THALES

Building a future we can all trust

Cipher Summit:
Quantum Resistant Security

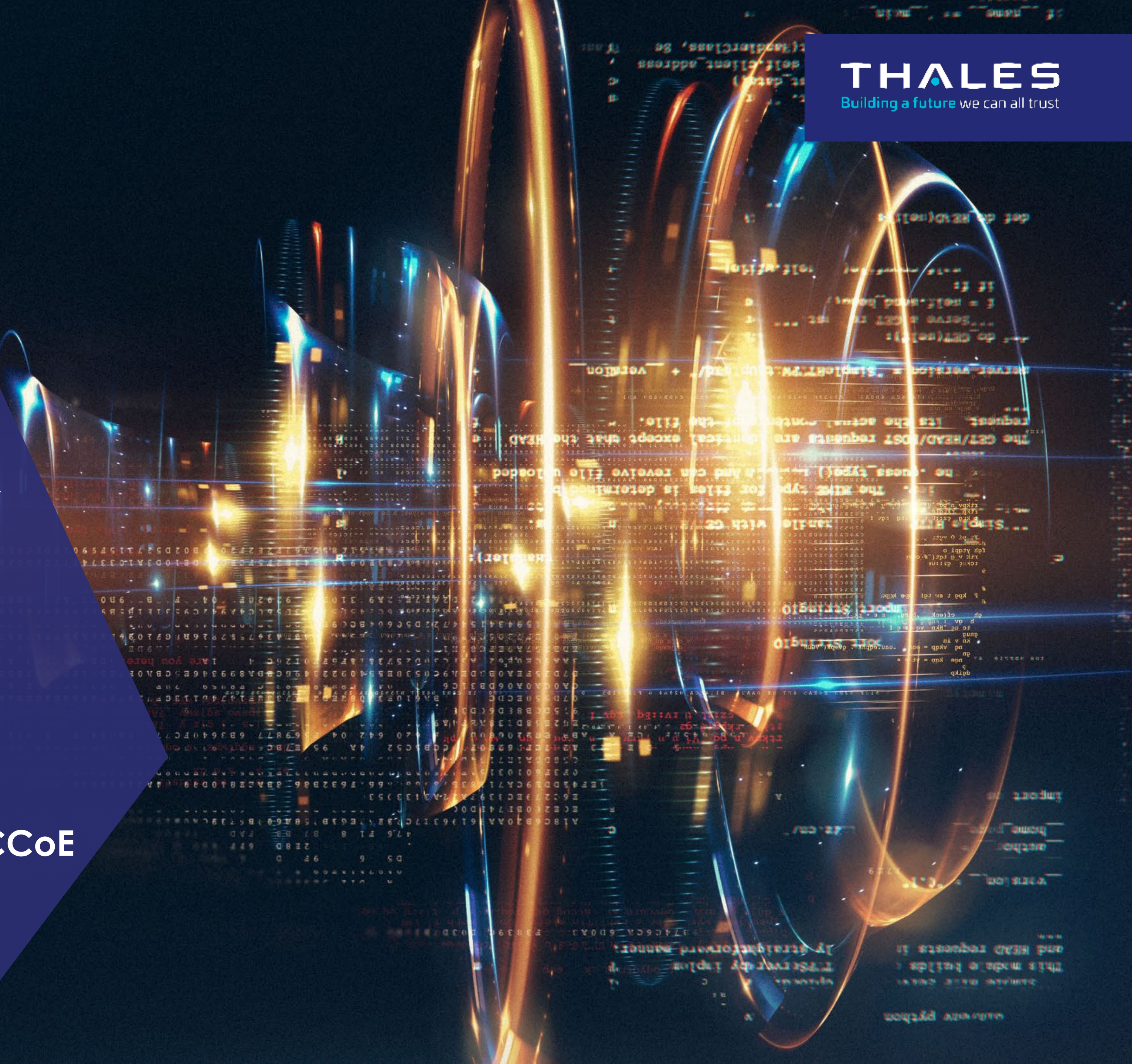
Gina Scinta

Deputy CTO, Thales TCT

Bill Newhouse

Cybersecurity Engineer & Project Lead, NCCoE

19 March 2024

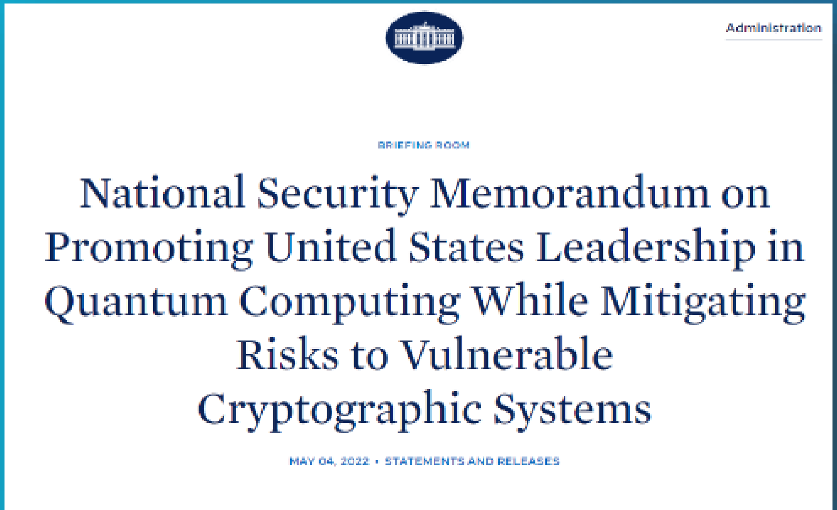


Thales Trusted Cyber Technologies

White House National Security Memo 10

"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."



