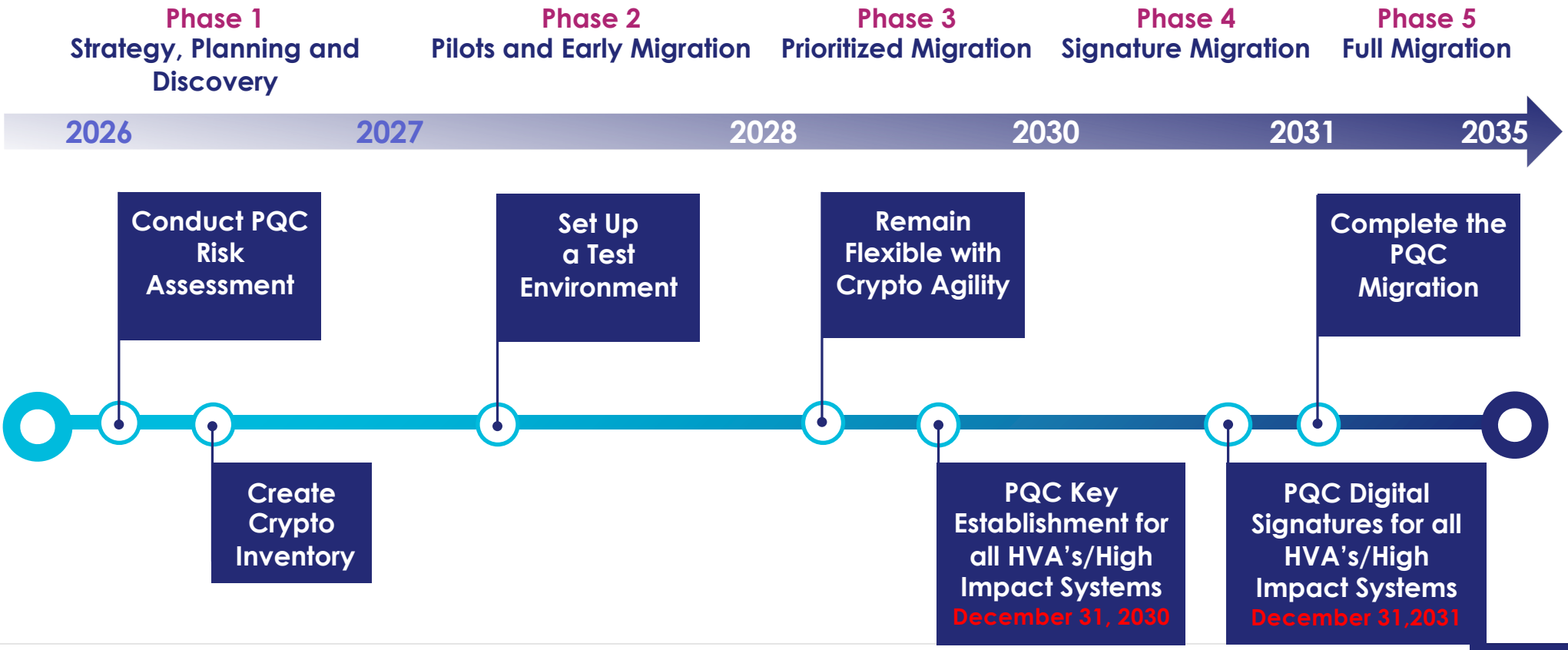
Transition all HVAs and high impact systems to use PQC for:
**Key establishment by December 31, 2030**

**Digital Signatures by December 31, 2031**

**Develop/submit a plan** to accomplish this directive


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# M-26-15: OMB PQC Migration Plan






Thales Trusted Cyber Technologies
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Commercial National Security Algorithm (CNSA) Suite 2.0

