(b) With a Brinell hardness measured in all parts of the product including mid thickness falling within one of the following ranges:

(i) 270–300 HBW,

(ii) 290–320 HBW, or

(iii) 320–350 HBW;

(c) Having cleanliness in accordance with ASTM E45 method A (Thin and Heavy): A not exceeding 1.5, B not exceeding 1.0, C not exceeding 0.5, D not exceeding 1.5; and

(d) Conforming to ASTM A578–S9 ultrasonic testing requirements with acceptance criteria 2 mm flat bottom hole;

(6) Alloy forged and rolled steel CTL plate over 407 mm in actual thickness and meeting the following requirements:

(a) Made from Electric Arc Furnace melted, Ladle refined & vacuum degassed, alloy steel with the following chemical composition (expressed in weight percentages):

- Carbon 0.23–0.28,
- Silicon 0.05–0.15,
- Manganese 1.20–1.50,
- Nickel not greater than 0.4,
- Sulfur not greater than 0.010,
- Phosphorus not greater than 0.020,
- Chromium 1.20–1.50,
- Molybdenum 0.35–0.55,
- Boron 0.002–0.004,
- Oxygen not greater than 20 ppm,
- Hydrogen not greater than 2 ppm, and
- Nitrogen not greater than 60 ppm;

(b) Having cleanliness in accordance with ASTM E45 method A (Thin and Heavy): A not exceeding 1.5, B not exceeding 1.5, C not exceeding 1.0, D not exceeding 1.5;

(c) Having the following mechanical properties:

(i) With a Brinell hardness not more than 237 HBW measured in all parts of the product including mid thickness; and having a Yield Strength of 75 ksi min and UTS 95 ksi or more, Elongation of 18% or more and Reduction of area 35% or more; having charpy V at −75 degrees F in the longitudinal direction equal or greater than 15 ft. lbs (single value) and equal or greater than 20 ft. lbs (average of 3 specimens) and conforming to the requirements of NACE MR01–75; or

(ii) With a Brinell hardness not less than 240 HBW measured in all parts of the product including mid thickness; and having a Yield Strength of 90 ksi min and UTS 110 ksi or more, Elongation of 15% or more and Reduction of area 30% or more; having charpy V at −40 degrees F in the longitudinal direction equal or greater than 21 ft. lbs (single value) and equal or greater than 31 ft. lbs (average of 3 specimens);

(d) Conforming to ASTM A578–S9 ultrasonic testing requirements with acceptance criteria 3.2 mm flat bottom hole; and

(e) Conforming to magnetic particle inspection in accordance with AMS 2301;

(7) Alloy forged and rolled steel CTL plate over 407 mm in actual thickness and meeting the following requirements:

(a) Made from Electric Arc Furnace melted, ladle refined & vacuum degassed, alloy steel with the following chemical composition (expressed in weight percentages):

- Carbon 0.25–0.30,
- Silicon not greater than 0.25,
- Manganese not greater than 0.50,
- Nickel 3.0–3.5,
- Sulfur not greater than 0.010,
- Phosphorus not greater than 0.020,
- Chromium 1.0–1.5,
- Molybdenum 0.6–0.9,
- Vanadium 0.08 to 0.12
- Boron 0.002–0.004,
- Oxygen not greater than 20 ppm,
- Hydrogen not greater than 2 ppm, and
- Nitrogen not greater than 60 ppm.

(b) Having cleanliness in accordance with ASTM E45 method A (Thin and Heavy): A not exceeding 1.0(t) and 0.5(h), B not exceeding 1.5(t) and 1.0(h), C not exceeding 1.0(t) and 0.5(h), and D not exceeding 1.5(t) and 1.0(h);

(c) Having the following mechanical properties: A Brinell hardness not less than 350 HBW measured in all parts of the product including mid thickness; and having a Yield Strength of 145 ksi or more and UTS 160 ksi or more, Elongation of 15% or more and Reduction of area 35% or more; having charpy V at −40 degrees F in the transverse direction equal or greater than 20 ft. lbs (single value) and equal or greater than 25 ft. lbs (average of 3 specimens);

(d) Conforming to ASTM A578–S9 ultrasonic testing requirements with acceptance criteria 3.2 mm flat bottom hole; and

(e) Conforming to magnetic particle inspection in accordance with AMS 2301.