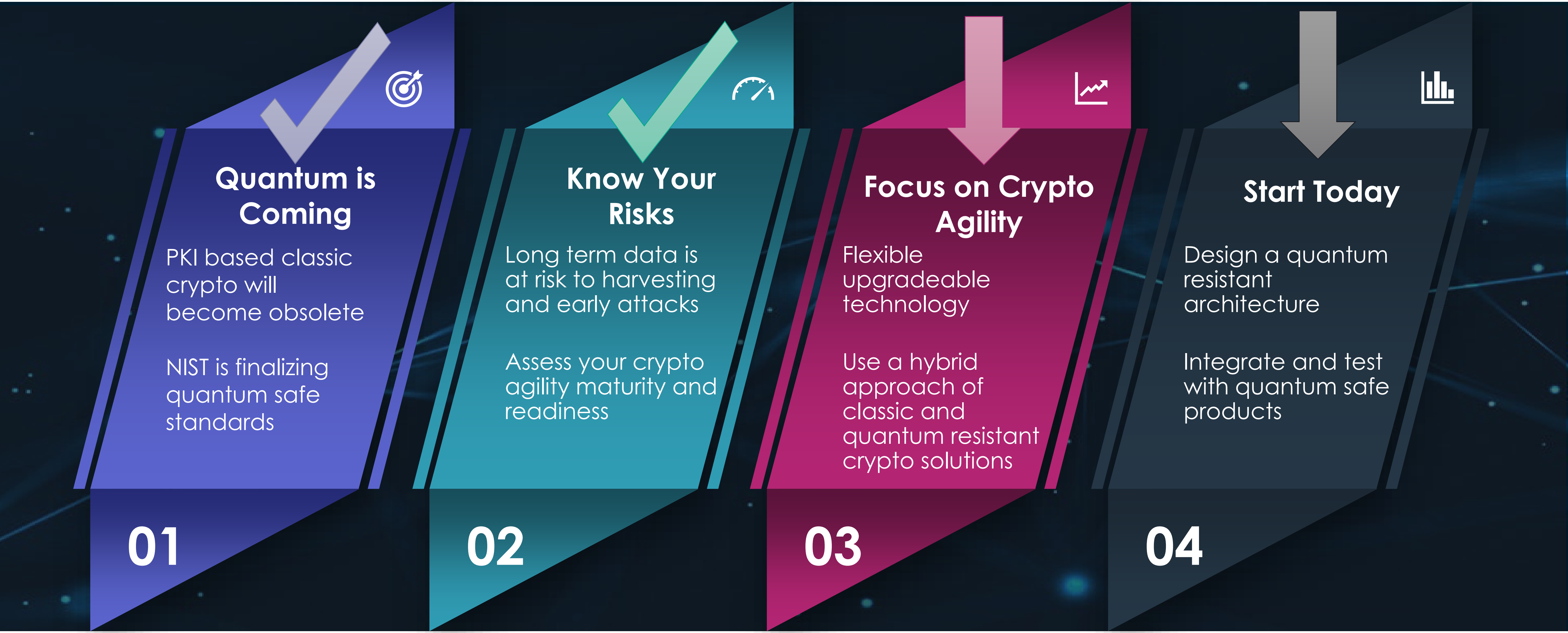
Administration

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

Recommended Quantum Safe Transition Strategy



Quantum is Coming

PKI based classic crypto will become obsolete

NIST is finalizing quantum safe standards

01

Know Your Risks

Long term data is at risk to harvesting and early attacks

Assess your crypto agility maturity and readiness