## > NSA Cybersecurity Advisory

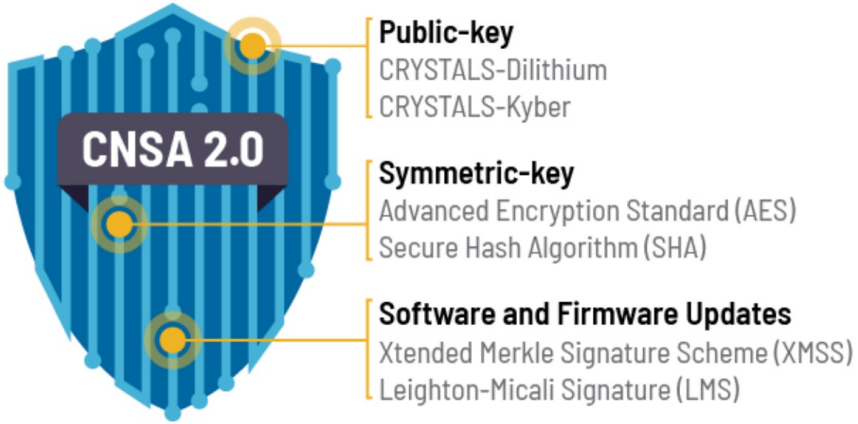
- Released: September 7, 2022
- FAQ v2.0: April 2024
- FAQ v2.1: December 2024

## > PQC requirements for National Security Systems

## > Symmetric-key (minor change)

## > Public-key

- Key establishment: ML-KEM (CRYSTALS-Kyber) Level V
- Digital signatures: ML-DSA (CRYSTALS-Dilithium) Level V

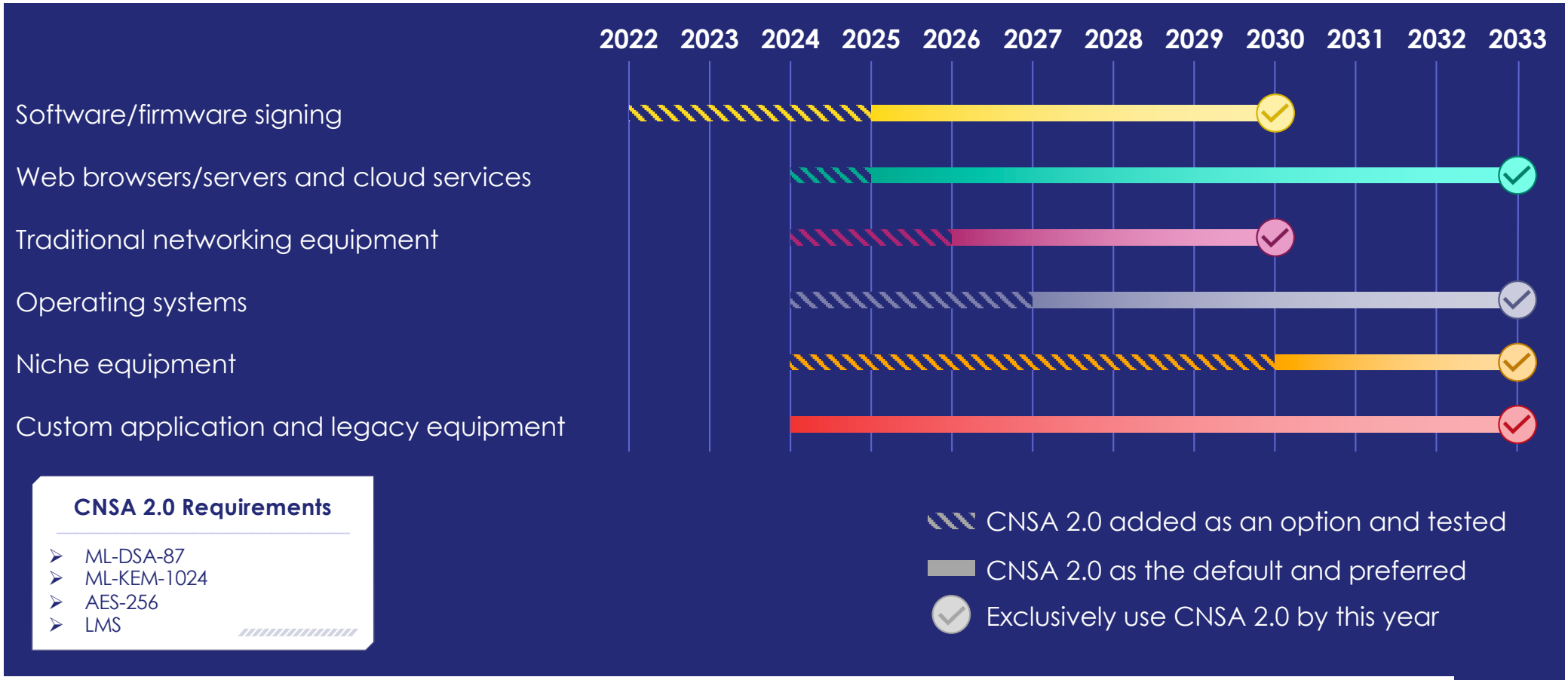



## > Software and firmware signing

- Recommends Hash Based Signatures per SP 800-208 using LMS SHA 256/192
  - Must manage state and sign in hardware
- Allows ML-DSA (per FAQ April 2024 v2)


