July 2024

REPORT ON POST-QUANTUM CRYPTOGRAPHY

as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260

PRESENTED TO

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Oversight and Accountability

Table of Contents

Introduction

Under the Quantum Computing Cybersecurity Preparedness Act ("the Act"), 6 U.S.C. § 1526, the Office of Management and Budget (OMB) is required to submit a report to Congress outlining key components of the strategy to migrate Federal information systems[1] to post-quantum cryptography (PQC). This report fulfills this requirement and consists of three sections. First, it outlines the Federal Government's strategy to address the risk that cryptographic systems currently used in Federal information systems may be vulnerable to future compromise by a cryptanalytically relevant quantum computer (CRQC). Second, it provides rough order of magnitude estimates for funding that may be required for agencies to move away from the use of quantum-vulnerable cryptography. Finally, the report details efforts by Federal agencies, led by the National Institute of Standards and Technology (NIST), to develop standards for PQC.

Under the leadership of the Biden-Harris Administration, the Federal Government is poised to make significant progress in migrating to PQC during 2024 and beyond, as required by the Act and National Security Memorandum 10, Promoting United States Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems ("NSM-10").

Quantum computers show tremendous promise for the advancement of many fields, from pharmaceuticals to materials science. However, it is also likely that a sufficiently powerful quantum computer (a CRQC) will be able to break some forms of cryptography that are now commonly used throughout government and the private sector. A CRQC is not yet known to exist; however, steady advancements in the quantum computing field may yield a CRQC in the coming decade. Accordingly, while the U.S. Government continues to ensure the Nation's ability to maintain a competitive advantage in quantum computing, Federal agencies must also bolster the defense of their existing information systems by migrating to the use of quantum-resistant public-key cryptographic systems (PQC).

Cryptography is the use of mathematical algorithms to perform security functions, such as encrypting data when it is transmitted between information systems or ensuring that the data is not altered in transit.[2] Execution of these functions depends on the keys created by those mathematical algorithms remaining secure. Just like a physical lock, a malicious actor can compromise the cryptography if they are able to obtain the full key.

Public-key cryptography addresses this issue by dividing the full key into two parts—a public key paired with a private key. The public key can be transmitted freely over an unsecure connection. Once received, the public key is combined with the private key to activate the cryptographic function. This technology is useful for many digital functions. For example, public-key cryptography allows the secure transmission of data over untrusted networks, such as the internet. It can provide methods for creating and verifying a "digital signature" that validates the identity of a person or computer on a network. It can verify the integrity of a software update by validating that the update has not been altered by a malicious actor. Public-key cryptography is a foundational capability for government, private sector, and critical infrastructure information systems. Almost every part of an information system, and almost every cyber defense, depends on some form of public-key cryptography.

Strong public-key cryptography[3] cannot be broken by current classical computers because the computing power required is too great. However, quantum computers operate differently from classical computers. PQC solves this security challenge by utilizing a different type of mathematical algorithm, one that a CRQC cannot easily solve. However, before agencies can start implementing PQC, it is critical to first ensure that the algorithms used are sufficiently secure against both classical and quantum computers. Additionally, these algorithms must be standardized in an internationally recognized manner. This standardization process ensures that agencies can continue to use commercial hardware and software and also communicate with the broader internet. NIST is at the forefront of the international process to develop these secure and standardized algorithms.

----

[1] This report does not address national security systems, as defined by 44 U.S.C. § 3552(b)(6). *See* the Act, Pub. L. No. 117-620, § 5 (6 U.S.C. § 1526 note).
[2] Additional functions of cryptography are enumerated later in this report.
[3] In addition to public-key cryptography, there is also a separate class of cryptography known as "symmetric cryptography." This cryptography is sufficiently resistant to a CRQC and therefore is not included in plans for migration to PQC.

