Dated: August 25, 2015.

Julia Harrison,

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

[FR Doc. 2015–21392 Filed 8–28–15; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XE009

Marine Mammals; File Nos. 18722, 18897, 19425, and 19497

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

ACTION: Notice; issuance of permits.

SUMMARY: Notice is hereby given that permits have been issued to the following entities to receive, import, and export specimens of marine mammals for scientific research:

Permit No. 18722: Cornell University, 157 Biotechnology Building, Ithaca, NY 14850 [Responsible Party: Sharron Mitchell, Ph.D.];

Permit No. 18897: Kathleen Colegrove, Ph.D., University of Illinois, College of Veterinary Medicine, Zoological Pathology Program, LUMC Room 0745, Building 101, 2160 South First Street, Maywood, IL 60153;

Permit No. 19425: Melissa McKinney, Ph.D., University of Connecticut, Center for Environmental Sciences and Engineering, 3107 Horsebarn Hill Road, U–4210, Storrs, CT 06269; and

Permit No. 19497: University of Florida, College of Veterinary Medicine, Department of Infectious Diseases and Pathology V3–100, VAB, PO BOX 110880, Gainesville, FL, 32611–0880 [Responsible Party: Thomas B. Waltzek, D.V.M., Ph.D.].

ADDRESSES: The permits and related documents are available for review upon written request or by appointment in the Permits and Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13705, Silver Spring, MD 20910; phone (301) 427–8401; fax (301) 713–0376.

FOR FURTHER INFORMATION CONTACT: The following Analysts at (301) 427–8401: Rosa L. González (Permit No. 19497), Carrie Hubard (Permit No. 19425), Brendan Hurley (Permit Nos. 18722 and 18897) and Jennifer Skidmore (Permit Nos. 18722, 18897, 19425, and 19497).

SUPPLEMENTARY INFORMATION: On June 26, 2015, notice was published in the **Federal Register** (80 FR 36768) that four requests for permits to receive, import, and export specimens of marine mammals for scientific research had been submitted by the above-named applicants. The requested permits have been issued under the authority of the Marine Mammal Protection Act of 1972, as amended (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.*), the regulations governing the taking, importing, and exporting of endangered and threatened species (50 CFR parts 222–226), and the Fur Seal Act of 1966, as amended (16 U.S.C. 1151 *et seq.*).

Permit No. 18722 authorizes Cornell University to receive, import, or export unlimited samples from up to 2000 pinnipeds (excluding walrus) and 2000 cetaceans world-wide. These samples will be used for genotyping on marine mammals including trait mapping, population/ecological studies, and germplasm characterization. No live animals would be harassed or taken, lethally or otherwise, under the authorized permit. The permit is valid through August 10, 2020.

Permit No. 18897 authorizes Dr. Colegrove to import unlimited biological samples from up to 100 individual cetaceans and up to 100 individual pinnipeds (except walrus) world-wide. All samples (bones and organ tissue samples) are being imported for diagnostic testing to determine the causes of outbreaks or unusual natural mortalities, the ecology of diseases in free-ranging animals, or unexpected mortalities in captive populations. Samples will be from animals found deceased or euthanized in nature, collected opportunistically during the animals' capture by other researchers possessing permits for such activities, or legally held in captivity (including those held for rehabilitation) outside the U.S. No live animals would be harassed or taken, lethally or otherwise, under the authorized permit. The permit is valid through August 10, 2020.

Permit No. 19425 authorizes Dr. McKinney to study marine mammal contaminant levels, specifically using fatty acid and stable isotopes to examine diets and contaminant loads and how they are affected by climate change. Tissue samples from cetaceans and pinnipeds may come from remote biopsy sampling, captured animals, and animals collected during subsistence harvests and may originate in the United States, Canada, and Greenland/Denmark. Samples (up to 50 of each species group per year, except for those species specified below) will be analyzed, with a focus on the following Arctic species: Ringed seal (30 per year), bearded seal (10 per year), and narwhal (10 per year). No live animals would be harassed or taken, lethally or otherwise, under the authorized permit. The permit is valid through August 1, 2020.

File No. 19497 authorizes the University of Florida to receive, import, and export marine mammal tissue and other specimen materials (*e.g.,* body fluids) to research the etiologies and cofactors of emerging marine mammal infectious diseases, utilizing standard molecular and sequencing approaches. Unlimited samples from up to 300 individual cetaceans and 700 individual pinnipeds (excluding walrus) are authorized to be received, imported, or exported annually on an opportunistic basis. They will be collected by others under separate existing permits and may be obtained from the following sources: (1) Animals killed during legal U.S. or foreign subsistence harvests; (2) animals stranded alive or dead in foreign countries; (3) animals that died incidental to commercial fishing operations in the U.S. where such taking is legal (*i.e.,* bycatch); (4) animals that died incidental to commercial fishing operations in foreign countries where such taking is legal; (5) animals in captivity where samples were taken as a result of routine husbandry procedures or under separate permit; and (6) samples from other authorized researchers or collections in academic, federal, state or other institutions involved in marine mammal research in the U.S. or abroad. Samples collected from stranded animals in the U.S. and received under separate authorization may be exported and re-imported. No takes of live animals are requested or would be permitted. The permit is valid through July 31, 2020.

