Post-Quantum
Cryptography Conference

Preparing the United States for PQC

Bill Newhouse
Cybersecurity Engineer & Project Lead, National Cybersecurity Center of Excellence (NCCoE) at NIST

Preparing the United States for Post-Quantum Cryptography

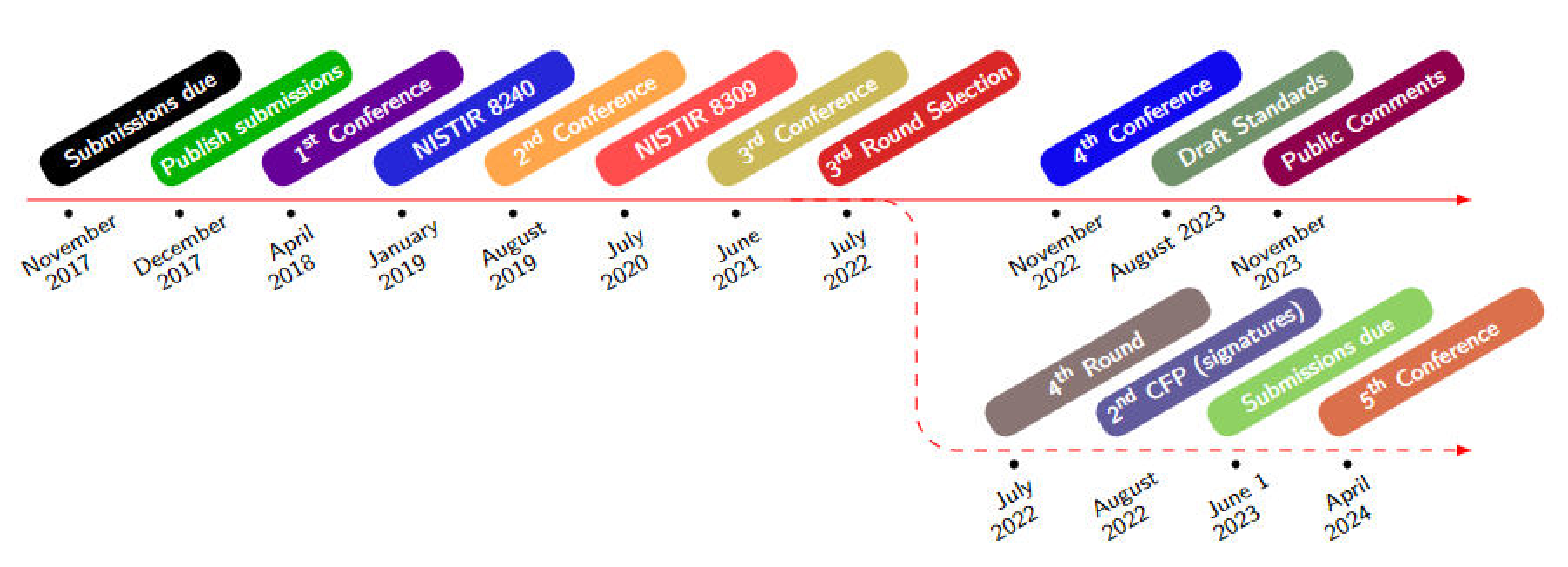
2nd hybrid Post-Quantum Cryptography (PQC) Conference in Amsterdam

