This document is scheduled to be published in the
Federal Register on 02/21/2019 and available online at
https://federalregister.gov/d/2019-02977, and on **govinfo.gov**

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 190204061-9061-01]

National Cybersecurity Center of Excellence (NCCoE) Critical Cybersecurity Hygiene: Patching the Enterprise 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 Critical Cybersecurity Hygiene: Patching the Enterprise 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 Critical Cybersecurity Hygiene: Patching the Enterprise Building Block. Participation in the building block 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 **[PLEASE 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 cyberhygiene@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://www.nccoe.nist.gov/sites/default/files/library/nccoe-consortium-crada-example.pdf.

FOR FURTHER INFORMATION CONTACT: Alper Kerman and Murugiah Souppaya via email to cyberhygiene@nist.gov; by telephone 301-975-0226 and 301-975-8443; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Critical Cybersecurity Hygiene: Patching the Enterprise Building Block are available at https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf.

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 building block has been completed, NIST will post a notice on the NCCoE Critical Cybersecurity Hygiene: Patching the Enterprise Building Block website at https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

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 Critical Cybersecurity Hygiene: Patching the Enterprise Building Block. The full building block can be viewed at: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf.

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 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 objective of this building block is to demonstrate a proposed approach for improving enterprise patching practices for general IT systems. A detailed description of the Critical Cybersecurity Hygiene: Patching the Enterprise Building Block is available at: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf.

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 Critical Cybersecurity Hygiene: Patching the Enterprise Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Personal computers (PCs) and mobile devices, including operating systems, firmware, and apps

- Unified endpoint management (UEM), enterprise mobility management (EMM), mobile device management (MDM), and mobile application management (MAM) solutions
- Firewalls and intrusion detection/protection systems
- Routers/switches
- Network-based storage
- Update sources
- Privilege access management (PAM) system and privileged access workstation
- Configuration management system
- Vulnerability management system
- On-premises datacenter and cloud infrastructure, including servers, virtual machine (VM) hosts, VMs, containers, apps, and firmware

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 2 of the Critical Cybersecurity Hygiene: Patching the Enterprise Building Block (for reference, please see the link in the PROCESS section above):

1. Free or commercial tools will be harnessed to enable inventory capabilities so that the assets in the form of firmware, operating systems, and applications across the environment can be discovered, identified, classified for different impact levels and then prioritized for the order of remediation.

2. Patches will be deployed on scheduled intervals as part of regular release cycles, as well as on demand upon active patching emergencies in crisis situations to endpoint firmware, OS, and applications hosted on-premises or in the cloud (e.g., Infrastructure as a Service), as well as "network devices" like firewalls, Storage Area Network (SAN) devices, routers, network switches, and other network appliances.
3. A cloud delivery model will be used as the mechanism for patching, such as a mobile device or a "Windows as a Service (WaaS)" model with Windows operating systems, Apple Software Update, and mobile software updates for Android and iOS devices provided by device manufacturers or mobile operators.
4. Vulnerabilities will be identified and categorized across the assets so that the appropriate patches can be deployed in a prioritized order for optimum effectiveness.
5. There will be implementation procedures for isolation methods in place for assets that cannot be easily patched such as legacy unsupported systems or systems with very high operational availability requirements.
6. There will be stringent security practices in place to safeguard the patch management systems and any associated components used to support the patch management activities.

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 Critical Cybersecurity Hygiene: Patching the Enterprise Building Block in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800-53, SP 800-40, SP 800-184 and NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

Additional details about the Critical Cybersecurity Hygiene: Patching the Enterprise Building Block are available at: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf.

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 Critical Cybersecurity Hygiene: Patching the Enterprise 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 Critical Cybersecurity Hygiene: Patching the Enterprise 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 Critical Cybersecurity Hygiene: Patching the Enterprise 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 enterprise patching practices for general IT systems as part of a crucial effort in maintaining a highly effective Critical Cybersecurity Hygiene 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 A. Kimball,

NIST Chief of Staff.

[FR Doc. 2019-02977 Filed: 2/20/2019 8:45 am; Publication Date: 2/21/2019]