Section 1:
Strategy for Migration to PQC

The strategy for migrating Federal information systems to PQC is based on four primary precepts:

1. A comprehensive and ongoing cryptographic inventory is a key baseline for successful migration to PQC;
2. The threat of “record-now-decrypt-later attacks” means that the migration to PQC must start before a CRQC is known to be operational;
3. Agencies must prioritize systems and data for PQC migration; and
4. Systems that will not be able to support PQC algorithms must be identified as early as possible.

This section explains each of these precepts and how it informs the Federal migration strategy.

1. A comprehensive and ongoing cryptographic inventory is a key baseline for successful migration to PQC

Public-key cryptography solves the challenge of how an information system can create a secure connection over a channel that is not inherently secure. On modern information systems, it performs the following functions:

- *Confidentiality* ensures that only users who hold the correct key or keys are able to view secured information;
- *Integrity allows users to verify that information has not been altered between two points in time—for example, between when it is created and when it is read;*
- *Authentication ensures that a user provides a proof of identity, such as an access card, PIN, or fingerprint, before accessing a system;*
- *Digital signature provides assurance of the identity of the source of stored or transmitted information; in other words, it indicates whether a third party can be confident about the identity of the source of the information.*

If public-key cryptography were not able to securely provide these functions, agency information systems and the technology ecosystem as a whole, as currently constituted, would not be able to function effectively. For example, public-key cryptography underpins the confidentiality of a vast array of sensitive transactions: submission of payment information during e-commerce, transmission of tax data to the Internal Revenue Service, and connection of veterans to medical professionals during telehealth visits. Integrity relies on public-key cryptography to ensure that malicious code has not been inserted into a software update and that the contents of an email have not been changed in transit between sender and recipient. Authentication relies on public-key cryptography to secure access to almost every type of digital system. Finally, digital signature schemes rely on public-key cryptography to demonstrate authorship and prevent forgeries of documents, conversations, websites, or messages sent using digital means. All of the public-key cryptography that enables each of these functionalities must be migrated to PQC, because a CRQC may someday be capable of undermining the algorithms that underpin this cryptography.

However, in order for this migration to be successful, agencies first need to map out where this public-key cryptography exists. A comprehensive cryptographic inventory enables agencies to plan out their migration to PQC and track that migration once it has started. It allows them to focus on identifying their use of quantum-vulnerable algorithms.

Automated cryptographic inventory solutions, which are rapidly emerging, can expedite and simplify aspects of an agencies' inventory process. Consistent with OMB Memorandum M-23-02, Migrating to Post-Quantum Cryptography ("M-23-02") the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) has developed a strategy for agencies to evolve their automated inventory capability. Automated inventories, however, may not identify all instances of public-key cryptography because automated tools may not have visibility over an entire agency network or be compatible with all digital systems. Accordingly, under M-23-02, each agency is required to perform an annual manual inventory. Completing this manual inventory entails researching each piece of hardware and software to discover the type of cryptography used and, if that cryptography is determined to be quantum-vulnerable, cataloging key attributes.

The ubiquitous and embedded nature of public-key cryptography means that maintaining a comprehensive inventory will be an iterative and ongoing process. Iterative inventories will enable agencies to improve automated and manual methodologies and improve the breadth and fidelity of data. Additionally, as hardware and software undergo periodic patching, updating, and lifecycle refreshes, the inventory will need to be updated accordingly. This ongoing process will require sustained investment by agencies; it will remain critical throughout the entire migration process and well into the future as the strength of cryptography needs to be continuously evaluated against new quantum and classical computers.

2. The threat of record-now-decrypt-later attacks means that the migration to PQC must start well before a quantum computer capable of breaking current encryption is known to be operational

By design, encrypted data must pass through numerous untrusted nodes when transiting the internet. Such routing is necessary because it would be impossible for every internet user to have a dedicated connection to each information system with which they need to communicate. Public-key encryption enables this global network; even if data is intercepted in transit, a classical computer cannot read it without the private key. While a CRQC is not yet known to exist, data encrypted using current classical algorithms is still vulnerable. This is because a malicious cyber actor could collect encrypted data in bulk today, store that data, and decrypt it if a CRQC becomes capable. Although cryptography guards against data being intercepted in readable format or altered when in transit, it does not stop a malicious actor from making an exact copy of the encrypted data. This type of attack is commonly known as a "record-now-decrypt-later" attack.

