DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 220208-0264]

National Cybersecurity Center of Excellence (NCCoE) *Responding to and Recovering from a Cyberattack: Cybersecurity 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 letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* 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 *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project. Participation in the project 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. Interested parties can access the letter of interest request by visiting https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack and completing the letter of interest webform. NIST will announce the completion

of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack. 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 an NCCoE consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: https://www.nccoe.nist.gov/publications/other/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: Michael Powell via telephone at 301-975-0310; by email at manufacturing_nccoe@nist.gov; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project are available at https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack.

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) and Operational Technology (OT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT and OT assets, the NCCoE will enhance trust in U.S. IT and OT communications, data, and storage systems; reduce risk for companies and individuals using IT and OT 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 an NCCoE Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project. The full project can be viewed at: https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack.

Interested parties can access the request for a letter of interest template by visiting the project website at https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project 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 project. When the project has been completed, NIST will post a notice on the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project website at https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack announcing the next phase of the project and informing the public that it will no longer accept letters of interest for this project. There may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective: This project is focused on responding to and recovering from a cyberattack within an Industrial Control System (ICS) environment. Manufacturing organizations rely on ICS to monitor and control physical processes that produce goods for public consumption. These same systems are facing an increasing number of cyberattacks resulting in a loss of production from destructive malware, malicious insider activity, or honest mistakes. This creates the imperative for organizations to be able to quickly, safely, and accurately recover from an event that corrupts or destroys data (e.g., database records, system files, configurations, user files, application code).

The purpose of this NCCoE project is to demonstrate how to operationalize the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST *Cybersecurity Framework*) Functions and Categories. Multiple systems need to work together to recover equipment and restore operations when data integrity is compromised. This project explores methods to effectively restore corrupted data in applications and software configurations as well as custom applications and data. The NCCoE—in collaboration with members of the business community and vendors of cybersecurity solutions—will identify standards-based, commercially available, and open-source hardware and software components to design a manufacturing lab environment that can address the challenge of responding to and recovering from a cyberattack in an ICS environment.

The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project description available at: https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special

Publication 1800 series, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Requirements for Letters of Interest: 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 5 of the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project description available at: https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack and include, but are not limited to:

Core Components:

- Event reporting (Detection)
    - Network event detection
    - Behavior Anomaly Detection
    - Endpoint detection and response (EDR) (Host based detection)
- Event management
    - Event/Alert notification
    - Case creation
- Log review
    - Collection
    - Aggregation
    - Correlation
- Forensic analysis
    - Categorize incidents based on MITRE ATT&CK for ICS tactics and techniques
    - Understand impact
    - Determine root cause
    - Determine extent of compromise
- Incident handling and response
    - Containment of the incident

- Eradication of artifacts of incident
- Recovery
    - Restoration of systems
    - Verification of restoration

To demonstrate the scope specified in this Project Description, NIST is seeking to include the following components:

- Identity and Access Management System
- Endpoint Detection and Response System
- Network Monitoring Tool
- Behavior Anomaly Detection Tool
- Network and Host-based Intrusion Detection Systems
- Security Information and Event Monitoring System (SIEM)
- Network Policy Engine (PE)
- Firewall (FW)
- Integration Tool for Security Server/PE/FW
- Configuration Management, Back Up, Patch Management System
- Secure Remote Access
- Data Historian
- Cloud Based OT Capabilities: Data Historian, Supervisory Control and Data Acquisition (SCADA), Asset Management System

In their letters of interest, responding organizations need to acknowledge the importance of 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.
2. Support for development and demonstration of the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project, which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800-82 and SP

800-53, the NIST Cybersecurity Framework, and the NIST Privacy Framework.

Additional details about the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project are available at https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack.

NIST cannot guarantee that all 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 NCCoE consortium CRADA in the development of the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* 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 *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project. These descriptions will be public information.

Under the terms of the NCCoE 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 *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the *Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector* project architecture can provide security capabilities to mitigate identified risks related to data throughout its lifecycle. 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/.

Alicia Chambers,
NIST Executive Secretariat.
[FR Doc. 2022-27995 Filed: 12/22/2022 8:45 am; Publication Date: 12/23/2022]