02

Focus on Crypto Agility

Flexible upgradeable technology

Use a hybrid approach of classic and quantum resistant crypto solutions

03

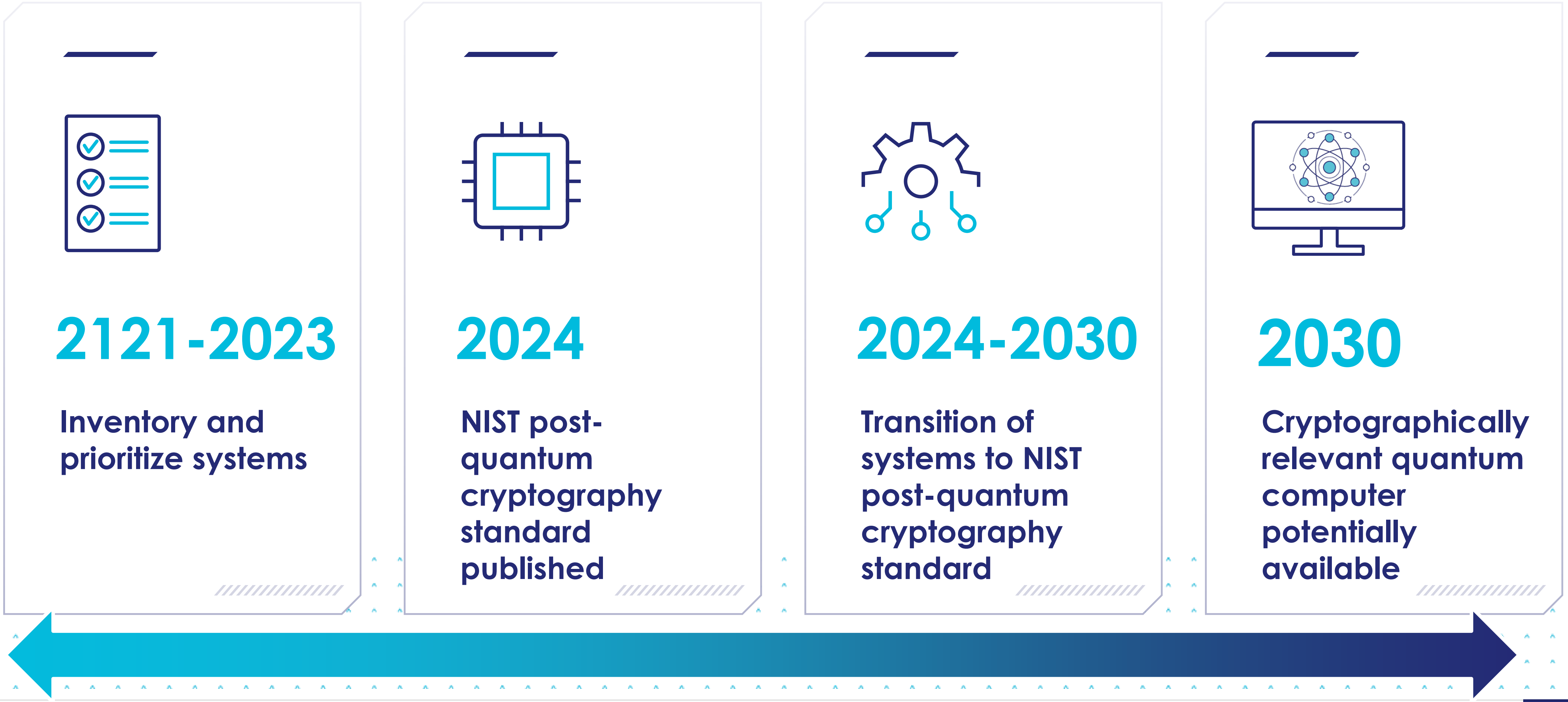
Start Today

Design a quantum resistant architecture

Integrate and test with quantum safe products

04

CISA, NSA and NIST Post-Quantum Cryptography Timeline



2121-2023

Inventory and prioritize systems

2024

