funded by USDA (not all bases apply to all programs).

USDA Non-Discrimination Policy

In accordance with Federal civil rights law and U.S. Department of Agriculture (USDA) civil rights regulations and policies, USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family or parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Individuals who require alternative means of communication for program information (for example, braille, large print, audiotape, American Sign Language, etc.) should contact the responsible Agency or USDA TARGET Center at (202) 720–2600 (voice and text telephone (TTY)) or dial 711 for Telecommunicaions Relay Service (both voice and text telephone users can initiate this call from any phone). Additionally, program information may be made available in languages other than English.

To file a program discrimination complaint, complete the USDA Program Discrimination Complaint Form, AD–3027, found online at *https://www.usda.gov/oascr/how-to-file-a-program-discrimination-complaint* and at any USDA office or write a letter addressed to USDA and provide in the letter all the information requested in the form. To request a copy of the complaint form, call (866) 632–9992. Submit your completed form or letter to USDA by mail to: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue SW, Washington, DC 20250–9410 or email: *OAC@usda.gov.USDA* is an equal opportunity provider, employer, and lender.

Dated: May 3, 2023.

Cikena Reid,

Committee Management Officer, USDA.

[FR Doc. 2023–10217 Filed 5–12–23; 8:45 am]

BILLING CODE 3410–16–P

DEPARTMENT OF COMMERCE

International Trade Administration

United States Travel and Tourism Advisory Board: Meeting of the United States Travel and Tourism Advisory Board

AGENCY: International Trade Administration, U.S. Department of Commerce.

ACTION: Notice of an open meeting.

SUMMARY: The United States Travel and Tourism Advisory Board (Board or TTAB) will hold a meeting on Thursday, June 1, 2023. The Board advises the Secretary of Commerce on matters relating to the U.S. travel and tourism industry. The main purpose of this meeting is for Board members to discuss priority issues related to travel and tourism. The final agenda will be posted on the Department of Commerce website for the Board at *https://www.trade.gov/ttab-meetings* at least two days prior to the meeting.

DATES: Thursday, June 1, 2023, 9 a.m.–12 p.m. EDT. The deadline for members of the public to register for the meeting or to submit written comments for dissemination prior to the meeting is 5 p.m. EDT on Tuesday, May 30, 2023.

ADDRESSES: The meeting will be held in person in Washington, DC and virtually. The access information will be provided by email to registrants. Requests to register (including to speak or for auxiliary aids) and any written comments should be submitted by email to *TTAB@trade.gov.*

FOR FURTHER INFORMATION CONTACT: Jennifer Aguinaga, the United States Travel and Tourism Advisory Board, National Travel and Tourism Office, U.S. Department of Commerce; telephone: 202–482–2404; email: *TTAB@trade.gov.*

SUPPLEMENTARY INFORMATION:

Public Participation: The meeting will be open to the public and will be accessible to people with disabilities. Any member of the public requesting to join the meeting is asked to register in advance by the deadline identified under the **DATES** caption. Requests for auxiliary aids must be submitted by the registration deadline. Last minute requests will be accepted but may not be possible to fill. There will be fifteen (15) minutes allotted for oral comments from members of the public joining the meeting. To accommodate as many speakers as possible, the time for public comments may be limited to three (3) minutes per person. Members of the public wishing to reserve speaking time during the meeting must submit a request at the time of registration, as well as the name and address of the proposed speaker. If the number of registrants requesting to make statements is greater than can be reasonably accommodated during the meeting, the International Trade Administration may conduct a lottery to determine the speakers. Speakers are requested to submit a written copy of their prepared remarks by 5 p.m. EDT on Tuesday, May 30, 2023, for inclusion in the meeting records and for circulation to the members of the Board.

In addition, any member of the public may submit pertinent written comments concerning the Board's affairs at any time before or after the meeting. Comments may be submitted to Jennifer Aguinaga at the contact information indicated above. To be considered during the meeting, comments must be received no later than 5 p.m. EDT on Tuesday, May 30, 2023, to ensure transmission to the Board prior to the meeting. Comments received after that date and time will be transmitted to the Board but may not be considered during the meeting. Copies of Board meeting minutes will be available within 90 days of the meeting.

