This document is scheduled to be published in the
Federal Register on 03/26/2020 and available online at
federalregister.gov/d/2020-06264, and on **govinfo.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 200313-0079]

National Cybersecurity Center of Excellence (NCCoE) Validating the Integrity of Computing Devices Building Block

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 products and technical expertise to support and demonstrate security platforms for the Validating the Integrity of Computing Devices 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 Validating the Integrity of Computing Devices project. Participation in the building block 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 supplychain-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the process set forth in the SUPPLEMENTARY INFORMATION section of this notice will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: https://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Nakia Grayson via email to supplychain-nccoe@nist.gov ; by telephone 301-975-0200 or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Validating the Integrity of Computing Devices project are available at https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance.

SUPPLEMENTARY INFORMATION: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST. Letters of interest will be accepted on a first come, first served basis. When the building block has been

completed, NIST will post a notice on the NCCoE Validating the Integrity of Computing Devices website at https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

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 Validating the Integrity of Computing Devices project. The full building block can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance.

Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest template, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the building block 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 building block. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above). NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Building Block Objective: The objective of this project is to produce example implementations to demonstrate how organizations can verify that the internal components of their purchased computing devices are genuine and have not been altered during the manufacturing and distribution process. Additionally, this project will demonstrate how to inspect the processes that verify that the components in a computing device match the attributes and measurements declared by the manufacturer. This project is intended to help organizations decrease the risk of a compromise to products in a

specific stage of their supply chain, which may result in risks to the end user. A detailed description of the Validating the Integrity of Computing Devices project is available at: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance.

Requirements: 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 Validating the Computing Devices project description (for reference, please see the link in the Process section above) and include, but are not limited to:

- Computing devices, including laptops, servers, and mobile devices
- Configuration management software
    - vulnerability scanning
    - detection
    - patch management
    - version control
    - synchronization
    - firmware
- Asset inventory software
    - asset management

    - asset discovery

- Security information and event management (SIEM)
    - event detection
    - log management
    - exfiltration activity
    - unauthorized activity
    - anomalous activity
- Certificate authority

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 3 of the Validating the Integrity of Computing Devices project (for reference, please see the link in the PROCESS section above):

1. Use verifiable and authentic artifacts that manufacturers produce during the manufacturing and integration process
2. Detect malicious component swaps of the computing device
3. Manage the automation process when accepting the delivery of a computing device and throughout the operational lifecycle of the device
4. Inspect computing devices to verify that the components in a delivered (or in-use) system computing device match the attributes and measurements declared by the manufacturer

Responding organizations need to understand and, in their letters of interest, 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 Validating the Integrity of Computing Devices project for multiple sectors in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800-53, SP 800-147B, SP 800-155 and SP 800-161. Additional details about the Validating the Integrity of Computing Devices project are available at: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance.

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 Validating the Integrity of Computing Devices 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 Validating the Integrity of Computing Devices 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 Validating the Integrity of Computing Devices' capability will be announced on the NCCoE Web site at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome of the demonstration is to improve supply chain assurance within the enterprise. 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 Web site https://nccoe.nist.gov/.

Kevin A. Kimball,
Chief of Staff.
[FR Doc. 2020-06264 Filed: 3/25/2020 8:45 am; Publication Date: 3/26/2020]