NIST post-quantum cryptography standard published

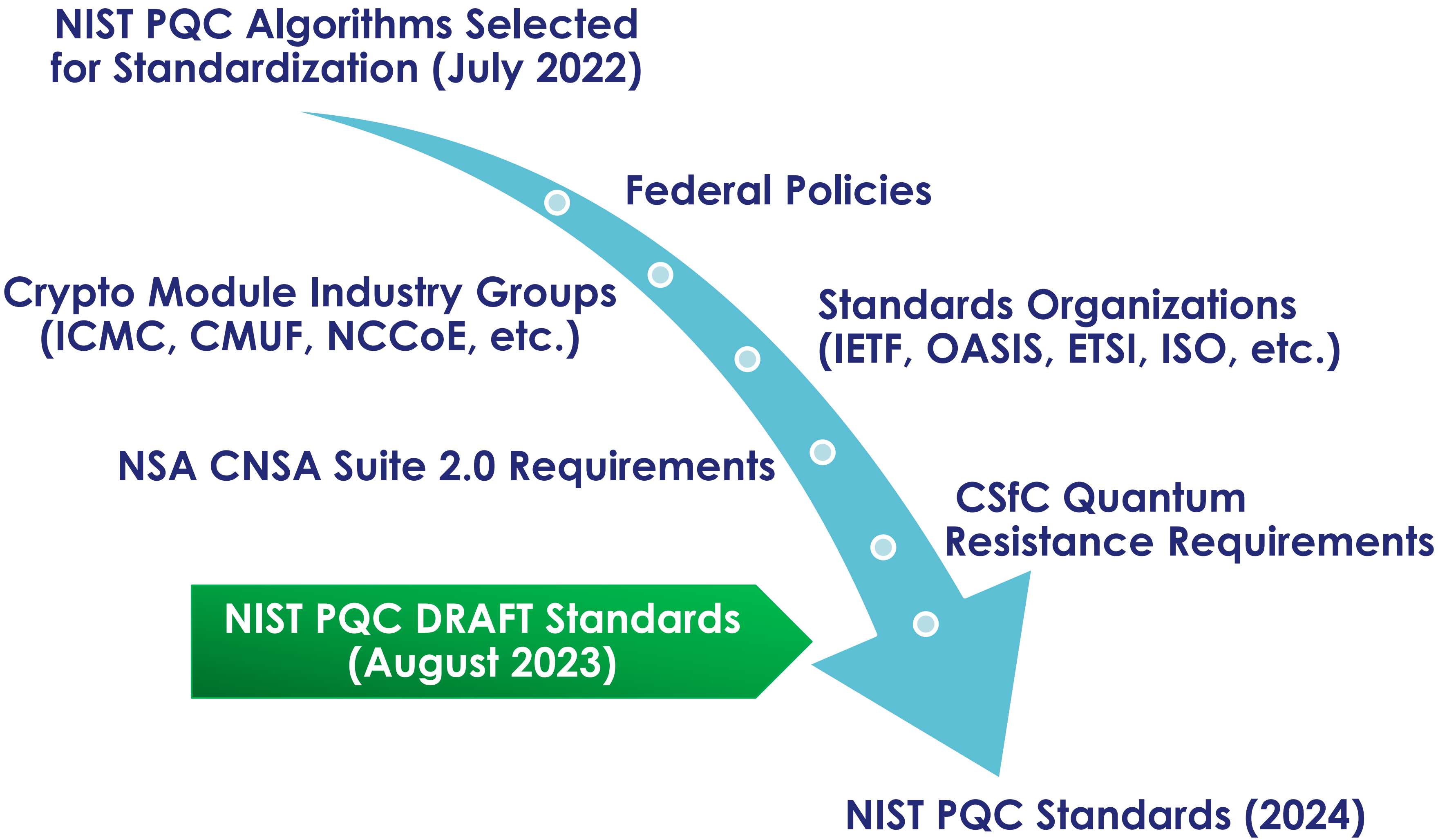
2024-2030

Transition of systems to NIST post-quantum cryptography standard

2030

Cryptographically relevant quantum computer potentially available

Industry PQC Activity



NIST PQC Algorithms Selected
for Standardization (July 2022)

Federal Policies

Crypto Module Industry Groups
(ICMC, CMUF, NCCoE, etc.)

