Comment: One commenter agreed with the inclusion of the Extendable-Output Functions in Draft FIPS 202, citing the TUAK algorithm—for authentication and key generation in mobile telephony—as a suitable application.

Response: NIST acknowledges the comment. No change to the Standard was made as a result of the comment.

Comment: Two commenters recommended a significant restructuring of Draft FIPS 202. One commenter's proposal was to emphasize the role of the Keccak-*p* permutation as a ''primitive,'' *i.e.,* a fundamental cryptographic technique. This permutation family is the main component of each SHA–3 function. The comment included a detailed outline of the commenter's proposal. The other commenter's proposal was to replace FIPS 202 with three standards. The first standard would specify the Keccak[*c*] sponge functions as a distinct primitive, and the second and third standards would specify the SHA–3 hash functions and extendable-output functions, respectively, as instances of these sponge functions. For both commenters, the rationale for their proposals was to provide greater flexibility to extend the technology in the future.

Response: The restructuring proposals were not accepted. The text in Section 7 on conformance already explicitly accommodates the possibility of developing new uses of the Keccak[*c*] sponge functions and other intermediate functions, as well as new functions based on the Keccak-*p* permutations. Moreover, the primary purpose of FIPS 202 is to standardize the winning algorithm from the SHA–3 competition. Both of the restructuring proposals would detract from the perception of the Standard as fulfilling that goal.

Comment: One of the previous commenters also submitted several editorial comments and one general comment on Draft FIPS 202. The general comment suggested that hyphens be inserted into the names ''SHAKE128'' and ''SHAKE256'' in order to separate the numerical parameter, which would be consistent with the naming convention for the SHA–3 hash functions.

Response: The editorial comments were accepted, with a modification to the suggested resolution in one case. In particular, the commenter observed that the following sentence in Section 3 could be clarified to distinguish between the input, which is fixed, and the state, which is mutable: ''The set of values for the *b*-bit input to the permutation, as it undergoes successive applications of the step mappings, culminating in the output, is called the state.'' The commenter suggested the following replacement: ''The permutation, as it undergoes successive applications of the step mappings, maintains a *b*-bit state, which is initially set to the input values.'' Instead, NIST revised the sentence as follows: ''The permutation is specified in terms of an array of values for *b* bits that is repeatedly updated, called the *state;* the state is initially set to the input values of the permutation.'' This revision is preferable because it retains an explicit definition of the term ''state.'' NIST did not include the change requested in the general comment. Although the stated rationale for the general comment is reasonable, it is preferable to omit the hyphens, as originally specified, in order to help distinguish the different roles of the parameters. In particular, the numerical suffixes in ''SHAKE128'' and ''SHAKE256'' indicate security strengths, while for the SHA–3 hash functions such as SHA3–256, the suffix indicates the digest length of the hash function.

Comment: One commenter requested that FIPS 202 clarify how the SHA–3 hash functions would be implemented within the keyed-hash message authentication code (HMAC) that is specified in FIPS 198–1.

Response: The comment was accepted and addressed with new text in the conformance section that identified the value of the HMAC parameter *B* for each of the SHA–3 hash functions.

Comment: One commenter expressed appreciation for the opportunity to review Draft FIPS 202.

Response: NIST acknowledges the comment. No change was made as a result of the comment.

Comment: One commenter discussed the use of the extendable-output functions specified in Draft FIPS 202. The comment distinguished between two types of applications: (1) Variable-length hash functions, and (2) random-looking functions, such as key derivation functions (KDFs). The comment explained why variable-length hash functions were not very interesting from a cryptographic perspective, suggesting that NIST approval be limited to KDF-like functions. The comment also pointed out that the incorporation of the output length into the input for these functions could be specified as a method of addressing the prefix property that is discussed in the Standard.

Response: The text in Section 7 on conformance explicitly asserts that approved uses of the extendable-output functions will be specified in NIST special publications. NIST will consider the commenter's suggestions in the development of those publications. Also, text was added to clarify that extendable-output functions are not yet approved as variable-length hash functions.

Comment: The only comment on FIPS 180–4 recommended that the SHA–1 hash algorithm be excluded ''due to highly untrusted security algorithm.''

Response: NIST made no change based on this comment. The comment does not directly apply to the Revised Applicability Clause of FIPS 180–4, which simply acknowledges that FIPS 202 specifies valid options for secure hash functions. Moreover, NIST has already developed and adopted an appropriate policy for the use of SHA–1, based on the latest security information, as described in NIST Special Publication 800–131A.

The Secretary of Commerce hereby approves FIPS 202 and FIPS 180–4. Copies of FIPS 202 and FIPS 180–4 are available at: *http://csrc.nist.gov/publications/PubsFIPS.html.*

Authority: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107–347), the Secretary of Commerce is authorized to approve FIPS. NIST activities to develop computer security standards to protect federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended.

Richard R. Cavanagh,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2015–19181 Filed 8–4–15; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE074

Atlantic Highly Migratory Species; Meeting of the Atlantic Highly Migratory Species Advisory Panel

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

ACTION: Notice of public meeting and webinar/conference call.

