

radiators; sound mufflers for vehicle engines; clutch assemblies; bearing holders; transmissions; transmission sub-assemblies; brakes; axle covers; brackets; stays; rods; muffler pipe; rod assemblies; flanges; supports; knobs; levers; wiper blades; control wire; control cable; shock absorbers; universal joints; bevel gears; spiral gears; pinion gears; guards; lenses; plates; planetary gears; splines; drive shafts; clutch rod shafts; u-joints; shaft assemblies; collars; differential cases; transmission cases; ball joints; axle cases; gear cases; gear shafts; pins; shims; bushings; drive shaft caps; shaft couplings; steering shafts; shaft yokes; thrust collars; synchronizer rings; dust covers; heater assemblies; tie rods; brackets; battery retainers; control pedals; fuel tanks; hand rails; radiator grilles; bonnet dampers; steering linkages; suspension linkages; muffler stays; struts for agricultural tractors and other off-road vehicles; unmounted glass lenses for vehicle signals and controls; glass lenses for vehicle signals and controls; thermometers; sensors; gauges; oil switches; electrical sensors and liquid and gas sensors; odometers; other panel meters for use in vehicle control; counters for use in vehicles and farm implements; volt meters for vehicle and farm implement controls; other instruments for vehicle and farm implement controls; test benches for vehicle and implement repair; measuring equipment for vehicle control and repair; thermostats; temperature controllers; speed sensors for vehicle control; regulators; rotary switches; seats and seat assemblies; slide rollers for seats; work lamps; toy tractors; brushes for vehicle repair; and, electric lighter covers for agricultural tractors and other off-road vehicles (duty rate ranges from duty-free to 12%). The request indicates that bearings are subject to antidumping/countervailing duty (AD/CVD) orders when imported from certain countries. The FTZ Board's regulations (15 CFR 400.14(e)) require that merchandise subject to AD/CVD orders, or items which would be otherwise subject to suspension of liquidation under AD/CVD procedures if they entered U.S. customs territory, be admitted to the zone in privileged foreign status (19 CFR 146.41).

Public comment is invited from interested parties. Submissions shall be addressed to the Board's Executive Secretary at the address below. The closing period for their receipt is January 3, 2018.

A copy of the notification will be available for public inspection at the Office of the Executive Secretary, Foreign-Trade Zones Board, Room

21013, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230-0002, and in the "Reading Room" section of the Board's Web site, which is accessible via [www.trade.gov/ftz](http://www.trade.gov/ftz).

For further information, contact Christopher Wedderburn at [Chris.Wedderburn@trade.gov](mailto:Chris.Wedderburn@trade.gov) or (202) 482-1963.

Dated: November 17, 2017.

**Andrew McGilvray,**  
Executive Secretary.

[FR Doc. 2017-25399 Filed 11-22-17; 8:45 am]

**BILLING CODE 3510-DS-P**

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

[Docket No. 171010985-7985-01]

#### National Cybersecurity Center of Excellence (NCCoE) Securing Property Management Systems for the Hospitality 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 Securing Property Management Systems for the Hospitality 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 Hospitality 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 26, 2017. When the use case has been completed, NIST will post a notice on the NCCoE Hospitality Sector program Web site at <https://nccoe.nist.gov/projects/use-cases/securing-property-management-systems> 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 [hospitality-nccoe@nist.gov](mailto:hospitality-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:** Mr. William Newhouse via email to [hospitality-nccoe@nist.gov](mailto:hospitality-nccoe@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 Hospitality Sector program are available at <https://nccoe.nist.gov/projects/use-cases/securing-property-management-systems>.

#### **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 Securing Property Management Systems for the Hospitality Sector. The full use case can be viewed at: <https://nccoe.nist.gov/projects/use-cases/securing-property-management-systems>.

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:* The objective of this project is to help the hospitality industry implement stronger security measures and reduce vulnerabilities within and around their Property Management Systems (PMS), with a focus on the connection to a point-of-sale (POS) system. The project will identify typical hotel IT infrastructures and PMS-POS configurations, systems, and components that integrate or interface with both applications. The project will also identify interactions between PMS operators and authorized third-party service provider (SP) systems (e.g., online booking, customer relationship marketing partners, etc.). This project will result in a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to effectively secure property management systems. A detailed description of the Securing Property Management Systems Use Case is available at: <https://nccoe.nist.gov/projects/use-cases/securing-property-management-systems>.

*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 Securing Property Management Systems Project Description for the Hospitality Sector (for reference, please see the link in the

PROCESS section above) and include, but are not limited to:

- PMS and POS system(s)
- Point-to-Point Encryption (P2PE)
- Data tokenization
- Multifactor authentication mechanism
- Access control platform
- User behavior analytics
- Network analytics
- Data logging
- Data storage
- Virtualization

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 Securing Property Management Systems for the Hospitality Sector (for reference, please see the link in the PROCESS section above):

1. Auditing, analytics and response capabilities such as:
  - Complete, near real-time auditing and reporting of activity, including:
    - User behavior analytics
    - Unauthorized access
    - Unauthorized user behavior
    - Network analytics
    - Access requests and decisions
  - Automated detection and/or response to incidents
  - Continuous monitoring and retention of information on component interactions
  - Continuous monitoring and retention of network events
2. System Protection and Authentication capabilities with enforcement such as:
  - Access control for internal and third-party users, including:
    - Access control policy creation
    - Determination of access control decisions based on policies
    - Access control policy enforcement
  - Multifactor Authentication for remote and third-party access
  - Adherence to principles of segmentation and zero-trust, including:
    - Multiple trust zones and logical trust boundaries
    - Network segmentation gateways
    - Network virtualization platform and micro-segmentation
3. Data Protection and Encryption capabilities to prevent damage to PCI/PII confidentiality, as well as the confidentiality and integrity of system data such as:
  - Point-to-point encryption (P2PE)
  - Limited/no storing/processing/transmission of payment card data
  - Secure data tokenization and token management capabilities, including:
    - Token generation

