DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 210826-0169]

National Cybersecurity Center of Excellence (NCCoE) *Automation of the Cryptographic Module Validation Program (CMVP)*

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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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-testing@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 https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it will no longer accept letters of interest for this project at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation. 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: Apostol Vassilev via phone (301) 975-3221 or email applied-crypto-testing@nist.gov; by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Automation of the Cryptographic Module Validation Program (CMVP)* project are available at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.

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 *Automation of the Cryptographic Module Validation Program (CMVP)* project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.

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/applied-cryptography/cmvp-automation 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 *Automation of the Cryptographic Module Validation Program (CMVP)* project website at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation announcing the completion of the project and informing the public that it will no longer accept 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 interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above).

Objective: The Cryptographic Module Validation Program (CMVP) validates third-party assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*. Current industry cryptographic product development, production, and maintenance processes place significant emphasis on time-to-market efficiency. A number of elements of the validation process are manual in nature, and the period required for third-party testing and government validation of cryptographic modules is often incompatible with industry requirements. The purpose of the project is to demonstrate the value and practicality of automation to improve the efficiency and timeliness of CMVP operation and processes. 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 *Automation of the Cryptographic Module Validation Program (CMVP)* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-

cryptography/cmvp-automation. 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.

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 *Automation of the Cryptographic Module Validation Program (CMVP)* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation and include, but are not limited to:

- Validation authority server
- ACV proxy server
- ACV client
- Hardware or software cryptographic modules
- Host processors for software cryptographic modules
- Network devices supporting web-based exchange of information in JSON format
- Harnesses for integration of ACV clients with hardware or software cryptographic modules
- Automated cryptographic module testing expertise

Each responding organization's letter of interest should identify how its products help address one or more of the following desired characteristics and properties in section 1 of the *Automation of the Cryptographic Module Validation Program (CMVP)* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation:

- Support necessary schemas and protocols for evidence submission and validation for a scalable application programming interface (API) based architecture
- Support standard tests for the functional tests of specific classes of technologies (e.g., software modules) and corresponding reporting of functional and non-functional security requirements
- Be compatible with an infrastructure required to support a new automated validation program architecture
- Include reusable test harnesses for test automation for different types of modules within the program architecture
- Support maintaining validation within a changing operational environment
- Support validation in third-party operational environments (e.g., cloud providers, contracted environments)
- Support identification of positive and negative impacts that the new automation program may have on cryptographic product development, production, integration, and testing organizations, including lessons learned
- Contribute to recommend policies and best practices for the automated validation scope in appropriate NIST documents
- Support a roadmap for migrating organizations and their customers from the current human-effort-centric CMVP to the new automated program, including recommended practices based on lessons learned
- Broadly support improvements in cryptographic modules across all vendors participating in the CMVP through voluntary sharing of test data (e.g., seeds or test vectors) that result in failures to improve regression testing for module vendors

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 Automation of the Cryptographic Module Validation Program (CMVP) project, which will be based on the most recent versions of FIPS 140, SP 800-140, and Handbook (HB) 150-17 and 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 *Automation of the Cryptographic Module Validation Program (CMVP)* project are available at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.

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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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. 2021-18868 Filed: 8/31/2021 8:45 am; Publication Date: 9/1/2021]