While data is especially vulnerable when transiting the internet, it may also be at risk on private networks. For that reason, key zero trust policies, including Executive Order 14028, Improving the Nation's Cybersecurity, and OMB Memorandum M-22-09, Federal Zero Trust Strategy, require that data be encrypted when transiting internal agency networks. A zero-trust architecture assumes compromise. Encrypting data transiting an internal network protects that data even if the perimeter defenses of that network are breached. Public-key cryptography also protects these internal data flows, and therefore this data is also vulnerable to a CRQC and a record-now-decrypt-later attack.

Several defenses do currently exist against a record-now-decrypt-later attack. Current public-key cryptographic implementations often rotate encryption keys rapidly, meaning that a CRQC could only decrypt small amounts of stored data at a time. Since encrypted data is currently unreadable, a malicious actor could only guess if stored stolen data will be valuable in the future. The widespread practice of encrypting all data in transit over the internet, from sports scores to bank account numbers, makes it even more difficult to guess if captured encrypted data is sensitive. Finally, because storage capacity is expensive and in high demand, adversary capacity to store encrypted data is limited.

However, these defenses will likely only slow an advanced adversary, and an advanced adversary may correctly guess which encrypted data they should store. Accordingly, and as outlined in NSM-10, diligent preparation and migration to PQC is the best long-term solution to defend against a record-now-decrypt-later type attack. To ensure long-term defense of critical information systems and the data they store and process, it is crucial to implement strong classical cryptography on those systems now and to prioritize migration of that cryptography to PQC once it becomes available.

3. Agencies must prioritize systems and data for PQC migration

Migrating public-key cryptography to PQC will require deliberate planning over multiple years. Interoperability is a primary concern for migration. For example, if one system creates a public key using a migrated PQC implementation, but the receiving system has not been migrated, an encrypted connection will not be established. Because many systems are configured to "fail secure" and not transmit data if an encrypted tunnel cannot be created, this interoperability failure may have operational impacts. As such, this migration will not be as simple as flipping a switch. Agencies will need to use developed cryptographic inventories to carefully plan and prioritize their migrations to focus on high value assets and high-impact systems.

Accordingly, agencies are prioritizing their most sensitive systems and datasets for migration to PQC. While agencies will eventually migrate all cryptography to PQC, M-23-02 anticipates that the following will be migrated first:

- High impact information systems; [4]
- Agency high value assets; [5] and
- Any other systems that an agency determines are likely to be particularly vulnerable to CRQC-based attacks, including information systems or assets that:
    - Contain data expected to remain mission-sensitive in 2035 ; [6] or
    - Are logical access control systems based in asymmetric encryption (such as public key infrastructure).

This prioritization schema ensures that agency will focus their resources on defending the cryptography, functions, and data most vulnerable to a CRQC. Once migration begins, agencies will continuously re-assess their prioritization and timelines.

[4] Defined by NSM-10 as "an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards (FIPS) 199 potential impact value of 'high.'"

[5] Defined by NSM-10 as "information or an information system that is so critical to an organization that the loss or corruption of this information, or loss of access to the system, would have serious impacts on the organization's ability to perform its mission or conduct business"

[6] This criterion refers to data that if recorded now, and later decrypted by a CRQC in 2035, would still be considered mission sensitive.

4. Systems that will not be able to support PQC must be identified as early as possible

The 2023 National Cybersecurity Strategy (NCS)[7] states that "the Federal Government must replace or update IT and OT systems that are not defensible against sophisticated cyber threats." Among these threats is the threat to cryptography posed by a CRQC. A key aspect of the cryptographic inventory process is early identification of systems that may not be able to migrate to PQC. There are numerous reasons why such a system may exist. Some hardware and software, both modern and legacy, is not designed with cryptographic implementations that can be changed. Many legacy systems may not have the processing speed, memory or bandwidth necessary to implement PQC implementations. Replacing hardware, software, and digital systems that are not PQC-compatible will likely be a time- and resource-intensive process. Many of these modernizations are underway as part of the NCS implementation. Agencies will incorporate these modernization timelines into PQC migration planning.

