

Algorithm ("Triple DES"), which is specified in FIPS 46-3.

NIST invites public comments on the Draft FIPS for the AES. After the comment period closes, NIST will analyze the comments, make changes to the document, as appropriate, and then propose the draft standard to the Secretary of Commerce for approval as a FIPS.

DATES: Comments on the Draft FIPS for the AES must be received on or before May 29, 2001.

Specifications: Specifications for the Draft FIPS for the AES are available through the AES home page: <http://www.nist.gov/aes/>.

ADDRESSES: Official comments on the Draft FIPS for the AES may either be sent electronically to AEScomments@nist.gov or by regular mail to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Draft FIPS for the AES, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

FOR FURTHER INFORMATION CONTACT: Mr. James Foti (301) 975-5237, jfoti@nist.gov, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930.

SUPPLEMENTARY INFORMATION: In January 1997, NIST initiated an effort to develop the Advanced Encryption Standard (AES), which would provide cryptographic security well into the twenty-first century. In August 1999, NIST announced five publicly submitted candidate algorithms as finalists for the AES, and invited public review, comment, and analysis in order to make a selection for the Draft FIPS for the AES. During the Round 2 technical evaluation period, these five finalists were subjected to extensive analysis and testing by the cryptographic community. After much careful study and consideration of the finalists and Round 2 public comments, NIST made its selection for the Draft FIPS for the AES, and issued a report explaining that selection. The report is available at <http://www.nist.gov/aes/>.

NIST strongly encourages the public to continue performing analyses of the security of the AES, and to submit those analyses as official comments in response to this request. Such analyses and other comments received will be considered by NIST in preparing the final version of the FIPS for the AES.

NIST seeks detailed comments regarding any intellectual property that may be infringed by the practice of the algorithm(s) in the Draft FIPS for the

AES. This includes comments from all parties regarding specific claims that the practice of a finalist's algorithm infringes on their patent(s). Claims regarding infringement of copyrighted software are also particularly solicited. NIST views this input as a critical factor in the eventual widespread adoption and implementation of the Draft FIPS for the AES.

NIST reminds all interested parties that the AES development effort is being conducted as an open standards-setting activity. Specifically, NIST has requested that all interested parties identify to NIST any patents or inventions that may be required for the use of AES. Public comments received in response to this request will be posted periodically during the comment period at <http://csrc.nist.gov/cryptval/aes/draftfips/>.

To encourage on-going discussions related to the AES, NIST will continue to maintain its AES electronic discussion forum at <http://aes.nist.gov/aes/>. Please note that comments posted at that site will NOT be considered "official" comments.

No additional conferences are planned for the Draft FIPS for the AES at this time.

NIST intends to develop a Draft FIPS for AES Modes of Operation. Given the need for further public discussion and study of suggested modes of operation, NIST will hold a public workshop to discuss the Draft FIPS. Details on this effort are located at <http://www.nist.gov/modes/>.

Authority: Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, Public Law 100-235.

E.O. 12866: This notice has been determined to be significant for purposes of E.O. 12866.

Dated: February 20, 2001.

Karen Brown,

Acting Director, NIST.

[FR Doc. 01-4886 Filed 2-27-01; 8:45 am]

BILLING CODE 3510-CN-M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 121200J]

Marine Mammals; File No. 87-1593-00

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and

Atmospheric Administration (NOAA), Commerce.

ACTION: Issuance of permit.

SUMMARY: Notice is hereby given that Dr. Daniel Costa (Principal Investigator), Institute of Marine Sciences, Earth & Marine Sciences Bldg. A316, University of California, Santa Cruz, CA, 95064, has been issued a permit to take California sea lions (*Zalophus californianus*) and Antarctic pinnipeds for purposes of scientific research.

DATES: Written or telefaxed comments must be received on or before March 30, 2001.

ADDRESSES: The permit and related documents are available for review upon written request or by appointment in the following office(s):

Permits and Documentation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13130, Silver Spring, MD 20910 (301/713-2289); and

Southwest Region, NMFS, 501 West Ocean Blvd., Suite 4200, Long Beach, CA 90802-4213; phone (562)980-4001; fax (562)980-4018.

FOR FURTHER INFORMATION CONTACT: Ruth Johnson, 301/713-2289.

SUPPLEMENTARY INFORMATION: On August 15, 2000, and on November 15, 2000, notices were published in the **Federal Register** (65 FR 49786 and 68983) that a request for a scientific research permit to take California sea lions and Antarctic pinnipeds had been submitted by the above-named individual.

Project I - The Holder is studying the foraging ecology and energetics of California sea lions of all age and sex classes in southern and central California, including San Nicolas, Ano Nuevo and San Miguel Islands. The Permit authorizes, annually, for 5 years, 40 adult sea lions and 100 pup sea lions will be captured, tagged, bleach marked, instrumented with satellite linked TDRs, blood sampled, and measured. In addition the Holder is authorized to incidentally harass up to 6,650 animals annually and is allowed up to five accidental mortalities over the five-year period.

Project II - The Holder is studying Crabeater seals (*Lobodon carcinophagus*). The Permit authorizes annually, for up to 5 years, 25 *L. carcinophagus* and 10 each for leopard seal (*Hydrurga leptonyx*), Weddell seal (*Leptonychotes weddellii*), and Ross seal (*Ommatophoca rossii*). Animals will be captured, immobilized, weighed/measured, sampled [blood and biopsy, whisker], administered tritiated saline water, flipper tagged, marked, lavaged for stomach contents, and instrumented

with VHF/satellite transmitters. The project will determine the distribution and foraging behavior of adult Crabeater seals and simultaneously assess the impact that oceanographic features and prey aggregations have on foraging strategies employed. Equivalent data will be obtained for other species. Research will occur in Marguerite Bay, West Antarctic Peninsula. Opportunistic samples will be collected from dead beach cast seals for deposit in the natural history collection at the University.

