Comments may also be submitted by facsimile to (301) 713–0376, or by email to *NMFS.Pr1Comments@noaa.gov.* Please include the File No. in the subject line of the email comment.

Those individuals requesting a public hearing should submit a written request to the Chief, Permits and Conservation Division at the address listed above. The request should set forth the specific reasons why a hearing on the application would be appropriate.

FOR FURTHER INFORMATION CONTACT: Carrie Hubard or Shasta McClenahan, (301) 427–8401.

SUPPLEMENTARY INFORMATION: The subject permits are requested under the authority of the Marine Mammal Protection Act of 1972, as amended (MMPA; 16 U.S.C. 1361 *et seq.*), the regulations governing the taking and importing of marine mammals (50 CFR part 216), the Endangered Species Act of 1973, as amended (ESA; 16 U.S.C. 1531 *et seq.*), and the regulations governing the taking, importing, and exporting of endangered and threatened species (50 CFR 222–226).

Dr. Sharpe (File No. 19703) proposes to study humpback and killer (*Orcinus orca*) whales in Alaska using both vessel and aerial surveys and a variety of methods including photo-identification, passive and active acoustics, underwater video/photography, unmanned aircraft systems, prey mapping, and suction-cup tagging. The purpose of the research is to continue a long-term study of the behavior of Alaskan humpback whales, focusing on social structure, vocalizations, and feeding. Forty harbor porpoises (*Phocoena phocoena*), 50 Dall's porpoises (*Phocoenoides dalli*), 130 harbor seals (*Phoca vitulina*), and 80 Steller sea lions (*Eumetopias jubatus*) may be incidentally harassed during research activities. The permit would be valid for five years.

Mr. Cilfone (File No. 20993) proposes to film humpback whales in Hawaiian waters of the Maui Nui Basin. Footage would be used to create a film about humpback whales and their conservation success that would be available on multiple platforms. Boats, unmanned aircraft systems, pole cameras, and snorkelers would all be used to get footage. Fifty humpback whales would be approached annually. In addition, pantropical spotted (*Stenella attenuata*), spinner (*S. longirostris*), and bottlenose (*Tursiops truncatus*) dolphins may be incidentally harassed during filming operations. Filming would occur in winter and spring and the permit would be valid until May 2017.

In compliance with the National Environmental Policy Act of 1969 (42 U.S.C. 4321 *et seq.*), an initial determination has been made that the activities proposed are categorically excluded from the requirement to prepare an environmental assessment or environmental impact statement.

Concurrent with the publication of this notice in the **Federal Register**, NMFS is forwarding copies of the applications to the Marine Mammal Commission and its Committee of Scientific Advisors.

Dated: January 10, 2017.

Julia Harrison,

Chief, Permits and Conservation Division, Office of Protected Resources, National Marine Fisheries Service.

[FR Doc. 2017–00807 Filed 1–13–17; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XF161

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

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

ACTION: Notice; public meeting.

SUMMARY: The Tilefish Advisory Panel of the Mid-Atlantic Fishery Management Council (Council) will hold a meeting.

DATES: The meeting will be held on Thursday, February 9, 2017, beginning at 9 a.m. and conclude by 12 noon. For agenda details, see **SUPPLEMENTARY INFORMATION**.

ADDRESSES: The meeting will be held via webinar with a telephone-only connection option: *http://mafmc.adobeconnect.com/tile-ap-2017/.*

Council address: Mid-Atlantic Fishery Management Council, 800 N. State Street, Suite 201, Dover, DE 19901; telephone: (302) 674–2331 or on their Web site at *www.mafmc.org.*

FOR FURTHER INFORMATION CONTACT: Christopher M. Moore, Ph.D., Executive Director, Mid-Atlantic Fishery Management Council, telephone: (302) 526–5255.

SUPPLEMENTARY INFORMATION: The purpose of the meeting is to create a fishery performance report by the Council's Tilefish Advisory Panel. The intent of this report is to facilitate a venue for structured input from the Advisory Panel members for the Golden and Blueline Tilefish specifications process, including recommendations by the Council and its Scientific and Statistical Committee (SSC).

Special Accommodations

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

Dated: January 11, 2017.

Jeffrey N. Lonergan,

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

[FR Doc. 2017–00818 Filed 1–13–17; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Multistakeholder Process on Internet of Things Security Upgradability and Patching

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of open meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene a virtual meeting of a multistakeholder process concerning Internet of Things Security Upgradability and Patching on January 31, 2017.

DATES: The meeting will be held on January 31, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time.

