Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 160429381-6381-01]

National Cybersecurity Center of Excellence 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 the Data Integrity Building Block. 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 Data Integrity Building Block is open to all interested organizations.

DATES: 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. 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]. When the Data Integrity Building Block has been completed, NIST will post a notice on the NCCoE Data Integrity Building Block website at https://nccoe.nist.gov/projects/building_blocks/data_integrity

announcing the completion of the Data Integrity Building Block and informing the public that it will no longer accept letters of interest for this Data Integrity Building Block.

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 Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: Don Tobin via email to donald.tobin@nist.gov, by telephone 301-975-0239, 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:

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 Data Integrity 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 Data Integrity 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 Data Integrity 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.

Data Integrity Building Block Objective: The goal of this project is to mitigate the impacts of data corruption when recovering systems from backup storage. The solution will provide guidance for incorporating post-attack data corruption detection and recovery strategies into a corporate IT architecture. The project will explore methods to address the integrity of commodity components (operating systems, applications, and software configurations), custom applications, and data (database and files) and provide corruption indicators and activity logs to the security analysts to identify the malicious activity. It will produce an architecture that includes components that will integrate notification of data corruption events coupled with approaches to automate recovery from such 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. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in the High-level Architecture section of the Data Integrity Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- File integrity monitors

- File versioning systems
- File integrity testing capabilities
- User activity monitoring tools
- Configuration management systems
- Database rollback tools
- Virtual machine integrity/snapshots/versioning capabilities
- Versioning file systems
- Journaling file systems

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in the High Level Architecture section of the Data Integrity Building Block (for reference, please see the link in the PROCESS section above):

- Automated data corruption testing
- Automated data corruption detection
- Automated data corruption event logging
- Secure data integrity monitoring and alerting information (checksums, off-site, hard-copy)
- Automated detection and reporting of all file modifications / creations / deletions
- Automated detection and reporting of all database modifications / creations / deletions
- Automated correlation of file changes and users

- Automated user activity recording
- Automated anomalous user activity detection
- Automated configuration management monitoring

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 Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

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 Kimball
NIST Chief of Staff
[FR Doc. 2016-12860 Filed: 5/31/2016 8:45 am; Publication Date: 6/1/2016]