Agencies must identify these unsupported systems as early as feasible in order to begin planning and avoid PQC migration delays. Because of the interconnected and interoperable nature of cryptography across agency networks, one system that cannot be migrated may prevent others from migrating as well. Identifying these unsupported systems and dependencies can best be done through testing in real-world environments. Agencies can also use pre-standardized PQC, and standardized PQC once completed by NIST, to perform such testing on their networks. M-23-02 encourages agencies to begin testing PQC as soon as possible and further states that "to ensure that tests are representative of real-world conditions, they may be conducted or allowed to operate in production environments, with appropriate monitoring and safeguards, alongside the use of current approved and validated algorithms."

[7] Available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Section 1: Federal Quantum Action Plan and Strategy

Actions Taken

In November 2022, OMB issued M-23-02, which directed agencies to inventory cryptography on a prioritized subset of information systems and develop funding estimates for the migration of that cryptography to PQC. The memorandum also encouraged agencies to test pre-standardized PQC algorithms to ensure proper functioning and interoperability and established an interagency PQC migration working group, which meets bi-weekly and reports to a quarterly interagency policy committee on NSM-10 implementation led by the National Security Council.

In January 2024, OMB and the Office of Science and Technology Policy convened the PQC interagency migration working group roundtable with government representatives and leaders from industry and academia in order to discuss options for addressing the requirements of NSM-10 and the Act. The lessons learned from this roundtable will inform future efforts.

Next Steps

As directed by NSM-10 and required by the Act, within one year of the adoption of the first set of NIST standards for PQC, OMB will release guidance directing agencies to develop a prioritized migration plan. OMB will issue this guidance in coordination with CISA and NIST and in consultation with ONCD. OMB will continue to use the PQC migration interagency working group to coordinate efforts across agencies and connect stakeholders and subject matter experts as inventory and planning activities continue.

Section 2:

Current estimate of the amount of funding needed by agencies to secure information technology

Section 2: Current estimate of the amount of funding needed by agencies to secure information technology

OMB and ONCD, in collaboration with CISA and NIST, have worked with Federal agencies to take specific steps to prepare for the transition to PQC. In particular, this has involved three key activities:

1. Developing an initial inventory of cryptographic systems present on agency information systems (other than national security systems (NSS));
2. Developing cost estimates for the transition; and
3. Developing prioritization criteria for the transition.

Agencies deliver an annual inventory to OMB and ONCD of quantum-vulnerable cryptography on prioritized systems and the estimates of the cost for migrating those systems. Based on those cost estimates, ONCD projects that that the total government-wide cost required to perform a migration of prioritized information systems to PQC between 2025 and 2035 will be approximately $7.1 billion in 2024 dollars. As directed by NSM-10, the Department of Defense, the Office of the Director of National Intelligence, and the National Manager for NSS are developing separate funding estimates for the migration of NSS to PQC.

This initial projection reflects a high, but expected, level of uncertainty associated with the inventory and transition to PQC. Agencies are required to update their cost estimates annually to allow for adjustments as they gain familiarity with the inventories, costing methodologies, and the transition process. Initial cost estimates represent a rough order of magnitude rather than precise calculations.

In developing their cost estimates, agencies accounted for the conditions and qualities of the specific host system and networks. In certain cases, agencies were aware of systems that could not accommodate new cryptographic systems. As mentioned previously in this report, such systems could include those whose cryptographic algorithms were hardwired into the hardware or firmware, or those that lack the capacity to accept replacement cryptographic algorithms. The cost to replace those systems constitutes a significant portion of the overall estimate.