SUMMARY: NMFS will hold a 2-day Atlantic Highly Migratory Species (HMS) Advisory Panel (AP) meeting in

September 2015. The intent of the meeting is to consider options for the conservation and management of Atlantic HMS. The meeting is open to the public.

DATES: The AP meeting and webinar will be held from 9 a.m. to 6 p.m. on Wednesday, September 9, 2015; and from 8:30 a.m. to 12 p.m. on Thursday, September 10, 2015.

ADDRESSES: The meeting will be held at the Sheraton Silver Spring, 8777 Georgia Avenue, Silver Spring, MD 20910. The meeting presentations will also be available via WebEx webinar/conference call.

On Wednesday, September 9, 2015, the conference call information is phone number 1–800–857–6552; Participant Code: 8099565; and the webinar event address is: *https://noaaevents2.webex.com/noaaevents2/onstage/g.php?d=393951018&t=a*; event password: NOAA.

On Thursday, September 10, 2015, the conference call information is phone number 1–800–857–6552; Participant Code: 8099565; and the webinar event address is: *https://noaaevents2.webex.com/noaaevents2/onstage/g.php?d=395887510&t=a*; event password: NOAA.

Participants are strongly encouraged to log/dial in fifteen minutes prior to the meeting. NMFS will show the presentations via webinar and allow public comment during identified times on the agenda.

FOR FURTHER INFORMATION CONTACT: LeAnn Hogan or Margo Schulze-Haugen at (301) 427–8503.

SUPPLEMENTARY INFORMATION: The Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.,* as amended by the Sustainable Fisheries Act, Public Law 104–297, provided for the establishment of an AP to assist in the collection and evaluation of information relevant to the development of any Fishery Management Plan (FMP) or FMP amendment for Atlantic HMS. NMFS consults with and considers the comments and views of AP members when preparing and implementing FMPs or FMP amendments for Atlantic tunas, swordfish, billfish, and sharks.

The AP has previously consulted with NMFS on: Amendment 1 to the Billfish FMP (April 1999); the HMS FMP (April 1999); Amendment 1 to the HMS FMP (December 2003); the Consolidated HMS FMP (October 2006); and Amendments 1, 2, 3, 4, 5a, 5b, 6, 7, 8, and 9 to the 2006 Atlantic Consolidated HMS FMP (April and October 2008, February and September 2009, May and September 2010, April and September 2011, March and September 2012, January and September 2013, April and September 2014 and March 2015), among other things.

The intent of this meeting is to consider alternatives for the conservation and management of all Atlantic tunas, swordfish, billfish, and shark fisheries. We anticipate discussing Final Amendment 6 to the 2006 Consolidated HMS FMP on the future of shark fishery, providing updates on Amendment 5b on dusky shark management and Amendment 9 on smoothhound shark management, reviewing the results of the smoothhound shark stock assessment, discussing implementation of Final Amendment 7 on bluefin tuna management measures, as well as discussing the Final HMS Essential Fish Habitat 5-Year Review and next steps. The meeting will also include discussion of a survey of Atlantic HMS tournaments that is in development, and providing updates on various topics relevant to Atlantic HMS fisheries management.

Additional information on the meeting and a copy of the draft agenda will be posted prior to the meeting at: *http://www.nmfs.noaa.gov/sfa/hms/advisory_panels/hms_ap/meetings/ap_meetings.html.*

Special Accommodations

This meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to LeAnn Hogan at (301) 427–8503 at least 7 days prior to the meeting.

Dated: July 30, 2015.

Emily H. Menashes,

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

[FR Doc. 2015–19148 Filed 8–4–15; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE056

Takes of Marine Mammals Incidental to Specified Activities; Taking Marine Mammals Incidental to a Wharf Recapitalization Project

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

ACTION: Notice; proposed incidental harassment authorization; request for comments.

SUMMARY: NMFS has received a request from the U.S. Navy (Navy) for authorization to take marine mammals incidental to construction activities as part of a wharf recapitalization project. Pursuant to the Marine Mammal Protection Act (MMPA), NMFS is requesting public comment on its proposal to issue an incidental harassment authorization (IHA) to the Navy to take, by Level B harassment only, during the specified activity.

DATES: Comments and information must be received no later than September 4, 2015.

ADDRESSES: Comments on this proposal 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.Laws@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 to the Internet at *www.nmfs.noaa.gov/pr/permits/incidental/construction.htm* 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: Ben Laws, Office of Protected Resources, NMFS, (301) 427–8401.

SUPPLEMENTARY INFORMATION:

Availability

An electronic copy of the Navy's application and supporting documents, as well as a list of the references cited in this document, may be obtained by visiting the Internet at: *www.nmfs.noaa.gov/pr/permits/incidental/construction.htm.* In case of problems accessing these documents, please call the contact listed above.

National Environmental Policy Act

The Navy prepared an Environmental Assessment (EA; 2013) for this project. We subsequently adopted the EA and signed our own Finding of No Significant Impact (FONSI) prior to