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# CNSA 2.0 Timeline




**CNSA 2.0 Requirements**

- ML-DSA-87
- ML-KEM-1024
- AES-256
- LMS


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# NIST Transition to Post-Quantum Cryptography Standards
## NIST IR 8547 (Initial Public Draft) November 2024




### Cryptography Standards

- NIST has released the initial public draft of IR 8547, detailing the strategy for transitioning from quantum-vulnerable cryptographic algorithms to post-quantum cryptography.
- Effectively, think about depreciating RSA by 2028. Get your PQC solutions ready now!

| Digital Signature Algorithm Family | Parameters | Transition |
|---|---|---|
| **ECDSA** [FIPS186] | 112 bits of security strength | ***Deprecated*** after 2030<br>***Disallowed*** after 2035 |
| | ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **EdDSA** [FIPS186] | ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **RSA** [FIPS186] | 112 bits of security strength | ***Deprecated*** after 2030<br>***Disallowed*** after 2035 |
| | ≥ 128 bits of security strength | ***Disallowed*** after 2035 |


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Best Defense is Crypto Agility

**Crypto agility** means:

- The ability to quickly modify underlying crypto primitives
- Flexible upgradeable technology
- No built-in obsolescence

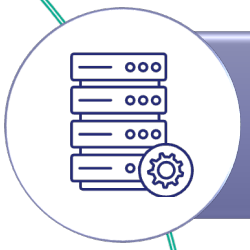




This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

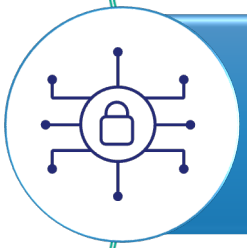
# NIST Considerations for Achieving Crypto Agility

## Cybersecurity White Paper (CSWP) 39, dated December 19, 2025



### Crypto Agility for a Computing System

- *Cryptographic algorithms implemented in software, hardware, firmware, and infrastructures to facilitate their use in applications.*



### Crypto Agility for a Communication Protocol

- Parties must agree on a common cipher suite
- A common set of cryptographic algorithms used for key establishment, signature generation, hash function computation, encryption, and/or data authentication.



### Crypto Agility for an Enterprise IT Architect

- Achieving crypto agility is also a task for information technology (IT) and cybersecurity architects, software and standards developers, hardware designers, and executives

