Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 190924-0035]

National Cybersecurity Center of Excellence (NCCoE) Securing the Industrial Internet of Things for the Energy 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 Securing the Industrial Internet of Things (IIoT) for the energy sector use case. 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 energy 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 energy_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://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Jim McCarthy via email to energy_nccoe@nist.gov; by telephone 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 energy sector program are available at https://www.nccoe.nist.gov/node/4741.

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 energy sector program website at https://www.nccoe.nist.gov/node/4741 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 cybersecurity and infrastructure 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 Securing the IIoT for the energy sector use case. The full use case can be viewed at: https://www.nccoe.nist.gov/node/4741.

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. NIST will select participants who have submitted complete letters of interest on a first come, first served basis up to the number of participants 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 the 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.

Use Case Objective: The objective of this use case is to provide an architecture that can be referenced and develop guidance for securing IIoT in commercial- and/or utility-scale distributed energy resource (DER) environments, and to include an example solution that uses existing, commercially available and/or open-source cybersecurity products.
A detailed description of the Securing the IIoT use case is available at https://www.nccoe.nist.gov/node/4741.

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 and capabilities are listed in section 4 of the Securing the IIoT for the energy sector use case (for reference, please see the link in the PROCESS section above) and include:

- Access control techniques for network, application, and data access
- Data integrity technologies that protect data at rest or in transit, detect data integrity violations, and ensure data authenticity
- Graph analytics, machine learning, behavioral monitoring, and predictive analytics that aid in detecting malware and data integrity violations
- Information visualization and dashboard techniques that present analytic results to human operators
- Infrastructure components to construct or emulate the elements of the conceptual architecture

- Infrastructure components that incorporate integrity and trustworthiness techniques
- Sensors, network monitoring, system monitoring, data acquisition devices, intelligent sensor gateways, and security information and event management, or SIEM, systems that provide data and event information for analysis
- System/device and human authentication techniques that support federation
- Trustworthy distributed audit trails for accountability
- Workflow techniques to orchestrate analysis

Each responding organization's letter of interest should identify how their products or infrastructure components address one or more of the following desired solution characteristics in section 4 of the Securing the IIoT for the energy sector use case (for reference, please see the link in the PROCESS section above):

1. Analysis and Visualization. The analysis and visualization capabilities collect and process monitoring data from communications, management systems, and control systems to detect anomalies and identify anomalies that represent potential malicious activity.
2. Authentication and Access Control. The authentication and access control capabilities are used on all communication among DER management and control systems. These capabilities ensure that only known, authorized systems/devices can exchange information. Further, these capabilities may limit the types of information exchanged. Attempted unauthorized communication or attempted

communication by unknown systems/devices is detected and reported to the analysis and visualization capabilities.

3. Behavioral Monitoring. The behavioral monitoring capabilities measure behavioral characteristics of the management and control systems. Measurements are compared with expected or normal behavioral characteristics that have been learned over time. Anomalies are reported to the analysis and visualization capability.
4. Command Register. The command register capability records transactions between the distribution control system and control systems managing DERs. This capability allows both the utility and the DER operator to verify information exchanges.
5. Data Integrity. Data integrity capabilities ensure that information is not modified in transit between the sender and receiver. If the information is modified, the capabilities detect the modification and notify the analysis and visualization capabilities.
6. Malware Detection. The malware detection capabilities monitor both information exchanges among the DER management and control systems and processing by the management and control systems, looking for indications of compromise by known malware.

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 Securing the IIoT for the energy sector use case in NCCoE facilities which will be conducted in a manner consistent with the NIST Cybersecurity Framework, and other relevant standards and guidance listed in section 4 of the Securing the IIoT for the energy sector use case.

Additional details about the Securing the IIoT for the energy sector use case are available at: https://www.nccoe.nist.gov/node/4741.

NIST cannot guarantee that all 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 Securing the IIoT for the energy 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 energy 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 Securing the IIoT for the energy 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 Securing the IIoT for the energy sector capability will be announced on the NCCoE Web site at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome of the demonstration is to improve the security of IIoT across an entire energy sector 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 https://nccoe.nist.gov/.

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2019-21852 Filed: 10/7/2019 8:45 am; Publication Date: 10/8/2019]