This Notice is published pursuant to the Federal Advisory Committee Act, as amended (FACA), 5 U.S.C. app. 9(c). It has been determined that the Committee is necessary and in the public interest. The Committee was established pursuant to Commerce's authority under 15 U.S.C. 1512, established under the FACA, as amended, 5 U.S.C. app., and with the concurrence of the General Services Administration.

Jennifer Aguinaga,

Designated Federal Officer, United States Travel and Tourism Advisory Board.

[FR Doc. 2023–10234 Filed 5–12–23; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

RIN 0693–XC127

National Cybersecurity Center of Excellence (NCCoE) Software Supply Chain and DevOps Security Practices

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 letters of interest describing products and

technical expertise to support and demonstrate an applied risk-based approach and recommendations for secure DevOps (software development and operations) and software supply chain practices for the *Software Supply Chain and DevOps Security Practices* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address DevOps and software supply chain security challenges identified under the *Software Supply Chain and DevOps Security Practices* project. Participation in the project 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 June 14, 2023.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *devsecops-nist@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can request the letter of interest template by visiting *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices* and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.* 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 NCCoE Cooperative Research and Development Agreement (CRADA) with NIST; a template NCCoE Consortium CRADA can be found at: *https://nccoe.nist.gov/library/nccoe-consortium-crada-example.*

FOR FURTHER INFORMATION CONTACT: Paul Watrobski via email *devsecops-nist@nist.gov,* by telephone at (240) 479–1830, or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Software Supply Chain and DevOps Security Practices* project are available at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.*

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 and document an applied risk-based approach and recommendations for secure DevOps (DevSecOps) and software supply chain practices consistent with the Secure Software Development Framework (SSDF), Cybersecurity Supply Chain Risk Management (C–SCRM), and other NIST, government, and industry guidance. Industry, government, and other organizations could then apply the guidelines when choosing and implementing DevSecOps practices in order to improve the security of the software they develop and operate. That, in turn, would improve the security of the organizations using that software, and so on throughout the software supply chain.

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 an applied risk-based approach and recommendations for secure DevOps (software development and operations) and software supply chain practices for the *Software Supply Chain and DevOps Security Practices* project. The full project can be viewed at: *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.*

Interested parties can access the template for a letter of interest by visiting the project website at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices* and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the 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 in the Requirements for Letters of Interest section below, up to the number of participants in each category necessary to carry out this project. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

When the project has been completed, NIST will post a notice on the *Software Supply Chain and DevOps Security Practices* project website at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices* announcing the completion of the project.

Project Objective

This project's goal is to develop and document an applied risk-based approach and recommendations for DevSecOps practices. This project is intended to help enable organizations to maintain the velocity and volume of software delivery in a cloud-native way and take advantage of automated tools. The project's objective is to produce practical and actionable guidelines that meaningfully integrate security practices into development methodologies. The project intends to demonstrate how an organization can generate artifacts as a byproduct of its DevSecOps practices to support and inform the organization's self-attestation and declaration of conformance to applicable NIST and industry-recommended practices for secure software development and cybersecurity supply chain risk management. The project will also strive to demonstrate the use of current and emerging secure development frameworks, practices, and tools to address cybersecurity challenges.

Project Background

DevOps brings together software development and operations to shorten development cycles, allow organizations to be agile, and maintain the pace of innovation while taking advantage of cloud-native technology and practices. Industry and government have fully embraced and are rapidly implementing these practices to develop and deploy software in operational environments, often without a full understanding and consideration of security. The NCCoE is undertaking a practical demonstration of technology and tools that meaningfully integrate security practices into development methodologies. DevSecOps helps ensure that security is addressed as part of all DevOps practices by integrating security practices and automatically generating security and compliance artifacts throughout the processes and

environments, including software development, builds, packaging, distribution, and deployment. Furthermore, there is increasing recognition of how security concerns inherent in modern day supply chains directly affect the DevOps process. DevSecOps practices can help identify, assess, and mitigate cybersecurity risk for the software supply chain.