Section 3:

Coordination efforts led by NIST, including timelines, to develop standards for PQC

Section 3: Coordination efforts led by NIST, including timelines, to develop standards for PQC

Migration to PQC is heavily contingent on the widespread availability and adoption of open PQC standards. Federal networks do not operate in a vacuum. These networks and constituent information systems are dependent on the same or similar commercial vendors and technology used throughout the private sector and internationally. When agencies utilize open standards in products they procure, they gain greater flexibility and security at a lower cost. NIST is driving the strength and interoperability of PQC standards by leading an open standards development process. This open process entails engaging extensively with cryptographers and security researchers in the United States and internationally, as well as publicly publishing proposed standards.

In December 2016, NIST initiated the PQC standardization process by issuing a public call for algorithm submissions. A total of 82 candidate algorithms were ultimately submitted. Of these 82, NIST accepted 69 algorithms into the first round of the standardization process that met both the submission requirements and the minimum acceptability criteria. In January 2019, after a year-long period for the public to review and comment on the candidates, NIST selected 26 algorithms to move to a second round of evaluation. Internal NIST analysis and public feedback identified these algorithms as the most promising candidates for standardization. During the second round, both NIST and the broader cryptographic community performed continued evaluation. In July 2020, after careful deliberation, NIST selected seven finalists and eight alternatives to move to the third round.

During the third round, NIST performed a more thorough analysis of the theoretical and empirical evidence used to justify the security of the finalists. They also carefully benchmarked the performance of the candidate algorithms using optimized implementations in a variety of hardware and software platforms. NIST held the third PQC standardization conference in June 2021, inviting each of the finalists and alternates to present an update on their candidate algorithm. In addition, several researchers presented work that was relevant to the PQC standardization process. After completing the third round, NIST selected four algorithms for initial standardization. NIST will consider these candidates for future standardization at the conclusion of the fourth round, and will also review and evaluate potential PQC algorithms for standardization as new use cases emerge.

Strong algorithms are critical to strong cryptography, but so is the manner in which these algorithms are implemented. By exploiting weaknesses in these implementations, malicious cyber actors can bypass the protections provided by the algorithms. Additionally, in some cases algorithms may not perform as expected when implemented. Accordingly, as vendors integrate these algorithms into hardware and software, NIST will evaluate these implementations under the Cryptographic Module Validation Program (CMVP), a joint effort with the Canadian Centre for Cyber Security.

The CMVP consists of an independent test to ensure that defenses using cryptographic algorithms are built correctly and function as intended. These tests are conducted by NIST-accredited testing labs. Following a test, the independent lab will send the results to NIST for final certification. In addition to Federal agencies, the governments of Canada, Japan, and several industry regulators use the CMVP certifications, driving international operability.

Section 3: Coordination efforts led by NIST, including timelines, to develop standards for PQC

As of this report, the volume of cryptographic modules waiting testing under the CMVP has increased beyond current program capacity. This increase is due to several cryptographic migrations occurring in a short period of time. The migration to PQC will be significantly more comprehensive than in previous cases and will therefore require a large amount of CMVP capacity. To address this current and future backlog, NIST is currently in the process of a CMVP modernization effort. This effort aims to expand testing lab capabilities, increase staffing to clear and issue certifications, and obtain contract support to increase capacity during submission surges. Funding to drive this modernization is part of the overall cost of the Federal Government's PQC migration.

Concurrent with NIST's standardization of PQC algorithms, the NIST National Cybersecurity Center of Excellence (NCCOE) has initiated a project titled "Migration to Post Quantum Cryptography." [8] The objective of this project is to explore and publish information regarding best practices to facilitate preparation for and migration to PQC. The NCCOE has developed partnerships with numerous private sector partners to share knowledge, lessons learned, and best practices. As of this report, the NCCOE has released two Special Publications (SP) for public comment:

- NIST SP 1800-38B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools; [9]
- NIST SP 1800-38C: Quantum Resistant Cryptography Technology Interoperability and Performance Report. [10]

----

[8] More information is available at https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
[9] Available at https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf
[10] Available at https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

Timeline

2015

April 2015: Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg, MD

February 2016: PQC Standardization: Announcement and outline of NIST's Call for Submissions presentation given at PQCrypto 2016

April 2016: NISTIR 8105, Report on Post-Quantum Cryptography, released

December 2016: Federal Register Notice – Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms

2017

November 2017: Submission Deadline for NIST PQC Standardization Process

December 2017: First-round candidates announced. The public comment period on the first-round candidates began.

