DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 210921-0192]

National Cybersecurity Center of Excellence (NCCoE) *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management*

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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* 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 iot-onboarding@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 template by visiting https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding and completing the letter of interest webform. NIST will announce the

completion of the selection of participants and inform the public that it will no longer accept letters of interest for this project at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding. Organizations whose letters of interest are accepted will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST; a template CRADA can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: Paul Watrobski via email to iot-onboarding@nist.gov; by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project are available at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding.

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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle*

Management project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding. Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project website at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding announcing the completion of the project and informing the public that it will no longer accept letters of interest for this project. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective: The NCCoE will build a trusted network-layer onboarding solution example using commercially available technology that will address a set of cybersecurity challenges aligned to the NIST Cybersecurity Framework and Risk Management Framework. The project's objective is to define recommended practices for performing

trusted network-layer onboarding, which will aid in the implementation and use of trusted onboarding solutions for IoT devices at scale. This project seeks to define and demonstrate onboarding solutions that can be broadly adopted for use by many industry sectors. 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security* available at: https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the onboarding security requirements and practical steps needed to implement a cybersecurity reference implementation.

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 3 of the *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security* project description at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding and include, but are not limited to:

Core Components:

- IoT devices: Each device must be able to participate in trusted network-layer onboarding and to securely store private keys, credentials, and other information. Each device may have other capabilities that enable its use with additional solution components, such as the examples listed below.

- Network onboarding component: The network onboarding component is a logical component on the network that runs the network-layer onboarding protocol. It is authorized to interact with IoT devices on behalf of the network and use the network layer onboarding protocol to onboard devices to the network.
- Authorization service: The authorization service must be able to determine which IoT devices are authorized to be onboarded to the network and maintain a record of onboarded devices.
- Supply chain integration service: The supply chain integration service receives information about devices that the organization has purchased and provides this information to the authorization service to help the authorization service determine which devices are authorized to be onboarded to the network.
- Access point, router or switch: The access point, router, or switch must be able to route all traffic exchanged between the IoT devices and the rest of the network.

Additional Functional Components:

- Device intent management: This could include device intent managers, information servers, and components applying device intent policy.
- Attestation service: An attestation service could receive attestation tokens from IoT devices, evaluate them, and generate results that it returns to the network onboarding component to enable that component to decide whether or not the devices are trustworthy enough to be onboarded. The attestation service could also receive attestation tokens from IoT devices and any other connected components on an ongoing basis to help determine their continued trustworthiness.

- Controller, application server or cloud service: This remote service could securely download one or more applications to the device during application-layer onboarding.
- Lifecycle management service: This service could perform ongoing, automated lifecycle management of the device, such as applying firmware, software, and configuration updates to manage the overall security posture of the device throughout its lifecycle.
- Asset management: This service could integrate with the onboarding system to enable cross-checking the list of devices that have been securely onboarded with the inventory of connected devices. It could also monitor the software and configuration of onboarded IoT devices for known vulnerabilities.

Devices and Network Infrastructure Components:

- Device endpoints: Assets include the devices/endpoints, such as laptops, tablets, and other mobile or IoT devices, that connect to the enterprise.
- Enterprise resources: Enterprise resources include data and compute resources as well as applications/services hosted and managed on premise, in the cloud, at the edge, or some combination of these.
- Network infrastructure: Network infrastructure components encompass network resources a medium or large enterprise might typically deploy in its environment. It is assumed that the IoT device network layer onboarding core and functional components and devices are connected via, or integrated into, the network infrastructure. The NCCoE will provide these components as part of its internal lab infrastructure.

Each responding organization's letter of interest should identify how their products help address one or more of the following desired security characteristics and properties in

section 3 of the *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security* project description at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding:

- There is ongoing enforcement of device intent-based communication constraints and network segmentation.
- There is ongoing automated device lifecycle management that keeps the device updated and patched.
- There is ongoing mutual attestation of the device and its lifecycle management service.
- There is ongoing device software and configuration monitoring that includes cross-checking of onboarded devices with discovered devices.
- Each device executes its defined application.
- Each device connects to the network securely.
- If device intent is supported, the traffic filters that were specified by the device intent information are enforced to ensure that communications to and from the device are restricted to only those that are required. Local network policy can also be applied in addition to the device intent-specified policy.
- The device can be assigned to a particular network segment, for example based on level of trust, device type, or attestation token evaluation. The device can be dynamically reassigned to another segment, such as quarantining the device if its trustworthiness comes into question.
- The device's firmware, software, and configuration are updated and patched as needed to address vulnerabilities.

- The device and its trusted lifecycle management service perform ongoing mutual attestation to ensure each other's trustworthiness.
- If the trusted network-layer onboarding solution and the organization's asset management system are integrated, the asset management system can periodically cross-check its discovered devices with the onboarded IoT devices to ensure there are no discrepancies. The asset management system can also monitor the devices' software and configurations to identify known vulnerabilities.

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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project, which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, SP 800-37, SP 800-53, SP 800-63, SP 1800-15, and NISTIR 8259A.
3. Additional details about the *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project are available at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding.

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 *Trusted Internet of Things (IoT) Device Network-Layer*

Onboarding and Lifecycle Management 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project. 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* 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 *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management* project architecture can provide security capabilities to mitigate onboarding identified risks. 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. 2021-23293 Filed: 10/25/2021 8:45 am; Publication Date: 10/26/2021]