PROJECT DESCRIPTION

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

William Barker

Dakota Consulting

Murugiah Souppaya

National Institute of Standards and Technology

DRAFT

June 2021

applied-crypto-pqc@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit http://www.nist.gov.

This document describes challenges associated with migration from current public-key cryptographic algorithms to quantum-resistant algorithms, and approaches to facilitating that migration.

ABSTRACT

The NIST National Cybersecurity Center of Excellence (NCCoE) is initiating the development of practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks. These practices will take the form of white papers, playbooks, and demonstrable implementations for organizations. In particular, the audience for these practices is intended to include organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products. This effort complements the NIST post-quantum cryptography (PQC) standardization activities.

ACKNOWLEDGMENTS

This project description was developed from the presentations and discussions that occurred at the NCCoE-hosted Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms. NCCoE thanks Dustin Moody, Lidong Chen, and Matthew Scholl for contributing to the development of this project description.

KEYWORDS

algorithm; cryptographic hardware; cryptographic module; cryptography; encryption; identity management; key establishment and management; post-quantum cryptography; public-key cryptography

DISCLAIMER

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to applied-crypto-pqc@nist.gov.

Public comment period: June 4, 2021 to July 7, 2021

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Purpose

As reflected in National Institute of Standards and Technology (NIST) Interagency or Internal Report (NISTIR) 8105, *Report on Post-Quantum Cryptography* [1] and NISTIR 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process* [2], work on the development of quantum-resistant public-key cryptographic standards is underway, and the algorithm selection process is well in-hand, with algorithm selection expected to be completed in the next one to two years (https://csrc.nist.gov/projects/post-quantum-cryptography).

To complement the ongoing effort, the National Cybersecurity Center of Excellence (NCCoE) has initiated a campaign to bring awareness to the issues involved in migrating to post-quantum algorithms, which will include developing white papers, playbooks, and proof-of-concept implementations. NIST has developed and posted a cybersecurity white paper, *Getting Ready for Post-Quantum Cryptography* [3] to start the discussion.

In addition, the NCCoE is forming a Cryptographic Applications community of interest in coordination with the NIST Post-Quantum Cryptography standardization team and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) team. The community of interest will work on a migration playbook that would address the challenges previously described and provide recommended practices to prepare for a smooth cryptographic migration.

Finally, the NCCoE has developed this project description for practical demonstration of technology and tools that can support a head start on executing a migration roadmap in collaboration with this community of interest.

Scope

There is currently no inventory that can guide updates to standards, guidelines, regulations, hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications that employ cryptography that meets the need to accelerate migration to quantum-resistant cryptography. As a starting point for expeditiously discovering where updates to quantum-resistant cryptography will be required, NIST is planning:

- discovery of all instances where NIST Federal Information Processing Standards (FIPS), 800-series Special Publications (SPs), and other guidance will need to be updated or replaced;
- discovery of which standards from the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Institute of Electrical and Electronics Engineers (IEEE), industry groups like the Trusted Computing Group, and other standards developing organizations will need to be updated or replaced; and
- discovery of which Internet Engineering Task Force (IETF) Request for Comments (RFCs) and other networking protocol standards will need to be updated or replaced.

Implementation of quantum-safe algorithms requires identifying hardware and software modules, libraries, and embedded code currently used in an enterprise to support cryptographic key establishment and management underlying the security of cryptographically-protected information and access management processes, as well as provide the source and content integrity of data at rest, in transit, and in use.

The initial scope of this project is to demonstrate the discovery tools that can provide automation assistance in identifying where and how public-key cryptography is being used in hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications employed in data centers on-premises or in the cloud and distributed compute, storage, and network infrastructures. The recommended project will engage industry in demonstrating use of automated discovery tools to identify all instances of public-key algorithm use in an example network infrastructure's computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms. The algorithm employed and the use for which the algorithm is employed would be identified for each affected infrastructure component.

Once the public-key cryptography components and associated assets in the enterprise are identified, the next element of the scope of the project is to prioritize those components that need to be considered first in the migration using a risk management methodology informed by "Mosca's Theorem" and other recommended practices.