Bill Newhouse, NIST NCCoE

November 7, 2023

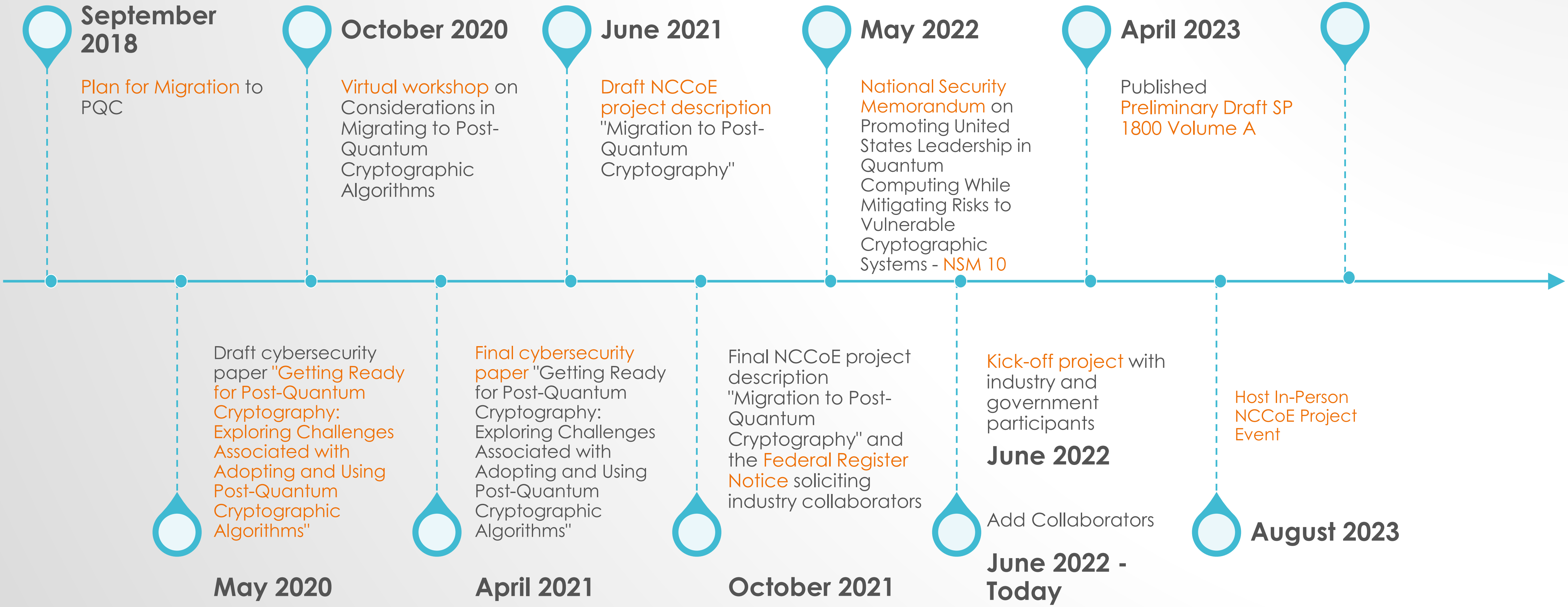
PQC STANDARDIZATIONTIMELINE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



- The 5th NIST PQC Standardization Conference
  - April 10-12, 2024 in Rockville, Maryland
- Draft standards for public comment released Aug 2023
  - Deadline for comments: November 22, 2023
- **The first PQC standards should be published in 2024**

MIGRATION TO PQC PROJECT TIMELINE



September 2018

Plan for Migration to PQC

May 2020

Draft cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

October 2020

Virtual workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms

April 2021

Final cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

June 2021

Draft NCCoE project description "Migration to Post-Quantum Cryptography"

October 2021

Final NCCoE project description "Migration to Post-Quantum Cryptography" and the Federal Register Notice soliciting industry collaborators

May 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems - NSM 10

June 2022

Kick-off project with industry and government participants

June 2022 - Today

Add Collaborators

April 2023

Published Preliminary Draft SP 1800 Volume A

August 2023

Host In-Person NCCoE Project Event

REFERENCES

- **NIST PQC**
  - https://csrc.nist.gov/projects/post-quantum-cryptography
    - https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- **NIST NCCoE Migration to PQC Project Website**
  - https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
- **NSA Post-Quantum Cybersecurity Resources**
  - https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/
- **CISA Post-Quantum Cryptography Initiative**
  - https://www.cisa.gov/quantum
  - https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

U.S GOVERNMENT PQC DRIVERS (1 OF 5)

- **May 04, 2022:** National Security Memo (NSM-10) Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems - https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
  - Sec. 3. Mitigating the Risks to Encryption
    - Emphasis on Cryptographic Agility
    - NIST – initiate an open working group with ith industry, including critical infrastructure owners and operators, and other stakeholders.
    - NIST establish a "Migration to Post-Quantum Cryptography Project"
    - CISA in coordination with Sector Risk Management Agencies shall engage critical infrastructure and state/local/tribal/territorial gov't and provide an annual report on risks posed by CRQC and recommendations for accelerating quantum readiness
    - CISA in coordination with NIST and NSA establish requirements for inventorying all cryptographic systems, list key IT assets to prioritize, benchmarks, and common assessment for evaluating progress on quantum resistant cryptographc migration in IT systems.
    - Federal Civilian Exec Branch (FCEB) agencies shall deliver inventory of IT systems that remain vulnerable to CQRCs
    - 90 days after NIST PQC standards are posted as final, NIST will release a proposed timeline for deprecation of quantum-vulnerable cryptography
    - 1 year after NIST PQC standars are posted as final, OMB in coord w/ CISA and NIST shall issue memo to FCEB
    - NSA shall provide guidance for National Security Sytems (consistent with tasking to NIST noted above for non-National Security Systems)

U.S GOVERNMENT PQC DRIVERS (2 OF 5)

- **Sep 22, 2022:** National Security Agency – Cybersecurity Advisory: Commercial National Security Algorithm Suite 2.0 - https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
  - Algorithms for software- and firmware-signing
    - The National Institute of Standards and Technology (NIST) standardized these algorithms some time ago, but using different algorithms for this special use case is new in CNSA 2.0.
  - Symmetric-key algorithms.
    - There is only a modest change from CNSA 1.0 in this section that allows a bit more flexibility.
  - General-use quantum-resistant public-key algorithms. These are the main public-key algorithms that most applications will require.
    - As they have not completed standardization, this section is forward-looking.
  - Timing. Discusses the timing of the transition to CNSA 2.0.
  - Enforcement. Summarizes requirements related to enforcing NSS algorithm
  - requirements.
  - Additional guidance: RFCs. Provides links to helpful Internet Engineering Task Force Requests for Comment (IETF RFCs) used to implement CNSA 1.0.
  - Reference tables. Features two tables that list algorithms for CNSA 2.0 and for CNSA 1.0.

