expanding domain with a range of applications and a broad diversity of designs. NIST's Engineering Laboratory will be developing methods to evaluate performance of exoskeletons in two key areas (1) The fit and motion of the exoskeleton device with respect to the users' body and (2) The impact that using an exoskeleton has on the performance of users executing tasks that are representative of activities in industrial settings. The results of these experiments will inform future test method development at NIST, other organizations, and under the purview of the new American Society for Testing Materials (ASTM) Committee F48 on Exoskeletons and Exosuits.

For the first research topic, NIST will evaluate the usefulness of a NIST prototype apparatus for measuring the difference in performance of a person wearing an exoskeleton versus the person's baseline without the exoskeleton while positioning loads and tools. The NIST Position and Load Test Apparatus for Exoskelons (PoLoTAE), which presents abstractions of industrial task challenges, will be evaluated in this research.

For the second research topic, NIST will evaluate a method for measuring the alignment of an exoskeleton to human joint (knee) and any relative movement between the exoskeleton and user. Measurement methods prototyped by NIST for evaluating exoskeleton on mannequin position and motion will be applied to human subjects to verify the usefulness of optical tracking system and designed artifacts worn by users as measurement methods.

Participants will be chosen from volunteers within NIST and adult NIST visitors to participate in the study. Gender and size diversity will be sought in the population of participants. No personally identifiable information (PII) will be recorded unless subject consent for PII disclosure is received. NIST intends to publish information on the analysis and results.

II. Method of Collection

Participants will give informed consent prior to participating in the research. Information may be collected via a paper background questionnaire which may include disclosure of health information which may be relevant for safety and research reasons. Data will be collected using a combination of heart rate monitor, and video and still cameras to collect time and subject activity to correlate heart rate with activity and an optical tracking system which detects markers. Participants will be asked to complete a paper survey once data is collected for the research.

III. Data

OMB Control Number: 0693–0083.

Form Number(s): None.

Type of Review: Revision and extension of a current information collection.

Affected Public: Individuals or households.

Estimated Number of Respondents: 250.

Estimated Time per Response: 1.5 hours.

Estimated Total Annual Burden Hours: 375 hours.

Estimated Total Annual Cost to Public: $0.

IV. Request for Comments

NIST invites comments on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Sheleen Dumas,

Departmental Lead PRA Officer, Office of the Chief Information Officer, Commerce Department.

[FR Doc. 2019–08816 Filed 4–30–19; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 170810743–8858–01]

RIN 0693–XC079

Announcing Issuance of Federal Information Processing Standard (FIPS) 140–3, Security Requirements for Cryptographic Modules

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's issuance of Federal Information Processing Standard (FIPS) 140–3, Security Requirements for Cryptographic Modules. FIPS 140–3 includes references to existing International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012(E) *Information technology—Security techniques—Security requirements for cryptographic modules* and ISO/IEC 24759:2017(E) *Information technology—Security techniques—Test requirements for cryptographic modules.* As permitted by the standards, the NIST Special Publication (SP) series 800–140 will specify updates, replacements, or additions to the currently cited ISO/IEC standard as necessary.

DATES: FIPS 140–3 is effective September 22, 2019. FIPS 140–3 testing will begin on September 22, 2020. FIPS 140–2 testing will continue for at least a year after FIPS 140–3 testing begins.

ADDRESSES: FIPS 140–3 is available electronically from the NIST website at: *https://csrc.nist.gov/publications/fips*. Comments that were received on the proposed changes are also published electronically at *https://csrc.nist.gov/projects/fips-140-3-development.*

FOR FURTHER INFORMATION CONTACT: Michael Cooper, (301) 975–8077, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *michael.cooper@nist.gov*.

SUPPLEMENTARY INFORMATION: NIST has been participating in the ISO/IEC process for developing standards for cryptographic modules and working closely with international industry to unify several cryptographic security standards. ISO/IEC 19790:2012(E), *Information technology—Security techniques—Security requirements for cryptographic modules,* is an international standard based on updates of the earlier versions of FIPS 140, *Security Requirements for Cryptographic Modules.* ISO/IEC 24759:2017(E), *Information technology—Security techniques—Test requirements for cryptographic modules* is an international standard based on the Derived Test Requirements for FIPS 140–2, *Security Requirements for Cryptographic Modules.* The National Technology Transfer and Advancement Act (NTTAA), Public Law 104–113, directs Federal agencies with respect to their use of and participation in the development of voluntary consensus standards. The NTTAA's objective is for Federal agencies to adopt voluntary consensus standards, wherever possible, in lieu of creating proprietary, non-consensus standards. The implementation of commercial

cryptography, which is used to protect U.S. non-national security information and information systems, is now commoditized and built, marketed and used globally. Therefore, FIPS 140–3 applies ISO/IEC 19790:2012(E) and ISO/IEC 24759:2017(E) as the security requirements for cryptographic modules. The SP 800–140 series, which is currently under development, will be used to specify updates, replacements, or additions to requirements as allowed by ISO/IEC 19790:2012(E), with the Cryptographic Module Validation Program (CMVP) executing the role of the validation authority as defined in the ISO/IEC standard.[1] During the transition period prior to FIPS 140–3 becoming effective, FIPS 140–2 testing will continue, and NIST will introduce the SP 800–140 series documents (at *https://csrc.nist.gov/publications/sp800*). The series is expected to consist of:

- SP 800–140, *FIPS 140–3 Derived Test Requirements (DTR);*
- SP 800–140A, *CMVP Documentation Requirements;*
- SP 800–140B, *CMVP Security Policy Requirements;*
- SP 800–140C, *CMVP Approved Security Functions;*
- SP 800–140D, *CMVP Approved Sensitive Security Parameter Generation and Establishment Methods;*
- SP 800–140E, *CMVP Approved Authentication Mechanisms;* and
- SP 800–140F, *CMVP Non-Invasive Attack Mitigation Test Metrics*.

FIPS 140–1, first published in 1994, was developed by a government and industry working group. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (*e.g.,* low value administrative data, million-dollar funds transfers, and life protecting data) and a diversity of application environments (*e.g.,* a guarded facility, an office, and a completely unprotected location). Four security levels were specified for each of 11 requirement areas. Each security level offered an increase in security over the preceding level. These four increasing levels of security allowed cost-effective solutions that were appropriate for different degrees of data sensitivity and different application environments.

In 2001, FIPS 140–2 superseded FIPS 140–1. FIPS 140–2 incorporated changes in applicable standards and technology since the development of FIPS 140–1 as well as changes that were based on comments received from the public. Though the standard was reviewed after five years, consensus to move forward was not achieved until the 2012 revision of ISO/IEC 19790.

FIPS 140–3 supercedes FIPS 140–2. FIPS 140–3 aligns with ISO/IEC 19790:2012(E) with modifications of the Annexes allowed by the specific user communities. The testing for these requirements shall be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2 of ISO/IEC 24759:2017(E).

On August 12, 2015, NIST published a notice in the **Federal Register** (80 FR 48295) requesting public comments on the potential use of ISO/IEC standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by FIPS 140–2. Comments were submitted by 17 entities, including four accredited cryptographic testing laboratories, eight vendors of cryptographic modules, one industry association, and four individuals. Some comments only addressed specific aspects of the proposal. Eleven of the comments supported a revised standard, five were neutral and one was opposed. Many comments asked for clarification on the continued use of implementation guidance and administration guidance to the testing laboratories. NIST will consolidate the implementation guidance and administration guidance into the SP 800–140 series documents, which will be made available for public review and comment. Other comments provided feedback on perceived market demand, comparisons of test coverage between FIPS 140–2 and the ISO/IEC standards and the potential risks that might be assumed with the use of the ISO/IEC standard. Most of the commenters were concerned about the payment model for accessing and obtaining the ISO/IEC standards compared with the free access to the current FIPS 140–2. All of the suggestions, questions, and recommendations within the scope of NIST's request for comments were carefully reviewed, and changes were made to the FIPS, where appropriate. Some comments submitted questions or raised issues that were related but outside the scope of this FIPS. Comments that were outside the scope of this FIPS, but that were within the scope of one of the related Special Publications, are deferred for later consideration in the context of development of the SP 800–140 series.

The following is a summary and analysis of the comments received during the public comment period, and NIST's responses to them, including the interests, concerns, recommendations, and issues considered in the development of FIPS 140–3:

Comment: Nine commenters responded that they have been asked by customers about testing for ISO/IEC standards or have had requests to test using the ISO/IEC standard.

Response: NIST will be revising its guidance by moving to the ISO/IEC standards embraced in FIPS 140–3.

Comment: Seven commenters responded that they were concerned about the ability of researchers, academics and small organizations to obtain the ISO/IEC standard due to the payment model used by ISO/IEC.

Response: NIST intends to work with the appropriate parties to help ensure that the ISO/IEC standard will be made reasonably available to researchers, academics and small organizations.

Comment: Eleven commenters indicated that changing to the ISO/IEC standard did not increase the risk of using cryptography or decrease trust in the use of cryptography as compared to the current FIPS 140–2.

Response: NIST intends to make the normative reference to the ISO/IEC standard specific to a version that NIST believes is acceptable to provide assurances in the cryptography used by the Federal Government. In its role as the approval authority[2] under ISO/IEC 19790:2012(E), NIST is permitted to replace most of the supporting requirements with NIST guidance, most of which are currently utilized in the existing FIPS 140–2.

