Filing Information

As a courtesy, we are making information related to sunset proceedings, including copies of the pertinent statute and Commerce's regulations, Commerce's schedule for Sunset Reviews, a listing of past revocations and continuations, and current service lists, available to the public on Commerce's website at the following address: *https://enforcement.trade.gov/sunset/.* All submissions in these Sunset Reviews must be filed in accordance with Commerce's regulations regarding format, translation, and service of documents. These rules, including electronic filing requirements via Enforcement and Compliance's Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS), can be found at 19 CFR 351.303.

In accordance with section 782(b) of the Act, any party submitting factual information in an AD/CVD proceeding must certify to the accuracy and completeness of that information. Parties must use the certification formats provided in 19 CFR 351.303(g). Commerce intends to reject factual submissions if the submitting party does not comply with applicable revised certification requirements.

Letters of Appearance and Administrative Protective Orders

Pursuant to 19 CFR 351.103(d), Commerce will maintain and make available a public service list for these proceedings. Parties wishing to participate in any of these five-year reviews must file letters of appearance as discussed at 19 CFR 351.103(d). To facilitate the timely preparation of the public service list, it is requested that those seeking recognition as interested parties to a proceeding submit an entry of appearance within 10 days of the publication of the Notice of Initiation. Because deadlines in Sunset Reviews can be very short, we urge interested parties who want access to proprietary information under administrative protective order (APO) to file an APO application immediately following publication in the **Federal Register** of this notice of initiation. Commerce's regulations on submission of proprietary information and eligibility to receive access to business proprietary information under APO can be found at 19 CFR 351.304–306. Note that Commerce has temporarily modified certain of its requirements for serving documents containing business proprietary information, until further notice.[1]

Information Required From Interested Parties

Domestic interested parties, as defined in section 771(9)(C), (D), (E), (F), and (G) of the Act and 19 CFR 351.102(b), wishing to participate in a Sunset Review must respond not later than 15 days after the date of publication in the **Federal Register** of this notice of initiation by filing a notice of intent to participate. The required contents of the notice of intent to participate are set forth at 19 CFR 351.218(d)(1)(ii). In accordance with Commerce's regulations, if we do not receive a notice of intent to participate from at least one domestic interested party by the 15-day deadline, Commerce will automatically revoke the order without further review.[2]

If we receive an order-specific notice of intent to participate from a domestic interested party, Commerce's regulations provide that *all parties* wishing to participate in a Sunset Review must file complete substantive responses not later than 30 days after the date of publication in the **Federal Register** of this notice of initiation. The required contents of a substantive response, on an order-specific basis, are set forth at 19 CFR 351.218(d)(3). Note that certain information requirements differ for respondent and domestic parties. Also, note that Commerce's information requirements are distinct from the ITC 's information requirements. Consult Commerce's regulations for information regarding Commerce's conduct of Sunset Reviews. Consult Commerce's regulations at 19 CFR part 351 for definitions of terms and for other general information concerning antidumping and countervailing duty proceedings at Commerce.

This notice of initiation is being published in accordance with section 751(c) of the Act and 19 CFR 351.218(c).

Dated: August 16, 2021.

James Maeder,
Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.
[FR Doc. 2021–18922 Filed 8–31–21; 8:45 am]
BILLING CODE 3510–DS–P

---

[1] *See Temporary Rule Modifying AD/CVD Service Requirements Due to* COVID–19, 85 FR 41363 (July 10, 2020).

[2] *See* 19 CFR 351.218(d)(1)(iii).

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 210826–0169]

National Cybersecurity Center of Excellence (NCCoE) Automation of the Cryptographic Module Validation Program (CMVP)

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 security platforms for the *Automation of the Cryptographic Module Validation Program (CMVP)* project. 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 October 1, 2021.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *applied-crypto-testing@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest template by visiting *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation* and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it will no longer accept letters of interest for this project at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.* Organizations whose letters of interest are accepted will be asked to sign a consortium Cooperative Research and Development Agreement (CRADA) with NIST; a template CRADA can be found at: *https://nccoe.nist.gov/library/nccoe-consortium-crada-example.*

FOR FURTHER INFORMATION CONTACT:
Apostol Vassilev via phone (301) 975–3221 or email *applied-crypto-testing@nist.gov;* by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Automation of the Cryptographic Module Validation Program (CMVP)* project are available at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.*

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 *Automation of the Cryptographic Module Validation Program (CMVP)* project. The full project can be viewed at: *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.*

Interested parties can access the template for a letter of interest by visiting the project website at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation* 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 below, up to the number of participants in each category necessary to carry out this project. When the project has been completed, NIST will post a notice on the *Automation of the Cryptographic Module Validation Program (CMVP)* project website at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation* announcing the completion of the project and informing the public that it will no longer accept letters of interest for this project.

Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

Objective: The Cryptographic Module Validation Program (CMVP) validates third-party assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140–3, *Security Requirements for Cryptographic Modules.* Current industry cryptographic product development, production, and maintenance processes place significant emphasis on time-to-market efficiency. A number of elements of the validation process are manual in nature, and the period required for third-party testing and government validation of cryptographic modules is often incompatible with industry requirements. The purpose of the project is to demonstrate the value and practicality of automation to improve the efficiency and timeliness of CMVP operation and processes. The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Automation of the Cryptographic Module Validation Program (CMVP)* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.* 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 implementation.

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 *Automation of the Cryptographic Module Validation Program (CMVP)* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation* and include, but are not limited to:

- Validation authority server
- ACV proxy server
- ACV client
- Hardware or software cryptographic modules
- Host processors for software cryptographic modules
- Network devices supporting web-based exchange of information in JSON format
- Harnesses for integration of ACV clients with hardware or software cryptographic modules
- Automated cryptographic module testing expertise

Each responding organization's letter of interest should identify how its products help address one or more of the following desired characteristics and properties in section 1 of the *Automation of the Cryptographic Module Validation Program (CMVP)* project description at *https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation:*

- Support necessary schemas and protocols for evidence submission and validation for a scalable application programming interface (API) based architecture
- Support standard tests for the functional tests of specific classes of technologies (*e.g.,* software modules) and corresponding reporting of functional and non-functional security requirements
- Be compatible with an infrastructure required to support a new automated validation program architecture
- Include reusable test harnesses for test automation for different types of modules within the program architecture
- Support maintaining validation within a changing operational environment
- Support validation in third-party operational environments (*e.g.,* cloud providers, contracted environments)
- Support identification of positive and negative impacts that the new automation program may have on cryptographic product development,

production, integration, and testing organizations, including lessons learned

- Contribute to recommend policies and best practices for the automated validation scope in appropriate NIST documents
- Support a roadmap for migrating organizations and their customers from the current human-effort-centric CMVP to the new automated program, including recommended practices based on lessons learned
- Broadly support improvements in cryptographic modules across all vendors participating in the CMVP through voluntary sharing of test data (*e.g.,* seeds or test vectors) that result in failures to improve regression testing for module vendors

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 component interfaces and the organization's experts necessary to make functional connections among security platform components.

2. Support for development and demonstration of the Automation of the Cryptographic Module Validation Program (CMVP) project, which will be based on the most recent versions of FIPS 140, SP 800–140, and Handbook (HB) 150–17 and conducted in a manner consistent with the most recent version of the following standards and guidance: FIPS 200, SP 800–37, SP 800–52, SP 800–53, SP 800–63, and SP 1800–16. Additional details about the *Automation of the Cryptographic Module Validation Program (CMVP)* project are available at *https:// www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation.*

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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the *Automation of the Cryptographic Module Validation Program (CMVP)* project. 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 *Automation of the Cryptographic Module Validation Program (CMVP)* 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 *Automation of the Cryptographic Module Validation Program (CMVP)* can enhance security capabilities that provide assurance of mitigation 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. 2021–18868 Filed 8–31–21; 8:45 am]
BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XB327]

Takes of Marine Mammals Incidental to Specified Activities; Taking Marine Mammals Incidental to the Fuel Pier Inboard Pile Removal Project in San Diego, California

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

ACTION: Notice; issuance of an Incidental Harassment Authorization.

SUMMARY: In accordance with the regulations implementing the Marine Mammal Protection Act (MMPA) as amended, notification is hereby given that NMFS has issued an IHA to the United States Navy to incidentally harass, by Level B harassment only, marine mammals during pile driving/ removal activities associated with the Fuel Pier Inboard Pile Removal Project in San Diego Bay, California.

DATES: This Authorization is effective from January 15, 2022 through January 14, 2023.

FOR FURTHER INFORMATION CONTACT: Kelsey Potlock, Office of Protected Resources, NMFS, (301) 427–8401. Electronic copies of the application and supporting documents, as well as a list of the references cited in this document, may be obtained online at: *https:// www.fisheries.noaa.gov/action/ incidental-take-authorization-us-navy-fuel-pier-removal-naval-base-san-diego-california.* In case of problems accessing these documents, please call the contact listed above.

SUPPLEMENTARY INFORMATION:

Background

The MMPA prohibits the "take" of marine mammals, with certain exceptions. Sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 *et seq.*) direct the Secretary of Commerce (as delegated to NMFS) to allow, upon request, the incidental, but not intentional, taking of small numbers of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) within a specified geographical region if certain findings are made and either regulations are issued or, if the taking is limited to harassment, a notice of a proposed incidental take authorization may be provided to the public for review.

Authorization for incidental takings shall be granted if NMFS finds that the taking will have a negligible impact on the species or stock(s) and will not have an unmitigable adverse impact on the availability of the species or stock(s) for taking for subsistence uses (where relevant). Further, NMFS must prescribe the permissible methods of taking and other "means of effecting the least practicable adverse impact" on the affected species or stocks and their habitat, paying particular attention to rookeries, mating grounds, and areas of similar significance, and on the availability of the species or stocks for taking for certain subsistence uses (referred to in shorthand as