The requested permit has been issued under the authority of the Marine Mammal Protection Act of 1972, as amended (16 U.S.C. 1361 *et seq.*), and the Regulations Governing the Taking and Importing of Marine Mammals (50 CFR part 216).

Dated: February 21, 2001.

Ann D. Terbush,

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

[FR Doc. 01-4892 Filed 2-27-01; 8:45 am]

BILLING CODE 3510-22-S

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 022000C]

National Plan of Action for the Reduction of Incidental Catch of Seabirds in Longline Fisheries

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

ACTION: Notice of availability; response to public comments.

SUMMARY: NMFS announces the availability of the National Plan of Action for the Reduction of Incidental Catch of Seabirds in Longline Fisheries (NPOA-S). NMFS also responds to public comments received on the draft NPOA-S.

DATES: The final version of the NPOA-S is now in effect and available on the NMFS web site (<http://www.nmfs.gov>). Hard copies of the document are available upon request (see **ADDRESSES**).

ADDRESSES: Requests for hard copies of the NPOA-S should be sent to Steve Leathery, NOAA-Fisheries/SF3, Room 14434, 1315 East-West Highway, Silver Spring, MD 20910.

FOR FURTHER INFORMATION CONTACT: Steve Leathery, 301-713-2341, or fax 301-713-1193.

SUPPLEMENTARY INFORMATION: The United States developed an NPOA-S through a collaborative effort between NMFS, the U.S. Department of State (DOS), and the U.S. Fish & Wildlife Service (FWS), pursuant to the International Plan of Action for the Reduction of Incidental Catch of Seabirds in Longline Fisheries (IPOA-S) that was adopted by the United Nations Food and Agriculture Organization Committee on Fisheries (COFI) in February 1999. The United States will report to COFI by February, 2001, on NPOA-S development and implementation.

An outline describing the proposed structure of the draft NPOA-S was published in the **Federal Register** on September 9, 1999 (64 FR 48987). The draft NPOA-S was released for public review and comment on December 29, 1999 (64 FR 73017), and the public comment period was subsequently extended through February 7, 2000.

Comments and Responses

NMFS received 10 written public comments and held one public meeting during the development of the NPOA-S. NMFS considered all comments received on the draft NPOA-S when drafting the final version of the NPOA-S.

Comment 1: The draft NPOA-S does not fulfill the responsibilities outlined in the IPOA-S and compromises U.S. leadership in international negotiations on reducing seabird bycatch in longline fisheries.

Response: The IPOA-S is a voluntary measure that calls on member states to assess their longline fisheries and, if a seabird bycatch problem is determined to exist, to develop an NPOA-S to reduce seabird bycatch within 2 years. NMFS has conducted a preliminary review of seabird bycatch in U.S. longline fisheries and has determined that a seabird bycatch problem exists in several U.S. longline fisheries, including Hawaii-based pelagic longline fisheries and Alaska halibut and groundfish demersal longline fisheries. Consistent with this NPOA-S, seabird bycatch regulations are in place for Alaska longline fisheries and under development for Hawaii longline fisheries, and research is underway in Alaska and Hawaii longline fisheries to determine the effectiveness of seabird bycatch measures and to improve those measures.

NMFS, FWS, and DOS developed this NPOA-S to provide policy guidance to reduce seabird bycatch in those longline fisheries where a problem is already known to exist and to assess all other U.S. longline fisheries within 2 years to

determine whether a seabird bycatch problem exists. If a seabird bycatch problem is found to exist, a fishery-specific plan should be developed within 1 year that would implement seabird bycatch mitigation measures in that fishery within 2 years.

Although incidental (i.e., unintended) catch of seabirds in longline fisheries is often termed "bycatch," the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act), which is the primary law covering management of marine fishery resources in U.S. waters, specifically excludes seabirds from the definition of "fish" and, therefore, bycatch. Unless certain requirements under the Endangered Species Act are involved, the Magnuson-Stevens Act does not require implementation of measures to reduce incidental catch of seabirds. However, the Magnuson-Stevens Act authorizes implementation of fishery management measures designed to protect the marine environment from the effects of fishing activities.

In order to strengthen NMFS' ability to effectively implement seabird conservation measures in U.S. fisheries, NMFS is supporting an amendment to the Magnuson-Stevens Act that would change the definition of bycatch to include seabirds and would require fishery management plans to specifically address seabird bycatch. For the purpose of the NPOA-S, the term "bycatch" is used for incidental seabird catch, and the term "seabird" refers to those bird species that habitually obtain their food from the sea below the low water mark.

NMFS believes that the final NPOA-S demonstrates strong U.S. leadership on this important international seabird conservation issue. The United States already has seabird bycatch mitigation regulations in place for all Alaska longline fisheries and under consideration for implementation in Hawaii longline fisheries. Additionally, the United States is likely to be one of the first COFI members to complete an NPOA-S, which calls on the United States to further advance the IPOA-S at future international fisheries management fora.

Comment 2: The draft NPOA-S does not contain any seabird bycatch reduction guidelines or performance standards.

Response: The final NPOA-S provides policy guidance to the Regional Fishery Management Councils (Councils) and the NMFS Regions to assess all U.S. longline fisheries within the next 2 years to determine if a seabird bycatch problem exists beyond what was determined in the preliminary