Comment: One commenter expressed concern that adoption of an international, consensus based standard would put the US in the position of using future versions of the ISO/IEC standard as it is updated and evolves.

Response: NIST plans on continuing its robust participation in the relevant ISO/IEC working groups, and will thoroughly discuss any changes necessary to keep these requirements relevant. If an update or change is made to the ISO/IEC standards that NIST does not feel is adequate for the security needs of the Federal Government, NIST will have the flexibility to adopt a different standard. By working with ISO/IEC experts, NIST can maintain flexibility within the standards as allowed by the validation authorities as

[1] ISO/IEC 19790 defines the validation authority as the entity that will validate the test results for conformance to this international standard.

[2] ISO/IEC 19790 defines the approval authority as any national or international organization/authority mandated to approve and/or evaluate security functions.

described in the ISO/IEC standards. Should these measures prove insufficient, NIST can, through FIPS 140–3 or the SP 800–140 series development process, create a revised standard, controlled by NIST, to maintain the most secure posture possible.

FIPS 140–3 is available electronically from the NIST website at: *https://csrc.nist.gov/publications/fips*.

Authority: 44 U.S.C. 3553(f)(1), 15 U.S.C. 278g–3.

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2019–08817 Filed 4–30–19; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XG874

Taking of Marine Mammals Incidental to Specific Activities; Taking of Marine Mammals Incidental to Pile Driving and Removal Activities During Construction of a Cruise Ship Berth, Hoonah, Alaska

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

ACTION: Notice; proposed incidental harassment authorization; request for comments on proposed authorization and possible renewal.

SUMMARY: NMFS has received a request Duck Point Development II, LLC. (DPD) for authorization to take marine mammals incidental pile driving and removal activities during construction of a second cruise ship berth and new lightering float at Cannery Point (Icy Strait) on Chichagof Island near Hoonah, Alaska. Pursuant to the Marine Mammal Protection Act (MMPA), NMFS is requesting comments on its proposal to issue an incidental harassment authorization (IHA) to incidentally take marine mammals during the specified activities. NMFS is also requesting comments on a possible one-year renewal that could be issued under certain circumstances and if all requirements are met, as described in *Request for Public Comments* at the end of this notice. NMFS will consider public comments prior to making any final decision on the issuance of the requested MMPA authorizations and agency responses will be summarized in the final notice of our decision.

DATES: Comments and information must be received no later than May 31, 2019.

ADDRESSES: Comments should be addressed to Jolie Harrison, Chief, Permits and Conservation Division, Office of Protected Resources, National Marine Fisheries Service. Physical comments should be sent to 1315 East-West Highway, Silver Spring, MD 20910 and electronic comments should be sent to *ITP.Egger@noaa.gov*.

Instructions: NMFS is not responsible for comments sent by any other method, to any other address or individual, or received after the end of the comment period. Comments received electronically, including all attachments, must not exceed a 25-megabyte file size. Attachments to electronic comments will be accepted in Microsoft Word or Excel or Adobe PDF file formats only. All comments received are a part of the public record and will generally be posted online at *https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection*-act without change. All personal identifying information (*e.g.,* name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

FOR FURTHER INFORMATION CONTACT: Stephanie Egger, 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/permit/incidental-take-authorizations-under-marine-mammal-protection-act*. 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 such species or stocks for taking for certain subsistence uses (referred to in shorthand as ''mitigation''); and requirements pertaining to the mitigation, monitoring and reporting of such takings are set forth.

National Environmental Policy Act

To comply with the National Environmental Policy Act of 1969 (NEPA; 42 U.S.C. 4321 *et seq.*) and NOAA Administrative Order (NAO) 216–6A, NMFS must review our proposed action (*i.e.,* the issuance of an incidental harassment authorization) with respect to potential impacts on the human environment. This action is consistent with categories of activities identified in Categorical Exclusion B4 (incidental harassment authorizations with no anticipated serious injury or mortality) of the Companion Manual for NOAA Administrative Order 216–6A, which do not individually or cumulatively have the potential for significant impacts on the quality of the human environment and for which we have not identified any extraordinary circumstances that would preclude this categorical exclusion. Accordingly, NMFS has preliminarily determined that the issuance of the proposed IHA qualifies to be categorically excluded from further NEPA review.

We will review all comments submitted in response to this notice prior to concluding our NEPA process or making a final decision on the IHA request.

Summary of Request

On December 28, 2018 NMFS received a request DPD for an IHA to take marine mammals incidental to pile driving and removal activities during construction of a second cruise ship berth and new lightering float at Cannery Point (Icy Strait) on Chichagof Island near Hoonah, Alaska. The application was deemed adequate and complete on April 3, 2019. The applicant's request is for take nine species of marine mammals by Level B harassment and three species by Level A harassment. Neither DPD nor NMFS