Michele Mosca's theorem in *Cybersecurity in an era with quantum computers: will we be ready?* (https://eprint.iacr.org/2015/1075) says that we need to start worrying about the impact of quantum computers when the amount of time that we wish our data to be secure for (X), added to the time it will take for our computer systems to transition from classical to post-quantum (Y), is greater than the time it will take for quantum computers to start breaking existing quantum-susceptible encryption protocols—or when X + Y > Z.

Finally, the project will provide systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across the different types of assets and supporting underlying technology. For example:

- Each enterprise that produces, supports, or uses public-key cryptography might conduct an inventory to determine what systems and components use public-key cryptography and how the cryptography is used to protect the confidentiality or integrity of information being exchanged, stored, or used to control processes (both information technology and operational technology processes.) Examples include code signing platforms, public-key infrastructure, and data security systems.
- At the same time, quantum-vulnerable information stored and/or exchanged within the enterprise and with customers and partners might be categorized with respect to criticality, disclosure sensitivity, and the consequences of unauthorized and undetected modification.
- Enterprises might also work with government and industry to identify emerging quantum-resistant cryptographic standards and products, their technical and operational characteristics, and their anticipated timeframe for availability to replace quantum-vulnerable systems and components.
- Enterprises might work with public and private sector experts and providers to implement the emerging quantum-resistant crypto algorithms into protocols and technology.

- Enterprises might then work with public and private sector experts and providers to identify any technical constraints that their cryptographically dependent systems impose on replacement systems and components, and to resolve any incompatibilities.
- Enterprises should also work with service providers, partners, and customers to coordinate adoption of technical solutions as necessary to maintain interoperability and to satisfy existing agreements regarding the security of information content and continuity of information distribution.
- Enterprises might then be able to work with their technology suppliers to establish a procurement process consistent with enterprise priorities and plans.

Assumptions & Challenges

The discovery of new cryptographic weaknesses or advances in the technologies supporting cryptanalysis often lead to the need to replace a legacy cryptographic algorithm. The advent of quantum computing technology will compromise many of the current cryptographic algorithms, 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.

Many information systems lack *crypto agility*. That is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure. As a result, an organization may not possess complete control over its cryptographic mechanisms and processes so that they can make accurate alterations to them without involving intense manual effort.

The replacement of algorithms generally requires the following first steps:

- identifying the presence of the legacy algorithms
- understanding the data formats and application programming interfaces of cryptographic libraries to support necessary changes and replacements
- discovering the hardware that implements or accelerates algorithm performance
- determining operating system and application code that uses the algorithm
- identifying all communications devices with vulnerable protocols
- identifying cryptographic protocol dependencies on algorithm characteristics

Once an enterprise has discovered where and for what it is employing public-key cryptography, the organization can determine the use characteristics, such as:

- current key sizes and hardware/software limits on future key sizes and signature sizes
- latency and throughput thresholds
- processes and protocols used for crypto negotiation
- current key establishment handshake protocols
- where each cryptographic process is taking place in the stack
- how each cryptographic process is invoked (e.g., by a call to a crypto library, using a process embedded in the operating system, by calling to an application, using cryptography as a service)
- whether the implementation supports the notion of crypto agility
- whether the implementation may be updated through software

- supplier(s) and owner(s) of each cryptographic hardware/software/process
- source(s) of keys and certificates
- contractual and legal conditions imposed by and on the supplier
- whether the use of the implementation requires validation under the Cryptographic Module Validation Program
- the support lifetime or expected end-of-life of the implementation, if stated by the vendor
- intellectual property impacts of the migration
- sensitivity of the information that is being protected

The new algorithms will likely not be drop-in replacements. They 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.