The products subject to the investigation are currently classified in the Harmonized Tariff Schedule of the United States (HTSUS) under item numbers: 7208.40.3030, 7208.40.3060, 7208.51.0030, 7208.51.0045, 7208.51.0060, 7208.52.0000, 7211.13.0000, 7211.14.0030, 7211.14.0045, 7225.40.1110, 7225.40.1180, 7225.40.3005, 7225.40.3050, 7226.20.0000, and 7226.91.5000.

The products subject to the investigation may also enter under the following HTSUS item numbers: 7208.40.6060, 7208.53.0000, 7208.90.0000, 7210.70.3000, 7210.90.9000, 7211.19.1500, 7211.19.2000, 7211.19.4500, 7211.19.6000, 7211.19.7590, 7211.90.0000, 7212.40.1000, 7212.40.5000, 7212.50.0000, 7214.10.0000, 7214.30.0010, 7214.30.0080, 7214.91.0015, 7214.91.0060, 7214.91.0090, 7225.11.0000, 7225.19.0000, 7225.40.5110, 7225.40.5130, 7225.40.5160, 7225.40.7000, 7225.99.0010, 7225.99.0090, 7226.11.1000, 7226.11.9060, 7226.19.1000, 7226.19.9000, 7226.91.0500, 7226.91.1530, 7226.91.1560, 7226.91.2530, 7226.91.2560, 7226.91.7000, 7226.91.8000, and 7226.99.0180.

The HTSUS subheadings above are provided for convenience and customs purposes only. The written description of the scope of the investigation is dispositive.

[FR Doc. 2016–28703 Filed 11–28–16; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 160830797–6797–01]

National Cybersecurity Center of Excellence (NCCoE) Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder sector. 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 Public Safety & First Responder sector program. Participation in the use case 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 December 29, 2016. When the use case has been completed, NIST will post a notice on the NCCoE Public Safety & First Responder sector program Web site at *https://nccoe.nist.gov/projects/building_blocks/mobile-sso* announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *PSFR–NCCoE@nist.gov* or via hardcopy to National Institute of Standards and Technology, 100 Bureau Drive Mail Stop 2002, Gaithersburg, MD 20899. 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: Paul Grassi or William Fisher via email to *PSFR–NCCoE@nist.gov;* by telephone 301–975–0200; or by mail to National Institute of Standards and Technology, NCCoE; 100 Bureau Drive Mail Stop 2002, Gaithersburg, MD 20899. Additional details about the Public Safety & First Responder sector program are available at *https://nccoe.nist.gov/projects/building_blocks/mobile-sso*.

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 Application Single Sign On (SSO) for the Public Safety & First Responder Sector. The full use case can be viewed at: *https://nccoe.nist.gov/projects/building_blocks/mobile-sso*.

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 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 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 **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

When responding to an emergency, public safety personnel require on-demand access to data. The ability to quickly and securely authenticate in order to access public safety data is critical to ensuring that first responders can deliver the proper care and support during an emergency. In order to adequately meet the need of diverse public safety personnel, missions, and operational environments, authentication mechanisms need to support deployments where devices may be shared amongst personnel and authentication factors have usability constraints.

The challenge that first responders face in authenticating quickly and securely to public safety systems is compounded when a first responder is forced to authenticate individually to multiple mobile applications. In addition, when authorizing application access to shared resources, first responders may be subjected to an additional authentication step at the resource provider. To address the challenge identified by the public safety community, the National Cybersecurity Center of Excellence (NCCoE) plans to develop a Mobile Application Single Sign On (SSO) reference design and implementation that meets these unique authentication requirements and allows first responders to take advantage of the latest mobile authentication technology and best practices.

A detailed description of the Mobile Application Single Sign On (SSO) is available at: *https://nccoe.nist.gov/projects/building_blocks/mobile-sso*.

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder use case (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Mobile devices
- Mobile platforms for biometric authentication
- Hardware based authenticators that interoperate with mobile platforms
- Software Development Kit (SDK) or platform that enables mobile single sign on capabilities

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder use case (for reference, please see the link in the PROCESS section above):

1. A standards-based approach and a solution architecture that selects the most effective and secure approach to implement mobile SSO leveraging native capabilities of the mobile OS.