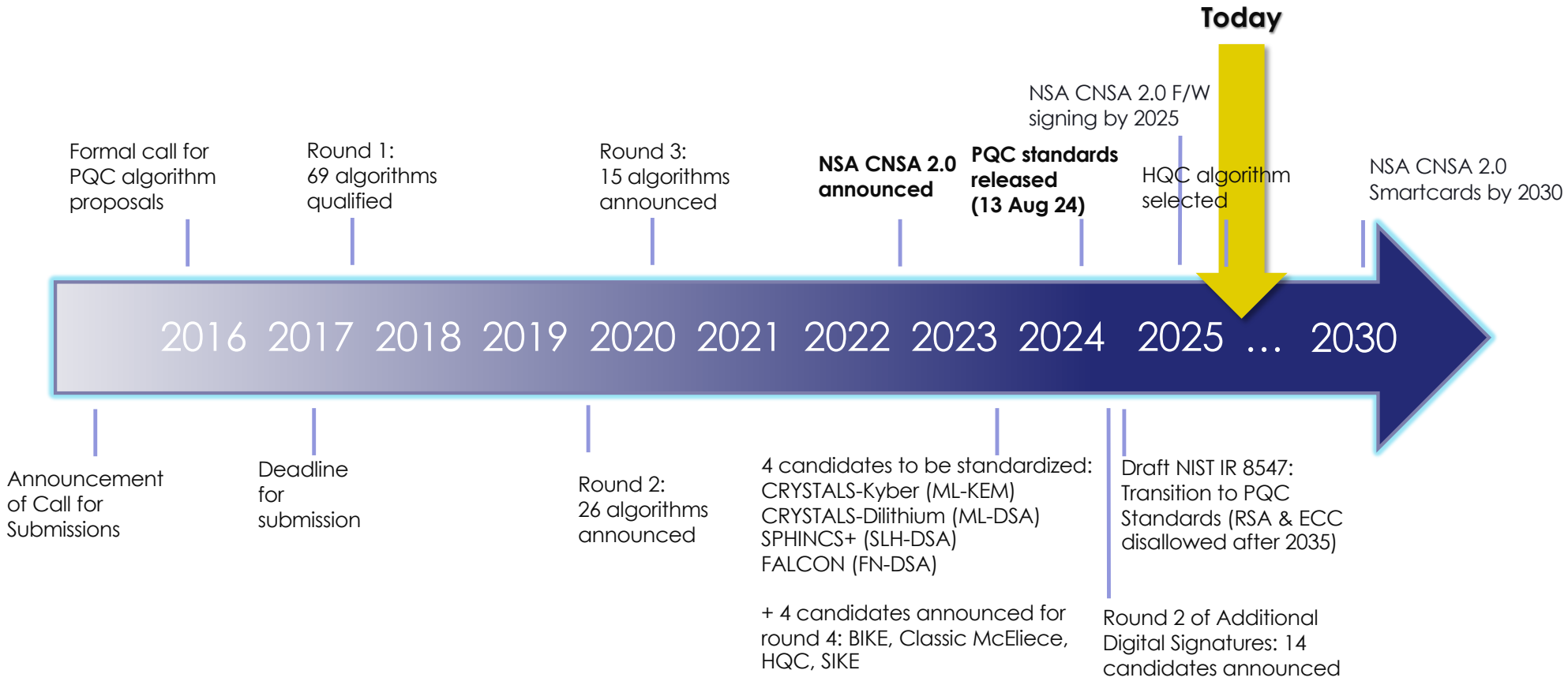
# Industry PQC Activities





Thales Trusted Cyber Technologies
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES **© 2024 THALES. All rights reserved.**

# The NIST Standardization Process





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# NIST Released First Three Post-Quantum Encryption Standards

## Start Getting Used to Names

**NIST Released August 13, 2024**

### ML-KEM

- Formerly CRYSTALS-KYBER
- FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism

### ML-DSA

- Formerly CRYSTALS-Dilithium
- FIPS 204 Module-Lattice-Based Digital Signature Standard

### SLH-DSA

- Formerly SPHINCS+
- FIPS 205 Stateless Hash-Based Digital Signature Standard

### FN-DSA

- Formerly FALCON
- Designed for digital signatures
- Draft FIPS under development

### HQC

- Serves as backup for ML-KEM
- NIST plans to issue draft standard 2026
- Final standard expected 2027

**Standardization Forthcoming**


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# NIST Down Selected Digital Signatures Candidate Algorithms

**NIST has down selected candidates for third round of Additional Digital Signatures for NIST PQC Standardization Process**

- **Third-round candidates have the option of submitting updated specifications and implementations (i.e., tweaks)**
- **Third phase of evaluation and review estimated to last approximately 2 years**
- **Advancing digital signature algorithms are:**
  - FAEST
  - MAYO
  - MQOM
  - QR-UOV
  - SDitH
  - SNOVA
  - SQIsign
  - UOV
- **On July 28, 2026, Anthropic announced that it used an AI model to discover a vulnerability in the HAWK lattice-based digital signature algorithm that was a part of the 9 algorithm down selected by NIST. HAWK was withdrawn from consideration.**


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# 2024 – PQC Implementation Becomes Reality

In 2024, NIST published the first PQC Standards – with other global standard bodies set to quickly adopt those as their own. Each of these bodies recommend beginning implementation **immediately** using solutions that are hybrid to start and crypto agile.

















