Dated: July 27, 2016.

Ronald K. Lorentzen,

Acting Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Preliminary Decision Memorandum

1. Summary.
2. Background.
3. Partial Rescission.
4. Scope of the Order.
5. Comparisons to Normal Value.
6. Product Comparisons.
7. Date of Sale.
8. Export Price.
9. Normal Value.
10. Currency Conversion.
11. Companies Not Selected for Individual Review.
12. Recommendation.

[FR Doc. 2016–18333 Filed 8–1–16; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 160606494–6494–01]

Request for Comments on Post-Quantum Cryptography Requirements and Evaluation Criteria

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

ACTION: Notice; request for comments

SUMMARY: The National Institute of Standards and Technology (NIST) is requesting comments on a proposed process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Current algorithms are vulnerable to attacks from large-scale quantum computers. The purpose of this notice is to solicit comments on the draft minimum acceptability requirements, submission requirements, evaluation criteria, and evaluation process of candidate algorithms from the public, the cryptographic community, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations so that their needs can be considered in the process of developing new public-key cryptography standards. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center Web site: *http://www.nist.gov/pqcrypto.*

DATES: Comments must be received on or before September 16, 2016.

ADDRESSES: Comments may be sent electronically to *pqc-comments@nist.gov* with ''Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria'' in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: Post-Quantum Cryptography Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930.

Comments received in response to this notice will be published electronically at *http://www.nist.gov/pqcrypto,* so commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: Dr. Lily Chen, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *Lily.Chen@nist.gov,* by telephone (301) 975–6974.

Technical inquiries regarding the proposed draft acceptability requirements, submission requirements, or the evaluation criteria should be sent electronically to *pqc-comments@nist.gov.*

A public email list-serve has been set up for announcements, as well as a forum to discuss the standardization effort being initiated by NIST. For directions on how to subscribe, please visit *http://www.nist.gov/pqcrypto.*

SUPPLEMENTARY INFORMATION: In recent years, there has been a substantial amount of research on quantum computers—machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms. In particular, quantum computers would completely break many public-key cryptosystems, including those standardized in FIPS 186–4, Digital Signature Standard (*http://dx.doi.org/10.6028/NIST.FIPS.186-4*), SP 800–56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (*http://dx.doi.org/10.6028/NIST.SP.800-56Ar2*), and SP 800–56B Revision 1, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography (*http://dx.doi.org/10.6028/NIST.SP.800-56Br1*).

Due to this concern, many researchers have begun to investigate post-quantum cryptography (PQC) (also called quantum-resistant cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers. A significant effort will be required in order to develop, standardize, and deploy new post-quantum algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs.

NIST has taken a number of steps in response to this potential threat. On April 2–3, 2015, NIST held a public workshop on Cybersecurity in a Post-Quantum World to solicit input on public-key cryptographic policy in the time of quantum computers. NIST also published NISTIR 8105, Report on Post-Quantum Cryptography (*http://dx.doi.org/10.6028/NIST.IR.8105*), in April 2016 which shares NIST's understanding of the status of quantum computing and post-quantum cryptography.

As a result of study and public feedback, NIST has decided to develop additional public-key cryptographic algorithms through a public standardization process, similar to the development processes for the hash function SHA–3 and the Advanced Encryption Standard (AES). To begin the process, NIST has drafted a set of minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The draft document containing these requirements and criteria is available at the Web site: *http://www.nist.gov/pqcrypto.* NIST seeks comments on these draft minimum acceptability requirements, submission requirements, evaluation criteria, and the evaluation process, as well as suggestions for other criteria and for the relative importance of each individual criterion in the evaluation process. Since neither the submission requirements nor the evaluation criteria have been finalized, and may evolve over time as a result of the public comments that NIST receives, candidate algorithms should NOT be submitted at this time.

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 (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.

Dated: July 27, 2016.

Kent Rochford,

Associate Director for Laboratory Programs.

[FR Doc. 2016–18150 Filed 8–1–16; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE769

Mid-Atlantic Fishery Management Council (MAFMC); Public Meeting

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

ACTION: Notice of public meeting.

SUMMARY: The Mid-Atlantic Fishery Management Council (Council) will hold a Webinar-based meeting of its River *Herring* and *Shad* (RH/S) Committee.

DATES: The meeting will be held Monday, August 15, 2016, from 1 p.m. to 4:30 p.m.

ADDRESSES: The meeting will be held via Webinar (*http://mafmc.adobeconnect.com/rh-s-com-aug15-2016/*) with a telephone audio connection (provided when connecting).

Council address: Mid-Atlantic Fishery Management Council, 800 N. State St., Suite 201, Dover, DE 19901; telephone: (302) 674–2331.

FOR FURTHER INFORMATION CONTACT: Christopher M. Moore, Ph.D. Executive Director, Mid-Atlantic Fishery Management Council; telephone: (302) 526–5255. The Council's Web site, *www.mafmc.org,* also has details on the proposed agenda, Webinar access, and briefing materials.

SUPPLEMENTARY INFORMATION:

Agenda

In October 2016, the Council will consider whether to develop an Amendment that could add several species of river *Herrings* and *Shads* as Council-managed species. This RH/S Committee meeting will review a white paper and draft decision document related to the need for Council management of blueback *Herring, Lewife,* American *Shad,* and hickory *Shad.* Public comments will also be taken.

Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aid should be directed to M. Jan Saunders, (302) 526–5251, at least 5 days prior to the meeting date.

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

Dated: July 28, 2016.

Tracey L. Thompson,

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

[FR Doc. 2016–18217 Filed 8–1–16; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE761

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 2016. 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 both Wednesday and Thursday, September 7 and September 8, 2016.

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

On Wednesday, September 7, 2016, the conference call information is phone number 1–888–469–2188; Participant Code: 7954019; and the webinar event address is: *https://noaaevents2.webex.com/noaaevents2/onstage/g.php?MTID=eec1bb32466dd8905125c5db01b539623*; event password: NOAA.

On Thursday, September 8, 2016, the conference call information is phone number 1–888–469–2188; Participant Code: 7954019; and the webinar event address is: *https://noaaevents2.webex.com/noaaevents2/onstage/g.php?MTID=e9fcef19f3c43ce6255dfad07807a71f4*; event password: NOAA.

Participants are strongly encouraged to log/dial in 15 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: Peter Cooper 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, 9 and 10 to the 2006 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, March and September 2015, March 2016), 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 the results of the 2016 dusky shark stock assessment and the Amendment 5b timeline; Draft Amendment 10 on Essential Fish Habitat, including potential Habitat Areas of Particular Concern; implementation updates for Final Amendment 7 on bluefin tuna management; and progress updates on various other rulemakings, including archival tag requirements, blacknose and small coastal shark management; domestic implementation of recommendations from the 2015 meeting of the International Commission for the Conservation of Atlantic Tunas; and potential changes to limited access vessel upgrading requirements and Individual Bluefin Quota program inseason transfer criteria. We also anticipate discussing recreational topics regarding data collection and economic surveys, as well as progress updates regarding the exempted fishing permit request to conduct research in pelagic longline closed areas. Finally, we also intend to