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 Derived PIV Credentials Building Block in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (*e.g.,* FIPS 200, FIPS 201, SP 800–53, and SP 800–63)

In addition, 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 Derived PIV Credentials 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 Derived PIV Credentials 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/.*

Richard Cavanagh,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2015–20039 Filed 8–13–15; 8:45 am]

BILLING CODE P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 141110948–5504–01]

National Cybersecurity Center of Excellence, Mobile Device Security 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 Mobile Device Security 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 Mobile Device Security 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 that identifies the organization requesting participation in the NCCoE Mobile Device Security Building Block and the capabilities and components that are being offered to the collaborative effort. 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 September 14, 2015. When the building block has been completed, NIST will post a notice on the NCCoE Mobile Device Security Building Block Web site at *http://nccoe.nist.gov/?q=content/mobile-device-security* 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 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to *mobile-nccoe@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; 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 Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: *http://nccoe.nist.gov/node/138.*

FOR FURTHER INFORMATION CONTACT: Joshua Franklin via email at *nccoe-mobile@nist.gov;* by telephone 240–314–6800; or by mail to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Mobile Device Security Building Block are available at *http://nccoe.nist.gov/?q=content/mobile-device-security.*

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 Mobile Device Security Building Block. The full building block can be viewed at: *http://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.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 and which identifies the organization requesting participation in the Mobile Device Building Block and the capabilities and components that are being offered to the collaborative effort. 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 and to obtain additional information. 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 the Mobile Device Security 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

NCCoE use cases address cybersecurity challenges that affect an entire industry sector while NCCoE building blocks are cybersecurity example solutions that are applicable across multiple industry sectors.

The Mobile Device Security Building Block proposes a system of commercially available technologies that provide enterprise-class protection for mobile platforms that access corporate resources. A detailed description of the Mobile Device Security Building Block is available at: *http://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.pdf.*

Traditionally, enterprises established boundaries to separate their trusted internal IT network(s) from untrusted external networks. When employees consume and generate corporate information on mobile devices, this traditional boundary erodes. Due to the rapid changes in today's mobile platforms, enterprises have the challenge of ensuring that mobile devices connected to their networks can be trusted to protect sensitive data as it is stored, accessed and processed, while still giving users the features they have come to expect from mobile devices.

This building block will demonstrate commercially available technologies that provide protection to both organization-issued and personally-owned mobile platforms. These technologies enable users to work inside and outside the business network with a securely configured mobile device, while allowing for granular control over the enterprise network boundary, and minimizing the impact on function. The architecture demonstrated by this building block will incorporate a modular technology stack that allows enterprises to tailor solutions to their business needs. Additional details about the mobile device building block are available at: *http://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.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 ten of the Mobile Device Security Building Block (for reference, please see the link in the PROCESS section above), and include, but are not limited to:

1. Mobile devices using modern operating systems, including but not limited to Android, iOS and Windows, to the extent possible, with a hardware root of trust
2. Enterprise mobility management suite
3. Mobile applications that can be put into a secure container and/or wrapped
4. Enterprise infrastructure which might include:
   a. Identity and access management platform
   b. Data loss prevention solution
   c. Security event and information management tool
   d. VPN gateway
   e. Certification authority

Each responding organization's letter of interest should identify how their product(s) addresses one or more of the desired security characteristics in section four of the Mobile Device Security Building Block description (for reference, please see the link in the PROCESS section above).

Additional details about the Mobile Device Building Block are available at *http://nccoe.nist.gov/?q=content/mobile-device-security.*

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 Mobile Device Security Building Block. Prospective participants' contributions 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 Mobile Device Security Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, participants will commit to providing:

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 Mobile Device Security Building Block in NCCoE facilities, which will be conducted in a manner consistent with Federal requirements (*e.g.,* FIPS 200, FIPS 201, SP 800–53, and SP 800–63)

In addition, NIST will support development of interfaces among participants' products, including 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 Mobile Device Security 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 mobile device security 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/.*

Richard Cavanagh,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2015–20040 Filed 8–13–15; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE106

Pacific Fishery Management Council; Public Meeting

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; public meeting.

SUMMARY: The Pacific Fishery Management Council's (Pacific Council) Groundfish Management Team (GMT) will hold a webinar that is open to the public.

DATES: The GMT meeting will be held Tuesday, September, 1, 2015, from 1 p.m. until business for the day is completed.