Standards Organizations
(IETF, OASIS, ETSI, ISO, etc.)

NSA CNSA Suite 2.0 Requirements

CSfC Quantum
Resistance Requirements

NIST PQC DRAFT Standards
(August 2023)

NIST PQC Standards (2024)

NIST PQC Draft Standards – Released August 24, 2023

Start Getting Used to New Names

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

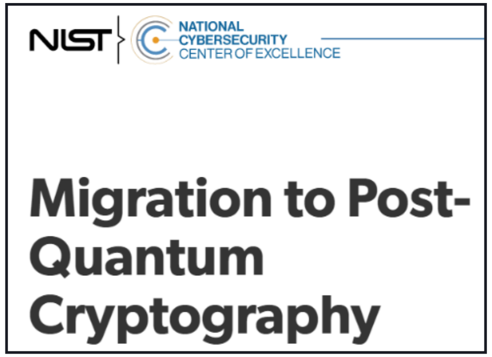
- Formerly SPHINCS+
- FIPS 205 Stateless Hash-Based Digital Signature Standard

FN-DSA

- Formerly FALCON
- Designed for digital signatures
- Slated for its own draft FIPS in 2024

NIST comment deadline was November 22, 2023

Participant in NCCoE “Migration to Post Quantum Crypto” Project



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Migration to Post-Quantum Cryptography

> Project Status

- Launched in June 2022
- Monthly Full CRADA Consortium meetings
- Workstream collaboration meetings (weekly/bi-weekly)
  - Discovery Workstream
  - Interoperability and Performance Workstream
    - Interop testing going well, some HSM vendors have made minor changes
- NIST SP 1800-38
  - Volume A: Executive Summary (Preliminary Draft)
  - Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools (Preliminary Draft)
  - Volume C: Quantum-Resistant Cryptography Technology Interoperability and Performance Report (Preliminary Draft)

> Thales TCT Contribution

- Luna T-Series Network HSM
  - Participating in the Interoperability and Performance Workstream
  - Developed a test methodology
- Thales CN Series Network Encryptors

NCCoE Migration to Post-Quantum Cryptography Project Consortium Participants

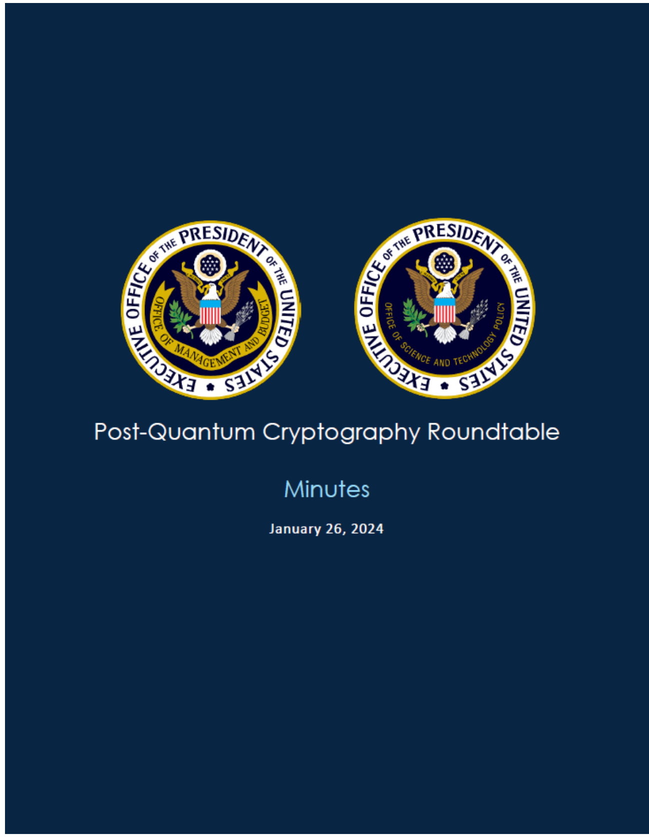
- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Cloudflare, Inc.
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Data Warehouse
- Dell Technologies
- DigiCert
- Entrust
- HP, Inc.
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- Microsoft
- National Security Agency (NSA)
- Palo Alto Networks Public Sector, LLC
- PQShield
- QuantumXChange
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- SSH Communications Security Corp
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Utimaco
- Verizon
- VMware, Inc.
- wolfSSL