Once the replacement algorithms are selected, other operational considerations to accelerate adoption and implementation across the organization include:

- developing a risk-based approach that takes into consideration security requirements, business operations, and mission impact
- developing implementation validation tools
- identifying cases where interim (e.g., hybrid) implementations are necessary to maintaining interoperability during migration.
- updating the processes and procedures of developers, implementers, and users
- establishing a communication plan to be used both within the organization and with external customers and partners
- identifying a migration timeline and the necessary resources
- updating or replacing security standards, procedures, and recommended practice documentation
- specifying procurement requirements to acquire quantum-safe technology
- providing installation, configuration, and administration documentation
- testing and validating the new processes and procedures

Background

Cryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. Cryptographic technologies include a broad range of protocols, schemes, and infrastructures, but they rely on a relatively small collection of cryptographic algorithms. Cryptographic algorithms are the information transformation engines at the heart of these cryptographic technologies.

Cryptographic algorithms are mathematical functions that transform data, generally using a variable, or key, to protect information. The protection of these key variables is essential to the continued security of the protected data. In the case of symmetric cryptographic algorithms, the same key is used by both the originator and recipient of cryptographically protected information. Symmetric keys must remain secret to maintain confidentiality; anyone with the key can recover the unprotected data. Asymmetric algorithms require the originator to use one key and the recipient to use a different but related key. One of these asymmetric keys (the private key) must be kept secret, but the other key (the public key) can be made public without degrading the security of the cryptographic process. These asymmetric algorithms are commonly called public-key algorithms.

Symmetric algorithms offer efficient processing for confidentiality and integrity, but key management (establishing and maintaining secrets known only to the communicating parties) poses a challenge. Symmetric algorithms offer weak proofs of origin since either party to an exchange can calculate the transformation. Asymmetric algorithms generally require more processing operations and time than are practical for providing confidentiality protection for more than very small volumes of data. However, use of these algorithms is feasible for cryptographic key establishment and digital signature processes. In the case of public-key cryptography, one of the keys in a pair can be made public and distribution of private keys is not needed. Asymmetric key algorithms can be used to establish pairwise keys and authenticate an entity and/or data source in many-to-many communications without demanding a secret channel for key distribution. As a result, most cryptographic entity or data source authentication and key establishment functions use public-key cryptography.

From time to time, the discovery of a cryptographic weakness, constraints imposed by dependent technologies, or advances in the technologies that support cryptanalysis make it necessary to replace a legacy cryptographic algorithm. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. While some components of some systems tend to be replaced by improved components on a relatively frequent basis (e.g., cell phones), other components are expected to remain in place for a decade or more (e.g., components in electricity generation and distribution systems). Communications interoperability and records archiving requirements introduce additional constraints on system components. As a general rule, cryptographic algorithms cannot be replaced until all components of a system are prepared to process the replacement. Updates to protocols, schemes, and infrastructures must often be implemented when introducing new cryptographic algorithms. Consequently, algorithm replacement can be extremely disruptive and often takes decades to complete.

Continued progress in the development of quantum computing, a technology required to support cryptanalysis using Shor’s algorithm, foreshadows a particularly disruptive cryptographic transition. All widely used public-key cryptographic algorithms are vulnerable to attacks based on Shor’s algorithm, but the algorithm depends upon operations that can only be achieved by a large-scale quantum computer. Practical quantum computing, when available to cyber adversaries, will break the security of nearly all modern public-key cryptographic systems.

Consequently, all secret symmetric keys and private asymmetric keys that are now protected using current public-key algorithms and the information protected under those keys will be subject to exposure. This includes all recorded communications and other stored information protected by those public-key algorithms. Any information still considered to be private or otherwise sensitive will be vulnerable to exposure. The same is true with respect to an undetected modification of the information.

Once exploitation of Shor’s algorithm becomes practical, protecting stored keys and data will require re-encrypting them with a quantum-resistant algorithm and deleting or physically securing “old” copies (e.g., backups). Integrity and sources of information will become unreliable unless they are processed or encapsulated (e.g., re-signed or timestamped) using a mechanism that is not vulnerable to quantum computing-based attacks. Nothing can be done to protect the confidentiality of encrypted material that was stored by an adversary before re-processing.

