Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: [180301235-8235-01]

National Cybersecurity Center of Excellence (NCCoE) Data Integrity 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 two data integrity projects within the Data Integrity Building Block. The two projects are 1) Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events and 2) Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. 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 Data Integrity Building Block. Participation in the building block is open to all interested organizations and organizations may participate in one or both data integrity projects.

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 di-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 separate consortium Cooperative Research and Development Agreement (CRADA) with NIST for each Data Integrity Building Block project. An NCCoE consortium CRADA template can be found at: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Timothy McBride via email to timothy.mcbride@nist.gov; by telephone 301.975.0214; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Data Integrity Building Block are available at https://nccoe.nist.gov/projects/building-blocks/data-integrity .

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. Parties interested in participating in both data integrity projects must submit a separate letter of interest for each data integrity project. When the building block has been completed, NIST will post a notice announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block on the NCCoE Data Integrity Building Block website at https://nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect for Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, and at

https://nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond for Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.

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 Data Integrity Building Block. The full building block can be viewed at: https://nccoe.nist.gov/projects/building-blocks/data-integrity.

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: Establish tools and procedures to defend, detect, and respond to data integrity events.

A detailed description of the Data Integrity Building Block is available at: https://nccoe.nist.gov/projects/building-blocks/data-integrity.

Requirements: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Responding organizations must submit a separate letter of interest and sign a separate consortium CRADA for each project the responding organization is interested in joining. 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 each of the data integrity projects (1) Data Integrity: Identifying and Protecting Assets Against Ransomware and

Other Destructive Events, and 2) Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events) (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- For Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events:
    - Secure storage
    - File integrity checking mechanisms backup capability for databases, VMs, and file systems
    - Vulnerability management and identification software
        - Signature based vulnerability detection
        - Behavior based vulnerability detection
        - Zero-day vulnerability detection
    - Log collection software
    - Asset inventory software
        - Asset management
        - Asset discovery
    - Maintenance software (including software versioning and distribution technology)
        - Software versioning
        - Software distribution
        - Update verification

- For Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
    - Integrity monitoring
    - Event detection
        - Malicious software detection

    - Unauthorized activity detection
    - Anomalous activity detection
- Logging and data correlation software
- Reporting capability
- Vulnerability management
- Forensics/analytics tools
- Mitigation and containment software

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 each of the Data Integrity projects (1) Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, and 2) Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events) (for reference, please see the link in the PROCESS section above):

1. For Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events:
    - Inventory assets both part of the enterprise and the solution itself
    - Be secure against integrity attacks against hosts
    - Be secure against integrity attacks that occur on the network
    - Support secure backups
    - Provide protected network and remote access
    - Provide audit capabilities
2. For Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events:
    - Detect unauthorized or malicious activity on the network
    - Detect unauthorized or malicious mobile code (such as web technologies like JavaScript, VBScript, and other code executed but loaded from an external site)

- Detect unauthorized or malicious executables
- Detect unauthorized or malicious behavior
- Report unauthorized or malicious activity on the network
- Report unauthorized or malicious mobile code events
- Report unauthorized or malicious executables
- Report unauthorized or malicious behavior
- Analyze the impact of unauthorized or malicious activity on the network
- Analyze the impact of unauthorized or malicious mobile code events
- Analyze the impact of unauthorized or malicious executables
- Analyze the impact of unauthorized or malicious behavior
- Mitigate the impact of unauthorized or malicious activity on the network
- Mitigate the impact of unauthorized or malicious mobile code events
- Mitigate the impact of unauthorized or malicious executables
- Mitigate the impact of unauthorized or malicious behavior
- Contain unauthorized or malicious activity on the network
- Contain unauthorized or malicious mobile code events
- Contain unauthorized or malicious executables
- Contain unauthorized or malicious behavior

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 Data Integrity Building Block in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201 (for the Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events Project), SP 800-53, FIPS 140-2, SP 800-37, SP 800-57, SP 800-61, SP 800-83, SP 800-150, SP 800-160, and SP 800-184.

Additional details about the Data Integrity Building Block are available at: https://nccoe.nist.gov/projects/building-blocks/data-integrity.

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 Data Integrity Building Block. 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 Data Integrity Building Block. 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 Data Integrity Building Block capability will be announced on the NCCoE Web site at least two weeks in advance at http://nccoe.nist.gov/. The expected outcome of the demonstration is to improve data integrity 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 http://nccoe.nist.gov/.

Kevin A. Kimball
Chief of Staff

[FR Doc. 2018-08829 Filed: 4/26/2018 8:45 am; Publication Date: 4/27/2018]