White House Post-Quantum Cryptography Roundtable

January 26, 2024

- **Government, Industry and Academia convened to address:**
  - Plans for addressing National Security Memorandum 10 (NSM-10)

- **Following topics were discussed:**
  - Among the four functions of cryptography (Confidentiality, Integrity, Authentication, and Non-Repudiation) which should be prioritized for migration to PQC?
  - Where will the use of hybrid cryptography (both PQC and quantum-vulnerable algorithms) be most appropriate?
  - How will networks need to be re-architected to prepare for PQC migration?
  - What additional costs should be anticipated as part of the PQC migration?
  - How can the PQC migration process be used to enhance cryptographic agility across a network?



Post-Quantum Cryptography Roundtable

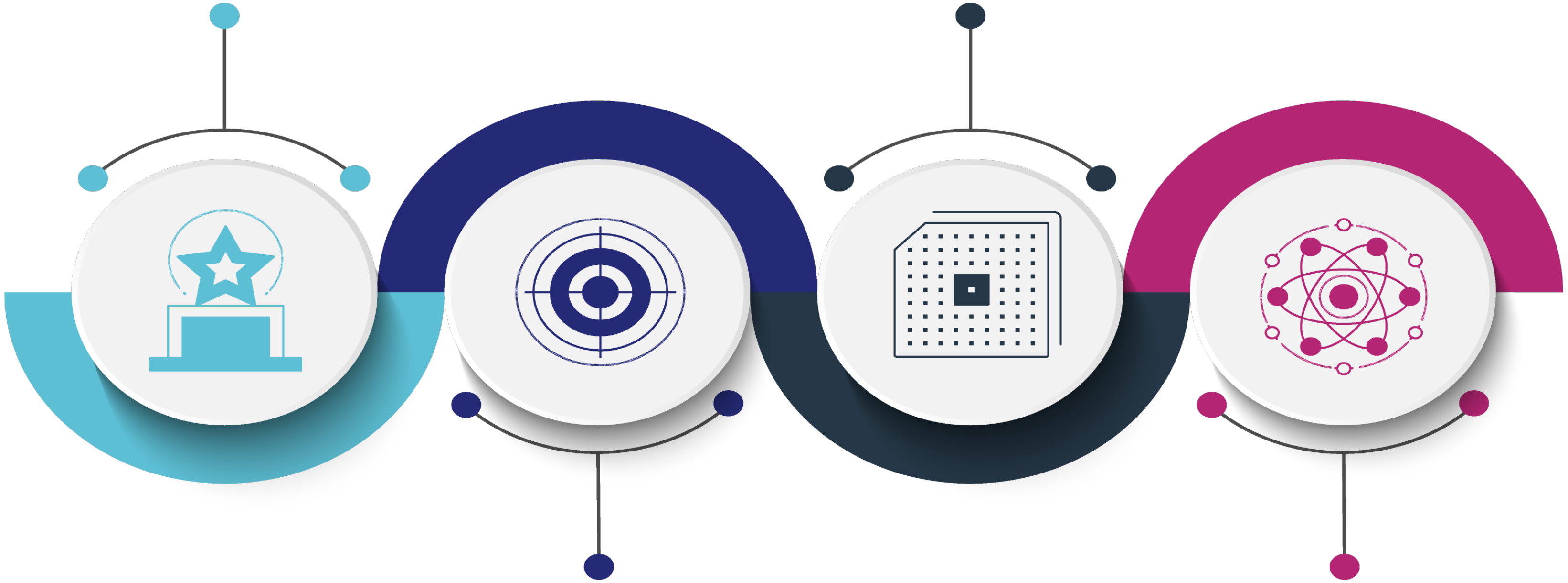
Minutes

January 26, 2024

Recommendations for Getting Started

GET EXECUTIVE SUPPORT

- Educate your agency directors, CISOs, etc.
- They must understand the risk



IDENTIFY AT-RISK DATA

- Long lived data
- Most valuable data
- Protected with asymmetric cryptography

CATALOG CRYPTO AGILE INFRASTRUCTURE

- Which products are impacted?
- Are they all crypto agile?
- How does it align with your IT tech refresh cycle?

DISCUSS PQC STRATEGY WITH VENDORS

- Roadmaps
- Available beta software / firmware
- Proof of concept testing

THALES
Building a future we can all trust

Questions