We refer to algorithms that are vulnerable to exploitation by quantum computing mechanisms as *quantum-vulnerable.*

2 DEMONSTRATION SCENARIOS

The quantum-safe cryptography discovery project will demonstrate tools for discovery of quantum-vulnerable cryptographic code or dependencies on such code for several implementation scenarios. Each of the scenarios involves discovery of quantum-vulnerable cryptographic code or dependencies on quantum-vulnerable cryptographic code. Each scenario also addresses some aspect of prioritization for replacement of quantum-vulnerable cryptographic code or elimination of dependencies on quantum-vulnerable cryptographic code. Finally, the scenarios address aspects of remediating deficiencies based on security control dependence on quantum-vulnerable cryptography.

Scenario 1: FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography

- The first step in this scenario involves discovery of FIPS-140 validated hardware and software modules present in the enterprise that employ quantum-vulnerable public-key cryptography.
- This step would be followed by determining the uses of each module (e.g., symmetric key wrapping, digital signature).
- Where the module is used to protect specific data sets or processes, an assessment of the criticality of the protected information or process should follow. Based on the purposes for which the module is used and what it protects, prioritize the identified modules for replacement.
- Since not all modules will be able to be replaced within the same timeframe due to availability, validation status, or other considerations, a replacement availability schedule will be developed that accommodates a staged or multiple step replacement process. Not all replacements should necessarily be made using new public-key algorithms. In some cases, use of a keyed hash, for example, may accomplish the same purpose with a module that is both applicable and available sooner. In other cases, high-priority components will not have near-term replacements, or the replacements may have interface or performance characteristics that conflict with system requirements. In such cases, compensating controls may be considered.
- The result of this scenario will be an identified set of quantum-vulnerable components, identification of priorities for replacement based on the documented risk assessment, and the migration/compensation strategy identified for each component (with estimated timeline).

Scenario 2: Cryptographic libraries that include quantum-vulnerable public-key cryptography

- This scenario has as its initial step identifying a set of cryptographic libraries that are commonly used in development of cryptographic software.
- This representative set of libraries will then be reviewed to identify the presence of calls to routines associated with quantum-vulnerable public-key algorithms.

- The libraries will also be reviewed to determine whether they also include algorithms or supporting components for quantum-resistant algorithms that were selected for standardization by the NIST post-quantum cryptography standardization process.
- Where a library does not include support for a NIST-selected algorithm, the library will be identified as such and a recommendation will be made regarding inclusion of one or more NIST-selected algorithms that fulfill one or more functions of the quantum-vulnerable routines that are included in the library.
- Where a library does include support for a NIST-selected algorithm, a recommendation will be made to determine that the algorithm or algorithmic element supports a correct implementation of the NIST-selected algorithm.
- Based on collaborator input, an attempt will be made to identify the most commonly called libraries.
- The result of this scenario will be identification of commonly employed cryptographic libraries that support only quantum-vulnerable algorithms, identification of cryptographic libraries that support one or more NIST-selected algorithms, and notes identifying algorithms/modes selected, issues associated with correct support for the quantum-resistant algorithms, and flagging of those libraries that have known malware or other security-relevant coding flaws.

Scenario 3: Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography

- The initial step in this scenario is identification and selection of example cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography. Applications supporting information exchange protocols such as Transport Layer Security (TLS) will be included, as well as those supporting critical operating system and infrastructure processes including financial systems and infrastructure control systems.
- Second, the team will identify the cryptographic function or functions supported by the quantum-vulnerable algorithm(s) in each cryptographic application and cryptographic support application (e.g., key agreement, key wrapping, digital signature, authentication). As part of this step, the team will flag system security dependencies on the availability of each cryptographic application and cryptographic support application (e.g., subject identification, access authorization, confidentiality of data in transit and/or at rest).
- The third step will be to identify any information exchange and processing protocols that are dependent on each cryptographic application and cryptographic support application being examined.
- Fourth, the team will identify the information technology or operational technology environment in which each cryptographic application and cryptographic support application is being used and will categorize the FIPS 199 [4] risk associated with the failure of or unavailability of the application. The team will identify any compensating controls that might be used to provide the needed control in lieu of an unavailable or non-functional application.
- The team will next identify algorithm characteristics required by or limited by each cryptographic or cryptographic support application examined (e.g., key size, block size, mode of operation supported, error tolerance, latency, throughput).