April 2018: First NIST PQC Standardization Conference

January 2019: Second-round candidates announced. NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, released. The public comment period on the second-round candidates began

2019

August 2019: Second NIST PQC Standardization Conference, Santa Barbara, CA

April 2020: NIST invited comments from submitters and the community to inform its decision-making process for the selection of third-round candidates

May 2020: Draft NIST Whitepaper Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms published

July 2020: Third-round finalists and alternate candidates announced. NISTIR 8309, Status Report on the Second Round of the NIST Post Quantum Cryptography Standardization Process, released. The public comment period on the third-round candidates began.

October 2020: NIST hosts Virtual Workshop on Considerations in Migrating to PQC Algorithms at the NCCoE *(https://www.nccoe.nist.gov/get-involved/attend-events/virtual-workshop-considerations-migrating-post-quantum-cryptographic)*

2021

April 2021: NIST Cybersecurity Whitepaper Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms published

June 2021: Third NIST PQC Standardization Conference, held virtually; NCCoE posts Draft NCCoE project description "Migration to Post-Quantum Cryptography" for public comment.

October 2021: NCCoE Final NCCoE project description "Migration to Post-Quantum Cryptography" and the Federal Register Notice soliciting industry collaborators *(https://www.federalregister.gov/documents/2021/10/13/2021-22223/national-cybersecurity-center-of-excellence-nccoe-migration-to-post-quantum-cryptography)*

2022

June 2022: NCCoE has online Migration to PQC project kickoff meeting with first fifteen consortium members – workstreams identified for cryptographic discovery (inventory) and interoperability/performance of the draft PQC algorithms in communication protocols

July 2022: Candidate algorithms to be standardized are announced, along with alternate candidates advancing to the fourth round. NIST-IR 8413-upd1, Status Report on the Third Round of the NIST Post Quantum Cryptography Standardization Process, released.

2023

August 2023: First three Draft Federal Information Processing Standards (FIPS) Published by NIST

December 2023: NIST Special Publication 1800-38B, Quantum Readiness: Cryptographic Discovery, is a preliminary draft offering (1) a functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities; (2) a use case scenario to provide context and scope our demonstration; (3) an examination of the threats addressed in this demonstration; (4) a multifaceted approach to start the discovery process that most organizations can start today; and (5) a high-level architecture based on our use case that integrates contributed discovery tools in our lab.

NIST Special Publication 1800-38C, Quantum Readiness: Testing Draft Standards for Interoperability and Performance, is a preliminary draft offering (1) identification of compatibility issues between quantum ready algorithms, (2) resolution of compatibility issues in a controlled, non-production environment, and (3) reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts.

Publication of Draft 1800-38 Series Guidance, "Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery"

2024

April 2024: Fourth NIST PQC Standardization Conference, Rockville MD

July 2024: Publication of Final first three PQC FIPS.

August 2024: Start of Standardization of FALCON Digital Standard.

September 2024: Continued inclusion of completed FIPS in national and international Standards Bodies.

Conclusion:

Securing the Federal Government against the risk posed by a CRQC will require a governmentwide effort sustained over multiple years.

As outlined in this report, cryptography is an essential, ubiquitous, and embedded component in all Federal information systems.

Securing this cryptography against current and future threats is critical to the deployment and maintenance of key cyber defenses as well as the ability of Federal agencies to provide essential services to the public.

By taking the steps set out in the Act and NSM-10, and drawing upon the combined authorities and expertise of OMB, ONCD, CISA, NIST, and NSA, the Federal Government is well positioned to accomplish this objective.