U.S GOVERNMENT PQC DRIVERS (3 OF 5)

- **Nov 18, 2022:** Memo From Exec Office of the President – Office of Management and Budget – M-23-02 for Heads of Exec Departments and Agencies; Migrating to Post-Quantum Cryptography - https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
  - Prioritized Inventory of Cryptographic Systems (by May 4, 2023 and annually thereafter)
    - Focus High Value Assets and High Impact Systems, or ny other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks. Data that is mission sensitive through 2035
    - Timelines
      - Within 30 days, Identify FCEB agency leads for inventory and migration
      - 90 days, Office of the National Cybersecurity Director (with OMB, CISA, Fedramp PMO) release instructions for inventory
    - Assessment of Funding required for PQC Migration
      - 30 days after May 4, 2023, agencies submit assessment of funding required to migrate systems and assets inventoried above
    - Within 1 year, CISA (in coord w/NIST and NSA) release a strategy on automated tooling and support for assessment of agency progress towards adoption of PQC
    - Testing pre-standardized PQC in production environments
      - Within 60 days of the publication of this memorandum, NIST, in coordination with CISA and the FedRAMP PMO, will establish a mechanism, as part of the working group described in Section VI, to enable the exchange of PQC testing information and best practices among agencies as well as with private sector partners.
    - Within 30 days, OMB and ONCD will establish a cryptographic migration working group consisting of NIST, CISA, NSA, the FedRAMP PMO, and agency representatives. This working group will be chaired by the Federal Chief Information Security Officer and will provide assistance and coordination for agencies conducting cryptographic inventories and migration.

U.S GOVERNMENT PQC DRIVERS (4 OF 5)

- **Dec 21, 2022**: H.R.7535 - Quantum Computing Cybersecurity Preparedness Act (117th Congress (2021-2022) - https://www.congress.gov/bill/117th-congress/house-bill/7535
  - Inventory/Priorization/Assessment
  - Budgetary Effects

U.S GOVERNMENT PQC DRIVERS (5 OF 5)

- **Jun 27, 2023:** U.S. General Services Administration Post-Quantum Cryptography - Market Research - https://sam.gov/opp/cd5127eb36bc4abd8144ef2ec2149a4a/view#20230628
  - Purpose of this RFI is to assist the Government in conducting market research focused on identifying companies who offer Post-Quantum Cryptography (PQC) services and products.