- The team will then, based on the algorithms remaining under consideration by the NIST post-quantum standardization process, identify which, if any, candidate algorithms meet the algorithm characteristics requirement for each application and flag those applications for which no candidate algorithm can meet a requirement.
- Finally, the result of the scenario will be a listing of the applications prioritized by risk category, functional criticality, and the number/scope of dependent systems and processes. For each application, candidate replacement algorithms and/or compensating controls will be identified. Those cases where no suitable algorithm or compensating control can be identified will be flagged.

Scenario 4: Embedded quantum-vulnerable cryptographic code in computing platforms

- The initial step in this scenario will be to identify one or more operating system environments (e.g., Microsoft Windows, Red Hat Enterprise Linux, macOS, iOS, Android) for which quantum-vulnerable cryptography is embedded in operating system code, access control utility code, cryptographic integrity applications and mechanisms, and code embedded in identity and access management systems and applications.
- For each operating system environment, determine and document how widely it is used and cite examples of dependent enterprises and infrastructures.
- For each operating system environment identified, the team will employ automated tools to identify the quantum-vulnerable cryptographic code.
- For each instance identified, the team will assess the criticality of the code for the ability of the system to function (e.g., are there settings that don't require the code instance, what is the security consequence of not invoking the code).
- For each instance of quantum-vulnerable cryptographic code, the team will identify algorithm characteristics that are required by or limited by the code (key size, block size, mode of operation supported, error tolerance, latency, throughput, etc.).
- The team will then, based on the algorithms remaining under consideration by the NIST post-quantum algorithm standardization process, identify which, if any, candidate algorithms meet the algorithm characteristics requirement for each code instance and flag those instances for which no candidate algorithm can meet a requirement.
- The result of this scenario will be a list of all quantum-vulnerable public-key cryptographic code identified, and for each code instance, the following information will be provided:
    - location and purpose of the code
    - candidate NIST algorithms that were identified as suitable for replacing the quantum-vulnerable code and projected impact of the replacement on performance of the intended system functionality (include replacements' characteristics such as rounds, key size, block size, etc.)
    - consequence of simply deleting the code and any mitigation approach that might be recommended
    - priority of the recommended replacement or other mitigation
    - flagging cases where neither replacement nor deletion appears to be practical, and failure to do either will impair operating system functionality and/or security

Scenario 5: Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms

- The team will conduct a search for references to quantum-vulnerable public-key algorithms in communications and network standards used by U.S.-based service providers and representative enterprises in the financial, healthcare, energy, transportation, and other sectors. Instances will be documented.
- The team will characterize how widespread use of the referenced protocol is and the applications that it supports.
- For each documented reference, the team will identify any limitations or specifications respecting key size, block size, or latency/throughput constraints.
- For each documented reference, the team will then, based on the algorithms remaining under consideration by the NIST post-quantum standardization process, identify which, if any, candidate algorithms satisfy the limitations and specifications and flag those instances for which no candidate algorithm can meet a requirement.
- The result of the scenario will be a list of protocols. The list will be prioritized based on how widespread its application is (the approximate number, size, and impact of users). For each protocol, the following information will be provided:
    - protocol identification
    - organization responsible for maintaining the protocol
    - protocol applications space (by whom it is used, and for what purpose)
    - quantum-vulnerable algorithm(s) referenced by the protocol
- NIST quantum-resistant algorithm candidates potentially suitable to replace the referenced quantum-vulnerable algorithm(s) will be identified
- Flag where no NIST quantum-resistant candidate is potentially suitable to replace the referenced quantum-vulnerable algorithm(s)

All scenarios will address enterprise data center environments which include on-premises data center and hybrid cloud deployment hosted by a third-party data center or a public cloud provider.

