Tuesday, June 8, 2021 - 10:00 – 10:20 AM EDT

Getting Ready for Post-Quantum Cryptography

Bill Newhouse
Cybersecurity Engineer
National Institute of Standards and Technology (NIST)
National Cybersecurity Center of Excellence (NCCoE)
william.newhouse@nist.gov

Nick Reese
Senior Cyber Policy Advisor
US Department of Homeland Security
Nicholas.reese@hq.dhs.gov

National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

Migration To Post-Quantum Cryptography (PQC) Project

Bill Newhouse, Cybersecurity Engineer

June 8, 2021

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

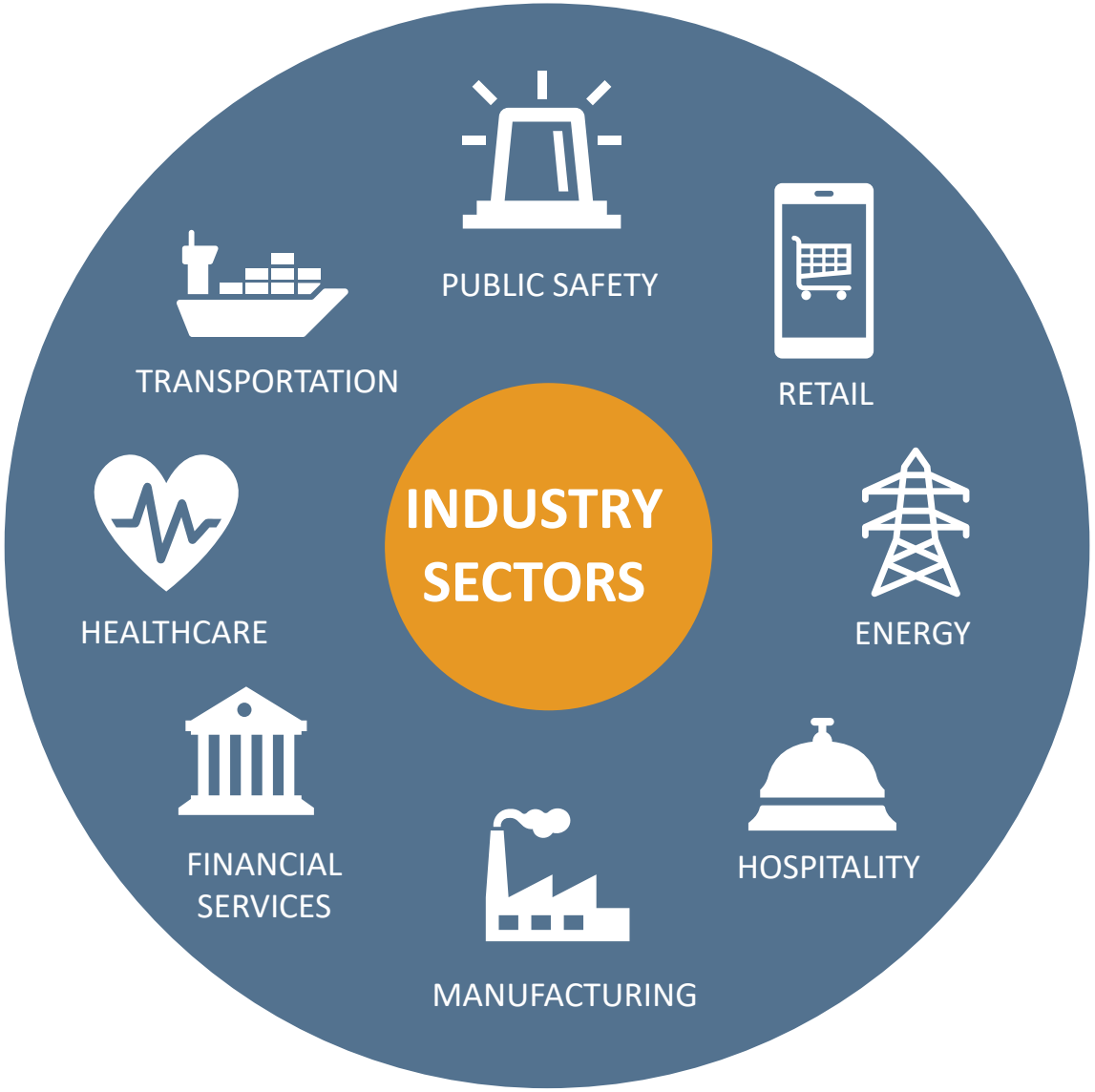
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