Project Activities

To meet the need to accelerate widespread adoption of improved DevOps and software supply chain security practices across various industry sectors, the NCCoE *Software Supply Chain and DevOps Security Practices* project will produce and demonstrate practical and actionable guidelines that meaningfully integrate security practices into development methodologies. Additionally, the project will demonstrate how an organization can generate artifacts as a byproduct of its DevSecOps practices to support and inform the organization's self-attestation and declaration of conformance to applicable NIST and industry-recommended practices for secure software development and cybersecurity supply chain risk management. The project will also strive to demonstrate the use of current and emerging secure development frameworks, practices, and tools to address cybersecurity challenges. Lessons learned during the project will be shared with the security and software development communities to inform improvements to secure development frameworks, practices, and tools. Lessons learned will also be shared with standards developing organizations to inform their DevSecOps-related work. The intention is to demonstrate DevSecOps practices, especially using automation, that would apply to organizations of all sizes and from all sectors, and to development for information technology (IT), operational technology (OT), Internet of Things (IoT), and other technology types.

Project Outcomes

The proposed proof-of-concept solution(s) will integrate free and open source software (FOSS) and closed source software to demonstrate the use case scenarios detailed in Section 2 of the *Software Supply Chain and DevOps Security Practices* project description at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.* This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the practical steps needed to implement a cybersecurity reference design that addresses this challenge. Supporting outputs may include public tools, code, and white papers.

Requirements for Letters of Interest: 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 *Software Supply Chain and DevOps Security Practices* project description at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices* and include, but are not limited to:

- Developer endpoints, including PCs (desktops or laptops) and virtual environments, both PC-based and cloud-based
- Network/infrastructure devices
- Services and applications, both on-premises and cloud-based, including:
  - Toolchains and their tools (build tools, packaging tools, repositories, etc.)
  - Vulnerability management (patch and configuration)
  - Version control software and services
  - Software security review, analysis, and testing tools (*e.g.,* static and dynamic code analyzers, fuzzers, just-in-time secure coding training for developers)
  - Secure software design tools (*e.g.,* threat modeling tools)
  - Memory safe programming languages
- Build systems (test, integration, production)
- Distribution/delivery systems
- Production systems that host apps

Each responding organization's letter of interest should identify how their products help address one or more of the following demonstration scenarios in Section 2 of the *Software Supply Chain and DevOps Security Practices* project description at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices:*

- Free and open source software development
- Closed source software development

In their letters of interest, responding organizations need to acknowledge the importance of and commit to provide:

1. Access for all participants' project teams to DevOps component interfaces and the organization's experts necessary to make functional connections among DevOps components.

2. Support for development and demonstration of the *Software Supply Chain and DevOps Security Practices* project at the NCCoE, which will be conducted in a manner consistent with the most recent version of the following standards and guidance: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800–161) (*https://doi.org/10.6028/NIST.SP.800-161r1*), Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) (*https://www.nist.gov/cyberframework/framework*), and Secure Software Development Framework (SSDF) (NIST SP 800–218) (*https://doi.org/10.6028/NIST.SP.800-218*). Additional details about the *Software Supply Chain and DevOps Security Practices* project are available at *https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.*

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 NCCoE consortium CRADA in the development of the *Software Supply Chain and DevOps Security Practices* project. 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 DevSecOps proof-of-concept builds and their characteristics sufficient to permit other organizations to develop and deploy DevSecOps practices that meet the objectives of the *Software Supply Chain and DevOps Security Practices* project. These descriptions will be public information.

Under the terms of the NCCoE 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, platform documentation, and demonstration activities.

The dates of the demonstration of the *Software Supply Chain and DevOps Security Practices* project capability will

be announced on the NCCoE website at least two weeks in advance at *https://nccoe.nist.gov/*. The expected outcome will demonstrate how the components of the solutions that address *Software Supply Chain and DevOps Security Practices* can enhance capabilities that provide assurance of management of identified risks while continuing to meet industry sectors' compliance requirements. 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 website *https://nccoe.nist.gov/*.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2023–10221 Filed 5–12–23; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Evaluation of Heeia National Estuarine Research Reserve; Notice of Public Meeting; Request for Comments

AGENCY: Office for Coastal Management, National Ocean Service, National Oceanic and Atmospheric Administration, Department of Commerce.

ACTION: Notice of public meeting and opportunity to comment.

SUMMARY: The National Oceanic and Atmospheric Administration (NOAA), Office for Coastal Management, will hold an in-person public meeting to solicit input on the performance evaluation of the Heeia National Estuarine Research Reserve. NOAA also invites the public to submit written comments.