3 HIGH-LEVEL ARCHITECTURE

The high-level architecture consists of a typical enterprise environment that connects the NCCoE PQC laboratory hosted in Rockville, Maryland to external sites and cloud resources hosted by the collaborators via the internet. This will enable the collaborators to install discovery tools in the NCCoE laboratory and operate them remotely via virtual private network. Conversely, it will enable staff in the NCCoE laboratory to use tools installed in the laboratory to discover quantum-vulnerable software in remote sites either directly or using cloud services. The NCCoE environment will be able to host physical, virtualized, and containerized workloads. It will provide core infrastructure services like routing, naming, etc.; a set of typical application services like directory, web servers, etc.; and core security services like firewalls. Various typical endpoints will be available to host client-side operating systems, protocols, and applications.

Component List

- General IT components:
    - compute, storage, and network resources necessary to running cryptographic code detection tools
    - cloud services
- Functional security components:
    - the data security component
    - the endpoint security component
    - the identity and access management component
    - the security analytics component
- Devices and network infrastructure components:
    - assets including the devices/endpoints
    - core enterprise resources such as applications/services
    - network infrastructure components
- Approaches and tools for discovering public-key cryptography components in:
    - operating systems
    - application code
    - hardware implementing, controlling, or accelerating crypto functionality
- Approaches and tools for discovering algorithm migration impacts on:
    - communications and network protocols
    - key management protocols, processes, and procedures
    - network management protocols, processes, and procedures
    - business processes and procedures

Desired Security Characteristics and Properties

All candidate quantum-resistant replacements for quantum-vulnerable public-key algorithms should have a security strength at least equivalent to that possessed by the quantum-vulnerable algorithm being replaced, where the security strength of the algorithm being replaced is measured in the absence of quantum computing.

Any suggestion for replacement of a quantum-vulnerable public-key algorithm by a compensating control(s) should be accompanied by an explanation of how the compensating control provides relevant confidentiality and integrity protection commensurate with that currently being provided in the absence of quantum computing.

Any projected performance degradation resulting from a suggested replacement of a quantum-vulnerable public-key algorithm by a NIST candidate quantum-resistant algorithm should be characterized in the project findings.

4 RELEVANT STANDARDS AND GUIDANCE

Here is a list of existing relevant standards and guidance documents.

- Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*
  https://doi.org/10.6028/NIST.FIPS.140-3
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
  https://doi.org/10.6028/NIST.FIPS.199
- *Framework For Improving Critical Infrastructure Cybersecurity*, Version 1.1
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*
  https://doi.org/10.6028/NIST.CSWP.04282021
- NIST Internal Report (NISTIR) 8105, *Report on Post-Quantum Cryptography*
  https://doi.org/10.6028/NIST.IR.8105
- NISTIR 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*
  https://doi.org/10.6028/NIST.IR.8309
- *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management*, Version 1.0
  https://doi.org/10.6028/NIST.CSWP.01162020
- NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
  https://doi.org/10.6028/NIST.SP.800-53r5

APPENDIX A REFERENCES

[1] L. Chen et al., *Report on Post-Quantum Cryptography*, National Institute of Standards and Technology Internal Report (NISTIR) 8105, Gaithersburg, Md., April 2016, 15 pp. Available: https://doi.org/10.6028/NIST.IR.8105

[2] G. Alagic et al., *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST Interagency or Internal Report (NISTIR) 8309, Gaithersburg, Md., July 2020, 39 pp. Available: https://doi.org/10.6028/NIST.IR.8309

[3] W. Barker, W. Polk, and M. Souppaya, *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, NIST Cybersecurity White Paper, Gaithersburg, Md., April 2021, 10 pp. Available: https://doi.org/10.6028/NIST.CSWP.04282021

[4] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard (FIPS) 199, Gaithersburg, Md., February 2004, 13 pp. Available: https://doi.org/10.6028/NIST.FIPS.199

APPENDIX B ACRONYMS

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IR	(NIST) Interagency or Internal Report
ISO	International Organization for Standardization
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
PQC	Post-Quantum Cryptography
RFC	Request for Comments
SP	Special Publication
TLS	Transport Layer Security