About the NCCoE

National Cybersecurity Center of Excellence Mission

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

Securing industry Sectors



- Commerce/Retail
- Energy
- Financial Services
- Healthcare
- Hospitality
- Manufacturing
- Public Safety/First Responder
- Transportation

Providing Building Blocks / Cross Sector Projects

- 5G Security
- Adversarial Machine Learning
- Data Security
- Internet of Things (IoT)
- Mobile Device Security
- Patching the Enterprise
- Supply Chain Assurance
- TLS Server Certificate Management
- Trusted Geolocation in the Cloud
- Zero Trust Architecture
- Post-Quantum Cryptography

NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

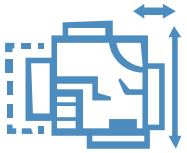
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide detailed guidance including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry



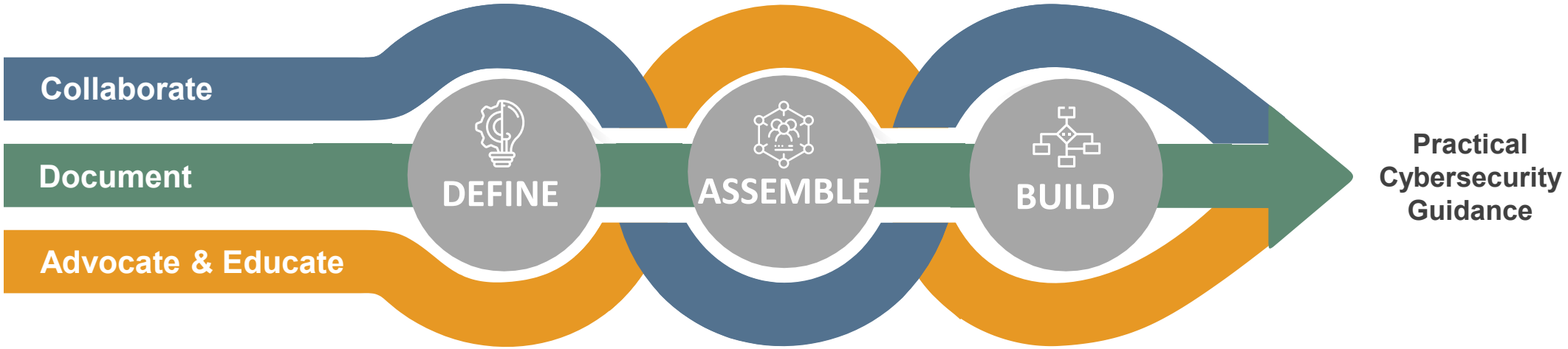
Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

OUR APPROACH



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

About the Migration to PQC Project

NCCOE PQC PROJECT

- Align and complement the NIST PQC standardization activities
- Develop 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
- Deliver white papers, playbooks, and demonstrable implementations for organizations
- Target organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products.

CONSIDERATIONS IN MIGRATING TO PQC ALGORITHMS

- The October 7, 2020 NCCoE-hosted Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms resulted in the following initiatives at the NCCoE:
  - 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.
    - Posted a cybersecurity white paper, *Getting Ready for Post-Quantum Cryptography* to start the discussion.
  - 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.
  - Developed a draft 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.
    - Posted June 4, 2021 on https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography, please submit comments

THE GAP

- 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.

SCOPE

- 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.
- 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.

SCOPE

- 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.

SCOPE

- 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 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

ASSUMPTIONS & CHALLENGES

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

ASSUMPTIONS & CHALLENGES

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

DEMONSTRATION SCENARIO 1

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).

DEMONSTRATION SCENARIO 2

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.

DEMONSTRATION SCENARIO 3

Scenario 3: Cryptographic applications and cryptographic support applications that include or 335 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 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.

DEMONSTRATION SCENARIO 4

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' 397 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

DEMONSTRATION SCENARIO 5

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)

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.

CALL TO ACTION

- Review and provide feedback to the project description https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography
- Join the community of interest to receive updates about the project applied-crypto-pqc@nist.gov
- Consider participating in the project when it is officially announced to contribute your technical expertise and technology

Bill Newhouse

applied-crypto-pqc@nist.gov

Project Description:
https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and PQC Algorithms
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

nccoe.nist.gov

@NISTcyber