DATES: NOAA will hold an in-person public meeting on Tuesday, June 6, 2023, at 6 p.m. Hawaii Standard Time. NOAA will consider all relevant written comments received by Friday, June 16, 2023.

ADDRESSES: Comments may be submitted by one of the following methods:

- *In-Person Public Meeting:* Provide oral comments during the in-person public meeting on Tuesday, June 6, 2023, at 6 p.m. Hawaii Standard Time at Kakoo Oiwi, 46–406 Kamehameha Hwy., Kaneohe, HI 96744.
- *Email:* Send written comments to Michael Migliori, Evaluator, NOAA Office for Coastal Management, at *Michael.Migliori@noaa.gov.* Include ''Comments on Performance Evaluation of Heeia National Estuarine Research Reserve'' in the subject line of the message. NOAA will accept anonymous comments; however, the written comments NOAA receives are considered part of the public record, and the entirety of the comment, including the name of the commenter, email address, attachments, and other supporting materials, will be publicly accessible. Sensitive personally identifiable information, such as account numbers and Social Security numbers, should not be included with the comments. Comments that are not related to the performance evaluation of the Heeia National Estuarine Research Reserve or that contain profanity, vulgarity, threats, or other inappropriate language will not be considered.

FOR FURTHER INFORMATION CONTACT: Michael Migliori, Evaluator, NOAA Office for Coastal Management, by email at *Michael.Migliori@noaa.gov* or by phone at (443) 332–8936. A copy of the reserve management plan, may be viewed and downloaded at *http://coast.noaa.gov/czm/evaluations/*. A copy of the evaluation notification letter and most recent progress report may be obtained upon request by contacting Michael Migliori.

SUPPLEMENTARY INFORMATION: Section 315(f) of the Coastal Zone Management Act (CZMA) requires NOAA to conduct periodic evaluations of federally approved national estuarine research reserves. The evaluation process includes holding one or more public meetings, considering public comments, and consulting with interested Federal, State, and local agencies and members of the public. During the evaluation, NOAA will consider whether the management and operation of the reserve is deficient and whether the research at the reserve is consistent with the research guidelines developed under section 315(c) of the CZMA. When the evaluation is complete, NOAA's Office for Coastal Management will place a notice in the **Federal Register** announcing the availability of the final evaluation findings.

(Authority: 16 U.S.C. 1461)

Keelin Kuipers,

Deputy Director, Office for Coastal Management, National Ocean Service, National Oceanic and Atmospheric Administration.

[FR Doc. 2023–10258 Filed 5–12–23; 8:45 am]

BILLING CODE 3510–JE–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XC920]

Determination of Overfishing or an Overfished Condition

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

ACTION: Notice.

SUMMARY: This action serves as a notice that NMFS, on behalf of the Secretary of Commerce (Secretary), has found that Pacific sardine is still overfished. NMFS, on behalf of the Secretary, is required to provide this notice whenever it determines that a stock or stock complex is subject to overfishing, overfished, or approaching an overfished condition.

FOR FURTHER INFORMATION CONTACT: Caroline Potter, (301) 427–8522.

SUPPLEMENTARY INFORMATION: Pursuant to section 304(e)(2) of the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act), 16 U.S.C. 1854(e)(2), NMFS, on behalf of the Secretary, must publish a notice in the **Federal Register** whenever it determines that a stock or stock complex is subject to overfishing, overfished, or approaching an overfished condition.

NMFS has determined that Pacific sardine remains overfished. This determination is based on an update assessment completed in 2022 using data through 2021, which indicates that the stock remains overfished because the biomass is less than the minimum stock size threshold. NMFS continues to work with the Pacific Fishery Management Council to rebuild the Pacific sardine stock.

Dated: May 10, 2023.

Jennifer M. Wallace,

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

[FR Doc. 2023–10320 Filed 5–12–23; 8:45 am]

BILLING CODE 3510–22–P

U.S. INTERNATIONAL DEVELOPMENT FINANCE CORPORATION

Notice of Public Hearing

AGENCY: U.S. International Development Finance Corporation.

ACTION: Announcement of public hearing.

SUMMARY: The Board of Directors of the U.S. International Development Finance