Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 200113-0014]

National Cybersecurity Center of Excellence (NCCoE) *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing Sector

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 *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector. 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 Manufacturing sector program. Participation in the use case 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 Manufacturing_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://www.nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: Michael Powell via email at michael.powell@nist.gov; by telephone 301-975-0310; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Manufacturing sector program are available at https://www.nccoe.nist.gov/projects/use-cases/Manufacturing.

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 use case has been completed, NIST will post a notice on the NCCoE Manufacturing sector program website at https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

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 CRADA to provide products and technical expertise to support and demonstrate security platforms for the *Protecting Information and System Integrity in Industrial Control System Environments* project for the Manufacturing sector. The full use case can be viewed at: https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics.

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 use case 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 use case. 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.

In March 2016, NIST issued a similar call for collaboration for a Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection use case which can be found here: https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics. This collaborative project was originally intended to yield a NIST Cybersecurity Practice Guide, but instead resulted in the publication of NISTIR 8219, Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection, https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf. NIST

anticipates that the collaborators who contributed to development of NISTIR 8219 will also participate in this use case.

Use Case Objective: The objectives of this project are to provide a proposed approach to prevent, mitigate, and detect threats from cyber attacks or insider threats within a Manufacturing industrial control system (ICS) environment, and demonstrate how the commercially available technologies deployed in this build provide cybersecurity capabilities that Manufacturing organizations can use to secure their operational technology (OT) systems.

A detailed description of the *Protecting Information and System Integrity in Industrial Control System Environments* is available at: https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics.

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 6 of the *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing use case (for reference, please see the link in the Process section above) and include, but are not limited to:

- ICS application white-listing tools
- ICS behavioral anomaly detection tools
- security incident and event monitoring

- malware detection and mitigation
- change control management
- access control
- file-integrity-checking mechanisms
- user authentication and authorization

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 6 of the *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing use case (for reference, please see the link in the Process section above):

1. tracking of approved software applications that are permitted to be present and active on the network
2. continuous monitoring of a network for unusual events or data packet trends process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time OT environment
3. detection of malicious software designed to cause damage to a computer, server, or computer network
4. monitoring for unapproved changes, that all changes are documented, and that services are not unnecessarily disrupted
5. validation of access to the ICS network by authenticated users
6. validation of operating system and application software file integrity

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 *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector use case in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, and SP 800-53.

Additional details about the *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector use case are available at: https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics.

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 *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector capability. 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 to the Manufacturing community. 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 *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector use case. 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 *Protecting Information and System Integrity in Industrial Control System Environments* for the Manufacturing sector capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome of the demonstration is to improve security to Manufacturing environments by demonstrating how Manufacturing organizations can take a comprehensive approach to protecting the data integrity of their industrial control systems. 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/.

Kevin A. Kimball,
Chief of Staff.

[FR Doc. 2020-02436 Filed: 2/6/2020 8:45 am; Publication Date: 2/7/2020]