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

As required by the ESA, issuance of these permits was based on a finding that such permits: (1) Were applied for in good faith; (2) will not operate to the disadvantage of such endangered species; and (3) are consistent with the purposes and policies set forth in section 2 of the ESA.

Dated: August 25, 2015.

Julia Harrison,

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

[FR Doc. 2015–21390 Filed 8–28–15; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Multistakeholder Process To Promote Collaboration on Vulnerability Research Disclosure

AGENCY: National Telecommunications and Information Administration, Commerce.

ACTION: Notice of open meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene meetings of a multistakeholder process concerning the collaboration between security researchers and software and system developers and owners to address security vulnerability disclosure. This Notice announces the first meeting, which is scheduled for September 29, 2015.

DATES: The meeting will be held on September 29, 2015, from 9:00 a.m. to 3:00 p.m., Pacific Time. See **SUPPLEMENTARY INFORMATION** for details.

ADDRESSES: The meeting will be held in the Booth Auditorium at the University of California, Berkeley, School of Law, Boalt Hall, Bancroft Way and Piedmont Avenue, Berkeley, CA 94720–7200.

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: On March 19, 2015, the National Telecommunications and Information Administration, working with the Department of Commerce's Internet Policy Task Force (IPTF), 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] This Request built on earlier work from the Department, including the 2011 Green Paper *Cybersecurity, Innovation, and the Internet Economy,*[2] as well as comments the Department had received on related issues.[3]

The IPTF asked for suggestions of security challenges that an NTIA-convened multistakeholder group could address, and offered a dozen potential topics for explicit feedback.[4] We received 35 comments from a range of stakeholders, including trade associations, large companies, cybersecurity startups, civil society organizations and independent computer security experts.[5] The comments highlight a range of issues that might be addressed through the multistakeholder process and suggest various ways in which the group's work could be structured.

Of the topics suggested, the challenge of collaboration between security researchers and system and software vendors stands out as a critical issue where reaching some consensus on shared goals, principles, and practices is both feasible and necessary. On July 9, 2015, after reviewing the comments, NTIA announced that the first issue to be addressed would be ''collaboration on vulnerability research disclosure.'' [6] While this is not the first discussion on the topic, stakeholders have presented the case that the time is right to make further progress among ecosystem players by achieving consensus and a commitment to baseline principles and accepted practices.

This issue is commonly referred to as the question of ''vulnerability disclosure.'' For as long as humans have created software there have been software ''bugs.'' [7] Many of these bugs can introduce vulnerabilities, leaving the users of the systems and software at risk. The nature of these risks vary, and mitigating these risks requires various efforts from the developers and owners of these systems. Security researchers of all varieties, including academics, professionals, and those who simply enjoy thinking about security may identify these bugs for a number of reasons, and in a wide range of contexts. How researchers should handle these vulnerabilities, and how vendors should work with researchers has been the matter of active debate for many years, since before the turn of the millennium.[8] Several points have been actively debated. Researchers have expressed concerns that vendors do not respond in a timely fashion, leaving users at risk. Vendors worry about the time, expense, and added complexity of addressing every vulnerability, as well as the risks introduced by potentially disclosing vulnerabilities before they can be patched or mitigated. Given that all good faith actors care about security, there is room to find common ground.

The goal of this process is neither to replicate past discussions nor duplicate existing initiatives. As information security is gaining more attention in the collective consciousness due to a series of high profile cybersecurity incidents and disclosed vulnerabilities, more firms and organizations are considering how to engage with third party researchers, just as they are exploring other security tools and processes. The security community itself has worked to promote better collaboration. More software vendors and system owners are offering ''bug bounty'' programs that reward researchers for sharing vulnerability information. In addition to enterprises that buy vulnerabilities and sell them to vendors, new business models have emerged to help organizations develop and manage bug bounty programs. Leading experts at the International Standards Organization have developed, and are continuing to revise, a formal standard for vendors on how to manage incoming vulnerability

[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: http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.*

[2] U.S. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (June 2011) (Green Paper), *available at: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.*

[3] *See* Comments Received in Response to **Federal Register** Notice Developing a Framework for Improving Critical Infrastructure Cybersecurity, Docket No. 140721609–4609–01, *available at: http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html.*

[4] Request for Public Comment, *supra* note 1.

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

[6] NTIA, *Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure* (July 9, 2015), *available at: http://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure.*

[7] *See, e.g.,* Peter Wayner, *Smithsonian Honors the Original Bug in the System,* N.Y. Times (Dec. 7, 1997), *available at: http://www.nytimes.com/library/cyber/week/120497bug.html.*

[8] For a bibliography of research, proposed standards, online discussions and other resources, *see* University of Oulu Secure Programming Group, Juhani Eronen & Ari Takanen eds., *Vulnerability Disclosure Publications and Discussion Tracking, available at: https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking* (last visited Aug. 20, 2015).