party's intellectual property rights). In addition, you agree to waive claims against the Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect, or consequential, arising from your participation in the RAMP Challenge, whether the injury, death, damage, or loss arises through negligence or otherwise.

NIST is not responsible for any miscommunications such as technical failures related to computer, telephone, cable, and unavailable network or server connections, related technical failures, or other failures related to hardware, software or virus, or incomplete or late Entries. Any compromise to the fair and proper conduct of the RAMP Challenge may result in the disqualification of an Entry or Participant, termination of the RAMP Challenge, or other remedial action, at the sole discretion of NIST. NIST reserves the right in its sole discretion to extend or modify the dates of the RAMP Challenge, and to change the terms set forth herein governing any phases taking place after the effective date of any such change. By entering, you agree to the terms set forth herein and to all decisions of NIST and/or all of their respective agents, which are final and binding in all respects.

NIST is not responsible for: (1) Any incorrect or inaccurate information, whether caused by a Participant, printing errors, or by any of the equipment or programming associated with or used in the RAMP Challenge; (2) unauthorized human intervention in any part of the Entry Process for the RAMP Challenge; (3) technical or human error that may occur in the administration of the RAMP Challenge or the processing of Entries; or (4) any injury or damage to persons or property that may be caused, directly or indirectly, in whole or in part, from a Participant's participation in the RAMP Challenge or receipt or use or misuse of an Award. If for any reason an Entry is confirmed to have been deleted erroneously, lost, or otherwise destroyed or corrupted, the Participant's sole remedy is to submit another Entry in the RAMP Challenge.

Termination and Disqualification

NIST reserves the authority to cancel, suspend, and/or modify the RAMP Challenge, or any part of it, if any fraud, technical failures, or any other factor beyond NIST's reasonable control impairs the integrity or proper functioning of the RAMP Challenge, as determined by NIST in its sole discretion.

NIST reserves the right to disqualify any Participant or Participant team it believes to be tampering with the Entry process or the operation of the RAMP Challenge or to be acting in violation of any applicable rule or condition.

Any attempt by any person to undermine the legitimate operation of the RAMP Challenge may be a violation of criminal and civil law, and, should such an attempt be made, NIST reserves the authority to seek damages from any such person to the fullest extent permitted by law.

Verification of Potential Winner(s)

All potential winners are subject to verification by NIST, whose decisions are final and binding in all matters related to the RAMP Challenge.

Potential winner(s) must continue to comply with all terms and conditions of the RAMP Challenge Rules described in this notice, and winning is contingent upon fulfilling all requirements. In the event that a potential winner, or an announced winner, is found to be ineligible or is disqualified for any reason, NIST may make an award, instead, to another Participant.

Privacy and Disclosure under FOIA

Except as provided herein, information submitted throughout the RAMP Challenge will be used only to communicate with Participants regarding Entries and/or the RAMP Challenge. Participant Entries and submissions to the RAMP Challenge may be subject to disclosure under the Freedom of Information Act (''FOIA'').

Authority: 15 U.S.C. 3719.

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2016–30437 Filed 12–16–16; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 161116999–6999–01]

National Cybersecurity Center of Excellence (NCCoE) Multifactor Authentication for e-Commerce Project for the Retail 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 the Multifactor Authentication for e-Commerce Project for the retail 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 retail sector program. Participation in the Multifactor Authentication for e-Commerce Project 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 January 18, 2017. When the Multifactor Authentication for e-Commerce Project search for collaborators has been completed, NIST will post a notice on the NCCoE retail sector program Web site at *https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce* announcing the completion of the search for collaborators and informing the public that it will no longer accept letters of interest for this Multifactor Authentication for e-Commerce Project.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *consumer-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 Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: *https://nccoe.nist.gov/library/nccoe-consortium-crada-example.*

FOR FURTHER INFORMATION CONTACT: William Newhouse via email to *william.newhouse@nist.gov;* by telephone 301–975–0232; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Multifactor Authentication for e-Commerce Project are available at *https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.*

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 Multifactor Authentication for e-Commerce Project for the retail sector. The full Multifactor Authentication for e-Commerce Project Description can be viewed at: *https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.*

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 Multifactor Authentication for e-Commerce 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 Multifactor Authentication for e-Commerce Project. 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.

Multifactor Authentication for e-Commerce Project Objective: The goal of this project is to increase the confidence of user identity and reduce the risk of fraud in the online, Card-Not-Present (CNP) space by implementing multifactor authentication for e-commerce transactions along with other security controls. The solution will provide guidance for implementing multifactor authentication mechanisms, risk calculation, web analytics, and potentially identity federation, in retail IT architecture segments that support or interface with e-commerce transactions such as online shopping or loyalty points programs. It will produce an architecture that includes components that will integrate multifactor authentication mechanisms (certificate-based, biometric, or others), risk calculation engines (risk score calculation and decisions), web analytics (pertaining to known user behavior and/or web threat detection), potentially identity federation (which can include authentication and risk information sent from a third-party business partner and Identity Provider), and automated logging within and between each component.