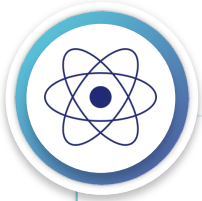










**Hybrid of classical cryptography and PQC**



**Crypto agile solutions**



Thales Trusted Cyber Technologies
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Ecosystem PQC Interoperability Challenges

## Complementary Technology

- Hardware Security Module (HSM) vendors
- Certificate Authorities & HSMs
- Web browsers & servers

## Broader Ecosystem

- PKI Systems
- Identity and Access Management
- Cybersecurity Systems





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# How We've Engaged

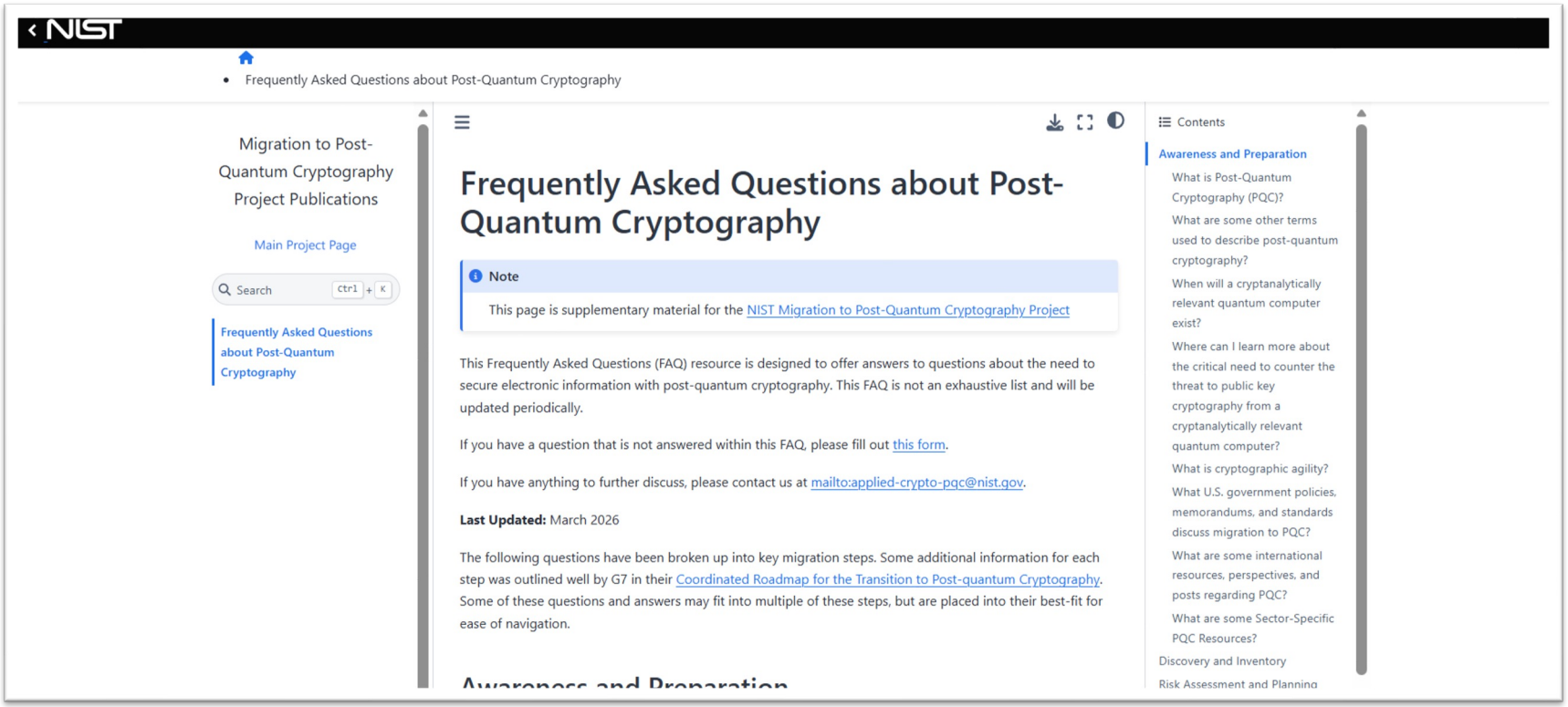
Founding participant in the National Cyber Security Center of Excellence project: Migration to Post-Quantum Cryptography

Hold a Cooperative Research and Development Agreement (CRADA) with the National Security Agency for the evaluation of NIST selected PQC algorithms on HSMs

Premier member of the Linux Foundation's Post-Quantum Cryptography Alliance to contribute to the industry advancement of PQC technology


