DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 210915-0186]

National Cybersecurity Center of Excellence (NCCoE) *Migration to Post-Quantum Cryptography*

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Migration to Post-Quantum Cryptography* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the *Migration to Post-Quantum Cryptography* project. Participation in the project is open to all interested organizations.

DATES: Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to applied-crypto-pqc@nist.gov

or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest template by visiting the website and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is

no longer accepting letters of interest for this project at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography. Organizations whose letters of interest are accepted will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST; a template CRADA can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: William Newhouse via telephone 301-975-0232; by email applied-crypto-pqc@nist.gov; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Migration to Post-Quantum Cryptography* project are available at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the *Migration to Post-Quantum Cryptography* project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography.

Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below, up to the number of participants in each category necessary to carry out this project. When the project has been completed, NIST will post a notice on the *Migration to Post-Quantum Cryptography* project website at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography announcing the completion of the project and informing the public that it is no longer accepting letters of interest for this project. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective: The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which are widely used to protect digital information. Work on the development of quantum-resistant public-key cryptographic standards is underway, and algorithm selection is expected to be completed in the next one to two years (https://csrc.nist.gov/projects/post-

quantum-cryptography). Replacement of cryptographic algorithms is both technically and logistically challenging. It can take years or even decades to complete. In order to address these challenges, the NCCoE is undertaking a practical demonstration of technology and tools that can provide a head start on executing a migration roadmap in collaboration with a public and private sector community of interest.

To meet the need to accelerate migration to quantum-resistant cryptography, the NCCoE *Migration to Post-Quantum Cryptography* project will demonstrate tools for discovery of quantum-vulnerable cryptographic code or dependencies on such code. The tools to be demonstrated provide automation assistance in identifying where and how public-key cryptography is being used in data centers on-premises or in the cloud and distributed compute, storage, and network infrastructures. The project can also contribute to updates to standards, guidelines, regulations, hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications that employ cryptography. The audience for the project includes developers of products that use public-key cryptographic algorithms, integrators of such products, customer organizations that acquire or configure such products, and bodies that standardize protocols that employ or are dependent on public-key cryptographic algorithms.

The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Migration to Post-Quantum Cryptography* project description at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the practical steps needed to implement a cybersecurity reference implementation. Supporting outputs may include playbook, tools, code, and white papers.

Requirements for Letters of Interest: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 3 of the *Migration to Post-Quantum Cryptography* project description at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography and include, but are not limited to:

- 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

Each responding organization's letter of interest should identify how their products help address one or more of the following demonstration scenarios in section 2 of the *Migration to Post-Quantum Cryptography* project description at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography:

- FIPS-140 validated hardware and software modules that employ quantum-vulnerable public-key cryptography
- Cryptographic libraries that include quantum-vulnerable public-key cryptography
- Cryptographic applications and cryptographic support applications that include or are focused on quantum-vulnerable public-key cryptography
- Embedded quantum-vulnerable cryptographic code in computing platforms
- Communication protocols widely deployed in different industry sectors that leverage quantum-vulnerable cryptographic algorithms

Considerations for desired characteristics include:

- 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.

In their letters of interest, responding organizations need to acknowledge the importance of and commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components.
2. Support for development and demonstration of the *Migration to Post-Quantum Cryptography* project, which will be conducted in a manner consistent with the most recent version of the following standards and guidance: FIPS 200, SP 800-37, SP 800-52, SP 800-53, SP 800-63, and SP 1800-16. Additional details about the *Migration to Post-Quantum Cryptography* project are available at https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography.

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium CRADA in the development of the *Migration to Post-Quantum Cryptography* project. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations,

NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the *Migration to Post-Quantum Cryptography* project. These descriptions will be public information.

Under the terms of the consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the *Migration to Post-Quantum Cryptography* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the solutions that address *Migration to Post-Quantum Cryptography* can enhance security capabilities that provide assurance of mitigation of identified risks while continuing to meet industry sectors' compliance requirements. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website https://nccoe.nist.gov/.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2021-22223 Filed: 10/12/2021 8:45 am; Publication Date: 10/13/2021]