A detailed description of the Multifactor Authentication for e-Commerce Project is available at: *https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.*

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 the High-Level Architecture section of the Multifactor Authentication for e-Commerce Project Description (for reference, please see the link in the Process section above) and include, but are not limited to:

- Online/e-commerce shopping cart and payment system (in-house or outsourced)
- Multifactor authentication mechanisms (types of which to be determined)
- Risk calculation platform/engine
- Web analytics engine
- Logging of risk calculation and web analytics data
- Data storage for risk calculation and web analytics data
- Identity federation mechanism (optional)

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in the High-Level Architecture section of the Multifactor Authentication for e-Commerce Project Description for the retail use case (for reference, please see the link in the Process section above):

- Authentication mechanisms that meet business security and regulatory requirements
- Automated web analytics including monitoring of user behavior and contextual details
- Automated logging of web analytics and risk calculation data
- Automated data storage of web analytics and risk calculation data
- Ability to establish and enforce risk decisions including performing risk calculations
- Automated alerting of suspected fraudulent activity
- Ease of use for the consumer, no substantial increase in friction during the e-commerce transaction
- Identity federation (optional)

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 Multifactor Authentication for e-Commerce Project for the retail 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 Multifactor Authentication for e-Commerce Project for the retail sector use case are available at: *https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.* 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 Multifactor Authentication for e-Commerce Project for the retail sector capability. Prospective participant's 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 retail 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 Multifactor Authentication for e-Commerce Project for the retail 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 Multifactor Authentication for e-Commerce Project for the retail 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 added security and reduced fraud stemming from an increased use of multifactor authentication for e-commerce transactions across an entire retail 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/.*

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2016–30435 Filed 12–16–16; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XF040

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 (Council) Ad Hoc Ecosystem Workgroup (EWG) will hold a webinar, which is open to the public.

DATES: The webinar will be held on January 10, 2017, from 1:30 to 4:30 p.m., or when business for the day is completed.

ADDRESSES: To join the webinar visit this link: *http://www.gotomeeting.com/online/webinar/join-webinar.* Enter the Webinar ID: 917–479–603. Enter your name and email address (required). Once you have joined the webinar, choose either your computer's audio or select ''Use Telephone.'' If you do not select ''Use Telephone'' you will be connected to audio using your computer's microphone and speakers (VolP). To use your telephone for the audio portion of the meeting dial this TOLL number +1 (914) 614–3221 (not a toll-free number); then enter the Attendee phone audio access code 462–275–391, then enter your audio phone pin (shown after joining the webinar). Participants are encouraged to use their telephone, as this is the best practice to avoid technical issues and excessive feedback. You may send an email to Mr. Kris Kleinschmidt *(kris.kleinschmidt@noaa.gov)* or contact him at (503) 820–2425 for technical assistance. A public listening station will also be provided at the Pacific Council office.

Council address: Pacific Council, 7700 NE Ambassador Place, Suite 101, Portland, OR 97220–1384.

FOR FURTHER INFORMATION CONTACT: Dr. Kit Dahl, Pacific Council Staff Officer; phone: (503) 820–2422; email: *kit.dahl@noaa.gov.*

SUPPLEMENTARY INFORMATION: The purpose of the webinar is for the EWG to discuss (1) preparation of the Annual State of the California Current Ecosystem Report and (2) future ecosystem initiatives under the Council's Fishery Ecosystem Plan (FEP).

Each March, the National Marine Fisheries Service's Northwest and Southwest Fisheries Science Centers deliver a State of the California Current Ecosystem Report to the Council. The Report assesses current status through a series of indicators covering physical, biological, and socioeconomic components of the ecosystem. The Council has provided advice to the Science Centers on how to make the report more relevant to Council decision-making including comments on the suite of indicators it uses. The webinar will provide an opportunity for the EWG to discuss preparation of the current Report with Science Center representatives and the contents of future reports.

At its March 2017 meeting, the Council will also consider taking up a new ecosystem-based fishery management initiative. Appendix A to the FEP contains a list of these initiatives, which are intended to address ecosystem gaps in ecosystem knowledge and FMP policies, particularly with respect to the cumulative effects of fisheries management on marine ecosystems and fishing communities. The FEP establishes a schedule by which each March the Council reviews progress to date on any ecosystem initiatives the Council already has underway and determines whether to take up a new initiative. In odd-numbered years the Council may also consider identifying new initiatives that are not already in Appendix A. The EWG will discuss current and potential new initiatives in preparation for the March 2017 Council meeting.

Although nonemergency issues not contained in the meeting agenda may be discussed, those issues may not be the subject of formal action during this meeting. Action will be restricted to those issues specifically listed in this document and any issues arising after publication of this document that require emergency action under section 305(c) of the Magnuson-Stevens Fishery Conservation and Management Act, provided the public has been notified of the intent to take final action to address the emergency.

Special Accommodations

This meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Mr. Kris Kleinschmidt at (503) 820–2425 at least 10 business days prior to the meeting date.

Dated: December 14, 2016.

Tracey L. Thompson,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2016–30416 Filed 12–16–16; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XF082

Marine Mammals; File No. 20527

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