2. Support mobile SSO both for authentication and delegated authorization (as in OAuth Client Applications).

3. Ensure that mobile applications do not have access to user credentials.

4. Support multiple authenticators taking into account unique environmental constraints faced by first responders in emergency medical services, law enforcement, and the fire service such as:

a. Gloved, one-handed, or hands-free operation
b. Use of smoke hoods, fire hoods or gas masks that may prevent facial or iris recognition
c. Proximity based authenticators (new yubikeys)
d. Biometric based continuous authentication mechanisms that meet the requirements of draft NIST Special Publication 800–63B

5. Allow multi-user operation of shared mobile devices.

6. Support for multiple authentication protocols. If appropriate, public sector agencies must be able to leverage multifactor authentication. This may be accomplished by adopting Fast IDentity Online (FIDO 2.0) Universal Authentication Framework (UAF), Universal 2nd Factor (U2F), PKI, or some other means.

7. Support a spectrum of BYOD (Bring Your Own Device) and COPE (Corporate Owned, Personally Enabled) scenarios.

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder use case 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)

Additional details about the Mobile Application Single Sign On (SSO) for the Public Safety & First Responder sector use case are available at: *https://nccoe.nist.gov/projects/building_blocks/mobile-sso*.

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 Application Single Sign On (SSO) for the Public Safety & First Responder 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 Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder sector 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 application single sign-on across an entire Public Safety & First Responder 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 *http://nccoe.nist.gov/*.

Kent Rochford,

Associate Director for Laboratory Programs.

[FR Doc. 2016–28627 Filed 11–28–16; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Ocean Exploration Advisory Board (OEAB)

AGENCY: Office of Oceanic and Atmospheric Research (OER) National Oceanic and Atmospheric Administration (NOAA) Department of Commerce (DOC).

ACTION: Notice of Membership Solicitation for the OEAB.

SUMMARY: OAR publishes this notice to solicit applications to fill a single membership vacancy on the Ocean Exploration Advisory Board (OEAB) with an individual demonstrating expertise in data science and management and one other area of expertise relevant to ocean exploration, such as seafloor mapping. The new OEAB member will serve an initial three-year term, renewable once.

The purpose of the OEAB is to advise the Under Secretary of Commerce for Oceans and Atmosphere on matters pertaining to ocean exploration including: The identification of priority areas that warrant exploration; the development and enhancement of technologies for exploring the oceans; managing the data and information; and disseminating the results. The OEAB also provides advice on the relevance of the program with regard to the NOAA Strategic Plan, the National Ocean Policy Implementation Plan, and other appropriate guidance documents.

APPLICATIONS: An application is required to be considered for OEAB membership. To apply, please submit (1) full name, title, institutional affiliation, and contact information (mailing address, email, telephones, fax); (2) a short description of his/her qualifications relative to data science and management, and at least one other area of expertise related to ocean exploration; (3) a resume or curriculum vitae (maximum length 4 pages); and (4) A cover letter stating their interest in serving on the OEAB and highlighting specific areas of expertise relevant to the purpose of the OEAB.

DATES: Application materials should be sent to the mailing or email address specified below and must be received no later than 15 days after publication of this **Federal Register** Notice.

ADDRESSES: Submit resume and application materials to Yvette Jefferson via mail or email. Mail: NOAA, 1315 East West Highway, SSMC3 Rm 10315, Silver Spring, MD 20910; Email: *Yvette.Jefferson@noaa.gov*.

FOR FURTHER INFORMATION CONTACT: David McKinnie, OEAB Designated Federal Officer, NOAA/OER, 7600 Sand Point Way NE., Seattle, WA 98115; 206–526–6950; *david.mckinnie@noaa.gov*.

SUPPLEMENTARY INFORMATION: The OEAB functions as an advisory body in accordance with the Federal Advisory Committee Act (FACA), as amended, 5 U.S.C. App., with the exception of section 14. It reports to the Under Secretary, as directed by 33 U.S.C. 3405.

The OEAB consists of approximately ten members including a Chair and Co-chair(s), designated by the Under Secretary in accordance with FACA requirements and the terms of the approved OEAB Charter.

The OEAB:

a. advises the Under Secretary on all aspects of ocean exploration including areas, features, and phenomena that warrant exploration; and other areas of program operation, including development and enhancement of technologies for exploring the ocean, managing ocean exploration data and information, and disseminating the results to the public, scientists, and educators;

b. assists the program in the development of a 5-year strategic plan for the fields of ocean, marine, and Great Lakes science, exploration, and discovery, as well as makes recommendations to NOAA on the evolution of the plan based on results and achievements;

c. annually reviews the quality and effectiveness of the proposal review process established under [correct]; and

d. provides other assistance and advice as requested by the Under Secretary.

OEAB members are appointed as special government employees (SGEs)