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# NCCoE FAQ Resource

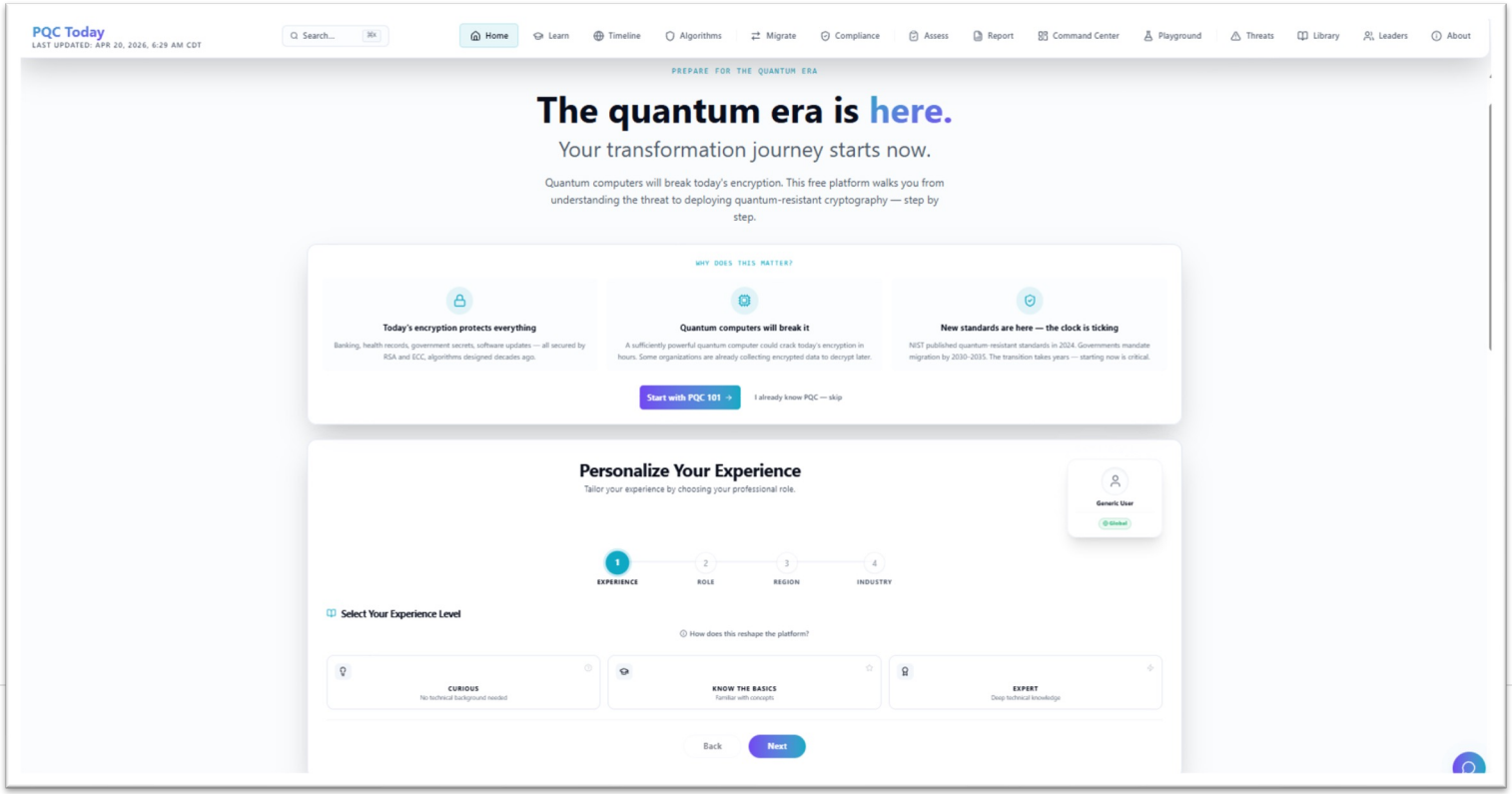



[Frequently Asked Questions about Post-Quantum Cryptography — Migration to Post-Quantum Cryptography Project Publications]


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# PQC Today: Open Source Step-by-Step Transformation Journey

**Free platform for understanding the quantum threat to deploying quantum-resistant cryptography**
**https://www.pqctoday.com**



# Recommendations for Getting Started





This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

# Count Down to Y2Q

**~April 14, 2030**




cloud security alliance®


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of THALES © 2024 THALES. All rights reserved.

THALES
Building a future we can all trust

# Questions


## Gina Scinta
Deputy CTO

Gina.Scinta@thalestct.com