NCCOE PROJECTS OVERVIEW

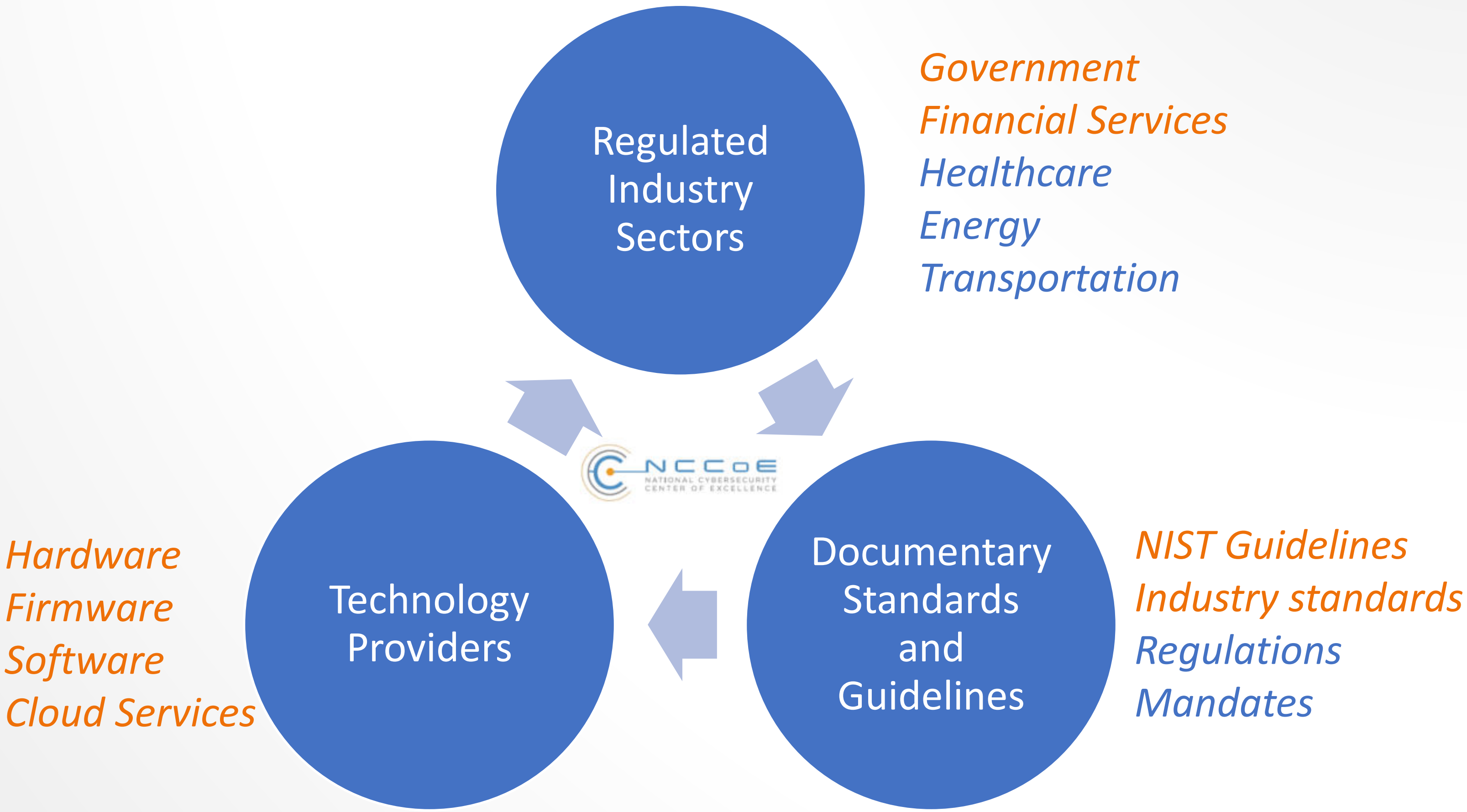
National Cybersecurity Center of Excellence (NCCoE)

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

Practice Guide SP 1800

Engagement Model



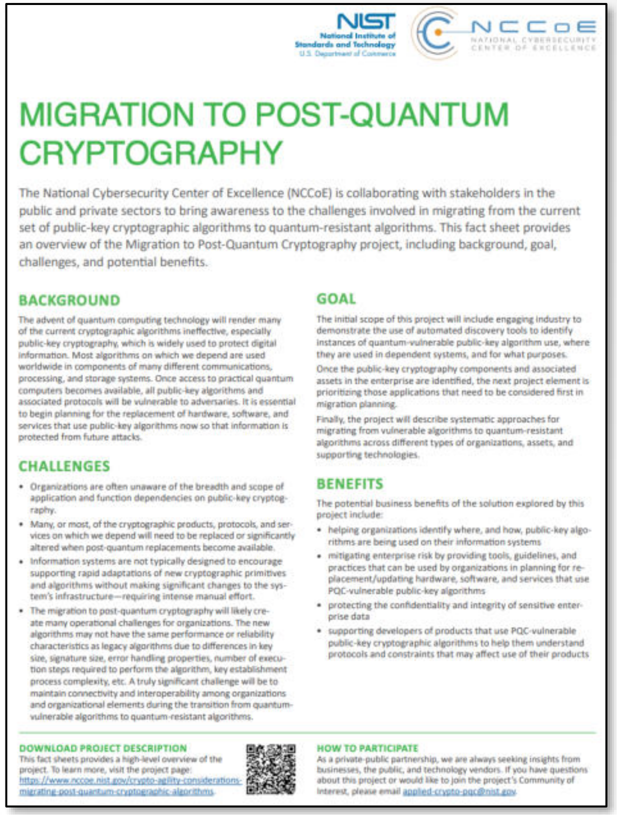
https://www.nccoe.nist.gov/

Migration to Post-Quantum Cryptography (PQC) Project Goal

Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks

MIGRATION TO PQC PROJECT FOCUS

- **Complement NIST PQC standardization effort**
- Support US Government PQC initiatives (White House NSM-10 (M-23-02), CISA, NSA CNSA 2.0, etc.)
- Tackle challenges with adoption, implementation, and deployment of PQC
- Engage with the community including industry collaborators and across government to bring awareness to the issues involved in migrating to post-quantum algorithms
- Coordinate with standard developing organizations and government and industry sectors community to develop guidance to accelerate the migration



MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes.

Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning.

Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION
This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

HOW TO PARTICIPATE
As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov.

Migration to PQC Project Collaborators

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

Post-Quantum Cryptography Conference

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

01 COMMUNIQUE

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia

PKI Consortium