This document is scheduled to be published in the
Federal Register on 12/27/2017 and available online at
https://federalregister.gov/d/2017-27870, and on **FDsys.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 171115999-7999-01]

National Cybersecurity Center of Excellence (NCCoE) Mitigating Internet of Things (IoT) Based Distributed Denial of Service (DDoS) Building Block

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 Mitigating IoT-Based DDoS Building Block. 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 Mitigating IoT-Based DDoS Building Block. Participation in the building block 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, but no earlier than [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the building block has been completed, NIST will post a notice on the NCCoE Mitigating IoT-Based DDoS Building Block website at: https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to mitigating-iot-based-ddos-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: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Tim Polk, William Haag and Murugiah Souppaya via email to mitigating-iot-based-ddos-nccoe@nist.gov; by telephone 301-975-

0239; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Mitigating IoT-Based DDoS Building Block are available at: https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

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 platforms for the Mitigating IoT-Based DDoS Building Block. The full building block can be viewed at: https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

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 building block 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 building block. 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 a National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Building Block Objective: The building block objective is to improve the overall security of IoT devices. A detailed description of the Mitigating IoT-Based DDoS Building Block is available at: https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos.

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 3 of the Mitigating IoT-Based DDoS Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Network gateways/routers supporting wired and wireless network access
- Personal computing devices (personal computers, tablets, and phones)
- Business computing devices
- Thermostats and temperature sensors in different rooms
- Home appliances (refrigerators, washers and dryers, stoves and microwaves)
- Heating ventilation and air conditioning (HVAC) systems
- Lighting
- Digital video recorders (DVR)
- Closed-circuit TV cameras and Webcams
- Baby monitors
- Smart TVs
- Set top boxes
- Security cameras
- Point of sale devices
- Printer/scanners/fax machines
- Home assistants (e.g., Alexa)

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 3 of the Mitigating IoT-Based DDoS Building Block (for reference, please see the link in the PROCESS section above):

- IoT device controllers are capable of address assignment and packet filtering based on routes that can be integrated into home or enterprise networks;

- Manufacturer Usage Description (MUD) controllers are able to retrieve MUD files from web sites using the HTTPS protocol;
- MUD controllers are able to provide route filtering commands for enforcement by routers;
- MUD servers at participating web sites are capable of storing and retrieving MUD files and providing device communications requirements to MUD controllers;
- IoT devices are capable of inserting the MUD extension into address requests when they are powered up;
- IoT devices are capable of contacting update servers to download and apply security patches;
- Routers and switches are capable of receiving threat feeds from cloud-based or infrastructure services like DNS that includes type, severity, and mitigation for threats; and
- Any cryptographic modules employed conform to FIPS 140-2.

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 Mitigating IoT-Based DDoS Building Block in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: OMB Circular A-130; NIST Special Publications 800-40; 800-52; 800-57; 800-63; 800-147; 800-193;

NISTIR 7823; NIST Framework for Improving Critical Infrastructure Cybersecurity; Ongoing Manufacturer Usage Description (MUD) Standards activities including Manufacturer Usage Description Specification, MUD Lifecyle: A Network Operator's Perspective, and MUD Lifecyle: A Manufacturer's Perspective; and RFCs 2131, 2818, 3315, 5280, 5652, and 6020.

Additional details about the Mitigating IoT-Based DDoS Building Block are available at: https://nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos.

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 Mitigating IoT-Based DDoS Building Block. 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 Mitigating IoT-Based DDoS Building Block. 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 Mitigating IoT-Based DDoS Building Block 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 of IoT devices within the 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 http://nccoe.nist.gov/.

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2017-27870 Filed: 12/26/2017 8:45 am; Publication Date: 12/27/2017]