- Token mapping
- Cryptographic key management
- Utilization of a non-PCI, sensitive consumer secure data vault
- Prevention of damage to PCI/PII confidentiality
- Prevention of damage to PMS functionality and security, and improved mitigation of cybersecurity risks
- Secure Payment Terminal
- Payment Information Proxy service

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 Securing Property Management Systems for the Hospitality Sector in NCCoE facilities, which will be conducted in a manner consistent with the following standards and guidance: FIPS 140–2, FIPS 200, FIPS 201, SP 800–53, SP 800–63–3, and Payment Card Industry Data Security Standard (PCI–DSS).

Additional details about the Securing Property Management Systems for the Hospitality Sector use case are available at: <https://nccoe.nist.gov/projects/use-cases/securing-property-management-systems>.

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 Securing Property Management Systems for the Hospitality 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 Hospitality 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 Securing Property Management Systems for the Hospitality

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 Securing Property Management Systems for the Hospitality 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 Securing Property Management Systems across an entire Hospitality 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. 2017-25427 Filed 11-22-17; 8:45 am]

**BILLING CODE 3510-13-P**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

**RIN 0648-XF849**

#### Fisheries of the South Atlantic; South Atlantic Fishery Management Council; Public Meetings

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

**ACTION:** Notice of public meetings.

**SUMMARY:** The South Atlantic Fishery Management Council (Council) will hold a meeting of its Citizen Science Advisory Panel Projects/Topics Management Action Team via webinar.

**DATES:** The Projects/Topics Management Action Team meeting will be held on Monday, December 11, 2017 at 3 p.m. The meeting is scheduled to last approximately 90 minutes. Additional Action Team webinar and plenary webinar dates and times will publish in a subsequent issue in the **Federal Register**.

**ADDRESSES:**

**Meeting address:** The meeting will be held via webinar and are open to members of the public. Webinar registration is required and registration links will be posted to the Citizen Science program page of the Council's Web site at [www.safmc.net](http://www.safmc.net).

**Council address:** South Atlantic Fishery Management Council, 4055 Faber Place Drive, Suite 201, N. Charleston, SC 29405.

**FOR FURTHER INFORMATION CONTACT:** Amber Von Harten, Citizen Science Program Manager, SAFMC; phone: (843) 302-8433 or toll free (866) SAFMC-10; fax: (843) 769-4520; email: [amber.vonharten@safmc.net](mailto:amber.vonharten@safmc.net).

**SUPPLEMENTARY INFORMATION:** The Council created a Citizen Science Advisory Panel Pool in June 2017. The Council appointed members of the Citizen Science Advisory Panel Pool to five Action Teams in the areas of *Volunteers, Data Management, Projects/Topics Management, Finance, and Communication/Outreach/Education* to develop program policies and operations for the Council's Citizen Science Program.

The Action Team will meet to continue work on developing recommendations on program policies and operations to be reviewed by the Council's Citizen Science Committee. Public comment will be accepted at the beginning of the meeting.

Items to be addressed during these meetings:

1. Discuss work on tasks in the Terms of Reference
2. Other Business

#### Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for auxiliary aids should be directed to the council office (see **ADDRESSES**) 3 days prior to the meeting.

**Note:** The times and sequence specified in this agenda are subject to change.

**Authority:** 16 U.S.C. 1801 *et seq.*

Dated: November 17, 2017.

**Tracey L. Thompson,**  
*Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.*

[FR Doc. 2017-25367 Filed 11-22-17; 8:45 am]

**BILLING CODE 3510-22-P**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### Marine Mammals and Endangered Species

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

**ACTION:** Notice; receipt of applications for permit amendments.

**SUMMARY:** Notice is hereby given that the permit holders listed below have applied for an amendment to their Scientific Research Permits.

**DATES:** Written, telefaxed, or email comments must be received on or before December 26, 2017.

**ADDRESSES:** The application and related documents are available for review by selecting "Records Open for Public Comment" from the "Features" box on the Applications and Permits for Protected Species home page, <https://apps.nmfs.noaa.gov>, and then selecting the File No. from the list of available applications.

These documents are also available upon written request or by appointment in the Permits and Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13705, Silver Spring, MD 20910; phone (301) 427-8401; fax (301) 713-0376.

Written comments on this application should be submitted to the Chief, Permits and Conservation Division, at the address listed above. Comments may also be submitted by facsimile to (301) 713-0376, or by email to [NMFS.Pr1Comments@noaa.gov](mailto:NMFS.Pr1Comments@noaa.gov). Please include the File No. in the subject line of the email comment.

Those individuals requesting a public hearing should submit a written request to the Chief, Permits and Conservation Division at the address listed above. The request should set forth the specific reasons why a hearing on the application(s) would be appropriate.

**FOR FURTHER INFORMATION CONTACT:** Shasta McClenahan or Amy Hapeman, (301) 427-8401.

**SUPPLEMENTARY INFORMATION:** The subject amendments to the permits listed below are requested under the authority of the Marine Mammal Protection Act of 1972, as amended (16 U.S.C. 1361 *et seq.*), the regulations governing the taking and importing of marine mammals (50 CFR part 216), the Endangered Species Act of 1973, as amended (16 U.S.C. 1531 *et seq.*), and the regulations governing the taking, importing, and exporting of endangered