Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

RIN: 0693-XC072

Docket No.: 170221188-7188-01

National Cybersecurity Center of Excellence (NCCoE) *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* 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 the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems*. 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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* use case 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 of the project, but no earlier than [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the use case has been completed, NIST will post a notice on the NCCoE Manufacturing sector program website at https://nccoe.nist.gov/projects/use_cases/manufacturing announcing the completion of the use case and informing the public that it will no longer accept letters of interest for the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* use case.

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 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: Jim McCarthy via email at James.McCarthy@nist.gov; by telephone at 301-975-0228; 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 can be found here: https://nccoe.nist.gov/projects/use_cases/manufacturing.

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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* for the Manufacturing sector. The full *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* use case can be viewed here:

https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems.

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 opportunities 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.

Capabilities Assessment for Securing Manufacturing Industrial Control Systems

Objective: This is the first of a four-part series designed to provide businesses with the information they need to establish an anomaly detection and prevention capability in their own environments. This project will be using commercially available hardware/software

deployed on an established lab infrastructure. The goal of this project is to provide businesses with a cybersecurity example solution that can be implemented or that can inform improved cybersecurity in their manufacturing processes. Implementing behavioral anomaly detection tools provides a key security component in sustaining business operations, particularly those based on Industrial Control Systems (ICS). One of the ways to disrupt operations is to introduce anomalous data into a manufacturing process, whether deliberately or inadvertently. Although the example solution will focus on cybersecurity, our example solution may also produce residual benefit to manufacturers for detecting anomalous conditions not related to security. A detailed description of the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* Project is available at https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems.

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 Architectures section of the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* use case (for reference, please see the link in the Process section above) and include, but are not limited to:

- ICS behavioral anomaly detection tools
- Human Machine Interfaces (HMIs)
- Programmable Logic Controllers (PLCs)
- Security Information and Event Management (SIEM) platform

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 Architectures section of the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* use case (for reference, please see the link in the Process section above):

- Detection of anomalous conditions
- Process and/or device damage prevention
- SIEM-based alerting/alarming capability

In their letters of interest, responding organizations need to understand 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; and
2. Support for development and demonstration of the *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* for the Manufacturing sector use case 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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* for the Manufacturing sector use case are available at: https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems. 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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* 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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* 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 *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* for the Manufacturing sector 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 security to manufacturing environments that employ the use of ICS, and subsequent adoption of behavioral anomaly detection tools by industry. Participating organizations will benefit from the knowledge that their products are interoperable with other participants' offerings.

For additional information on NCCoE governance, business processes, and operational structure, visit the NCCoE website http://nccoe.nist.gov/.

Kevin Kimball
NIST Chief of Staff
[FR Doc. 2017-05759 Filed: 3/22/2017 8:45 am; Publication Date: 3/23/2017]