ADDRESSES: This is a virtual meeting. NTIA will post links to online content and dial-in information on the multistakeholder process Web site at *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230; telephone: (202) 482–4281; email: *afriedman@ntia.doc.gov.* Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482–7002; email: *press@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION:

Background: In March of 2015 the National Telecommunications and Information Administration issued a Request for Comment to ''identify substantive cybersecurity issues that

affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers.'' [1] We received comments from a range of stakeholders, including trade associations, large companies, cybersecurity startups, civil society organizations and independent computer security experts.[2] The comments recommended a diverse set of issues that might be addressed through the multistakeholder process, including cybersecurity policy and practice in the emerging area of Internet of Things (IoT). On August 2, 2016, NTIA announced that it would convene a new multistakeholder process on security upgradability and patching for consumer IoT.[3] NTIA subsequently announced that the first meeting of this process would be held on October 19, 2016.[4]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[5] Unaddressed technical flaws in systems leave the users of software and systems at risk. The nature of these risks varies, and mitigating these risks requires various efforts from the developers and owners of these systems. One of the more common means of mitigation is for the developer or other maintaining party to issue a security patch to address the vulnerability. Patching has become more commonly accepted, even for consumers, as more operating systems and applications shift to visible reminders and automated updates. Yet as one security expert notes, this evolution of the software industry has yet to become the dominant model in IoT.[6]

To help realize the full innovative potential of IoT, users need reasonable assurance that connected devices, embedded systems, and their applications will be secure. A key part of that security is the mitigation of potential security vulnerabilities in IoT devices or applications through patching and security upgrades.

The ultimate objective of the multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT requires common definitions so that manufacturers and solution providers have shared visions for security, and consumers know what they are purchasing. Currently, no such common, widely accepted definitions exist, so many manufacturers struggle to effectively communicate to consumers the security features of their devices. This is detrimental to the digital ecosystem as a whole, as it does not reward companies that invest in patching, and it prevents consumers from making informed purchasing choices.

At the October 19, 2016, meeting, stakeholders discussed the challenge of patching, and how to scope the discussion. Participants identified five distinct work streams that could help foster better security across the ecosystem, and established working groups to more fully evaluate options in each of these areas.[7] The main objective of the January 31, 2016, meeting is to share progress from the working groups examining the five work streams, and hear feedback from the broader stakeholder community. Stakeholders will also discuss overall progress on the initiative, and identify any additional work that may be needed.

More information about stakeholders' work will be available at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

Time and Date: NTIA will convene a virtual meeting of the multistakeholder process on IoT Security Upgradability and Patching on January 31, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time. Please refer to NTIA's Web site, *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security,* for the most current information.

Place: This is a virtual meeting. NTIA will post links to online content and dial-in information on the multistakeholder process Web site at *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

Other Information: The meeting is open to the public and the press. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meetings through a moderated conference bridge, including polling functionality. Access details for the meetings are subject to change. Requests for a transcript of the meeting or other auxiliary aids should be directed to Allan Friedman at (202) 482–4281 or *afriedman@ntia.doc.gov* at least seven (7) business days prior to each meeting. Please refer to NTIA's Web site, *http://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security,* for the most current information.

Dated: January 11, 2017.

Kathy D. Smith,

Chief, National Telecommunications and Information Administration.

[FR Doc. 2017–00817 Filed 1–13–17; 8:45 am]

BILLING CODE 3510–60–P

[1] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 FR 14360, Docket No. 150312253–5253–01 (Mar. 19, 2015), *available at: https://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.*

[2] NTIA has posted the public comments received at *https://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem.*

[3] NTIA, Increasing the Potential of IoT through Security and Transparency (Aug. 2, 2016), *available at: https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.*

[4] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (Sept. 15, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/10192016-meeting-notice-msp-iot-security-upgradability-patching.*

[5] *See, e.g.,* Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies, Special Publication 800–40 Revision 3,* National Institute of Standards and Technology, NIST SP 800–40 (2013) *available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.*

[6] Bruce Schneier, *The Internet of Things Is Wildly Insecure—And Often Unpatchable,* Wired (Jan. 6, 2014) *available at: https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.*

[7] *See* NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

DEPARTMENT OF DEFENSE

Office of the Secretary

Charter Amendment of Department of Defense Federal Advisory Committees

AGENCY: Department of Defense.

ACTION: Amendment of Federal Advisory Committee.

SUMMARY: The Department of Defense (DoD) is publishing this notice to announce that it is amending the charter for the Advisory Committee on Arlington National Cemetery.

FOR FURTHER INFORMATION CONTACT: Jim Freeman, Advisory Committee Management Officer for the Department of Defense, 703–692–5952.

SUPPLEMENTARY INFORMATION: This committee's charter is being amended in accordance with the Federal Advisory Committee Act (FACA) of 1972 (5 U.S.C., Appendix, as amended) and 41 CFR 102–3.50(d). The amended charter and contact information for the Committee's Designated Federal Officer (DFO) can be obtained at *http://www.facadatabase.gov/.*

The DoD is amending the charter for the Advisory Committee on Arlington