the integrity of information and verifying the sender of the information. This FIPS will benefit federal agencies by providing a robust cryptographic algorithm that can be used to protect sensitive electronic data for many years.

EFFECTIVE DATE: This standard is effective August 6, 2002.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

A copy of FIPS 198 is available electronically from the NIST website at: http://csrc.nist.gov/publications/drafts/dfips-HMAC.pdf.

SUPPLEMENTARY INFORMATION: A notice was published in the **Federal Register** (Volume 66, Number 4, pp.1088–9) on January 5, 2001, announcing the proposed FIPS for Keyed-Hash Message Authentication Code (HMAC) for public review and comment. The **Federal Register** notice solicited comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. In addition to being published in the **Federal Register**, the notice was posted on the NIST Web pages; information was provided about the submission of electronic comments. Comments and responses were received from four individuals and private sector organizations, and from one Canadian government organization. None of the comments opposed the adoption of the Keyed-Hash Message Authentication Code (HMAC) as a Federal Information Processing Standard. Some comments offered editorial suggestions that were reviewed. Changes were made to the standard where appropriate.

Following is an analysis of the technical and related comments received.

Comment: A comment expressed concern about the security of the recommended FIPS. It specifies a 32-bit MAC, as compared to a requirement of a voluntary industry standard of the retail banking community for an 80-bit MAC (using the Triple Data Encryption Algorithm). Also a clarification was requested concerning the requirement in the recommended FIPS for ''periodic key changes.''

Response: HMAC for the banking community is specified in a draft voluntary industry standard (ANSI X9.71), and mandates a 80-bit MAC. This recommended FIPS is based on that draft standard, but was written to allow the 32-bit MAC, which is used by the banking community and in other applications where there is little risk in the use of a relatively short MAC. NIST believes that the strengths of the 32-bit HMAC and the Triple DES MAC against collision type attacks mentioned in the comment are equivalent; collision type attacks use trial and error tactics to try to guess the MAC. NIST believes that the recommended FIPS provides adequate security, and that it will encourage a broad application of message authentication techniques.

NIST believes that changing keys periodically is a good practice. This issue is not addressed in ANSI X9.71. Key changes are recommended even when very strong algorithms with large keys are used, since keys can be compromised in ways that do not depend on the strength of the algorithm. The recommended FIPS does not specify how often keys should be changed. This will be addressed in a guidance document on key management that is currently under development. Information about this guidance document is posted on NIST's web pages *(http://www.nist.gov/kms).*

Comment: A comment suggested that a table of equivalent key sizes for different algorithms was needed, and that the values allowed for the key size and MAC length should be more restrictive.

Response: Advice about key sizes and the equivalent sizes between different cryptographic algorithms is more properly addressed in FIPS 180–1, Secure Hash Standard (currently under revision as FIPS 180–2) and the planned guidance document on key management. With regard to restrictions on the key size and MAC length, NIST believes that the marketplace will determine the predominating sizes.

Comment: A comment recommended that references to and examples of new hash algorithms (SHA–256, SHA–384 and SHA–512) be included.

Response: The new hash algorithms mentioned have not yet been approved for use. NIST believes that it is inappropriate to provide references to and examples of algorithms that are not yet approved standards. When the new hash algorithms have been approved, examples using these algorithms will be available on NIST's web pages. *http://www.nist.gov/cryptotoolkit.*

Comment: A comment recommended that OIDs (Object Identifiers) should be included for HMAC using the new hash algorithms mentioned above.

Response: The need for different object identifiers keeps changing. In addition, the new hash algorithms have not been approved as standards. Therefore, NIST believes that OIDs should not be included in this recommended standard. A reference to a NIST web site has been provided in the standard to help users obtain HMAC OIDs.

Comment: An observation was made regarding the different restrictions for the key size and MAC size (truncated output) for the recommended FIPS, for RFC 2104 and for ANSI X9.71. The comment mentioned incompatibilities when products are validated against these standards.

Authority: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems.

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

Dated: March 25, 2002.

Karen H. Brown,

Deputy Director.

[FR Doc. 02–7880 Filed 4–1–02; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 032602F]

Gulf of Mexico Fishery Management Council; Public Meeting

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

ACTION: Notice of public meeting.

SUMMARY: The Gulf of Mexico Fishery Management Council (Council) will convene public meetings to discuss the content of a Programmatic Environmental Impact Statement (PEIS) for the Council's Generic Amendment for Essential Fish Habitat (EFH) in the Gulf of Mexico and potential alternatives.

DATES: The meetings will be held on Tuesday April 16, 2002 in Silver Spring, MD, and Wednesday, April 17, 2002 in Kenner, LA, from 9 a.m. to 3 p.m.

ADDRESSES: The meeting on April 16, 2002 will be held at the Holiday Inn, 8777 Georgia Avenue (Route 97), Silver Spring, MD; telephone: 301-589-0800. The meeting on April 17, 2002 will be held at the New Orleans Airport Hilton, 901 Airline Drive, Kenner, LA; telephone: 504-469-5000.

Council address: Gulf of Mexico Fishery Management Council, 3018 U.S.

Highway 301 North, Suite 1000, Tampa, FL 33619.

FOR FURTHER INFORMATION CONTACT: Heidi Lovett, MRAG Americas (Contractor), 110 South Hoover Blvd, Suite 212, Tampa, FL 33609; telephone: 813-639-9519; email: heidilovett@compuserve.com.

SUPPLEMENTARY INFORMATION: The meetings will begin with a focus group workshop of interested participants that will be held from 9 a.m. to 12 noon, to discuss the PEIS for the Council's Generic Amendment for EFH in the Gulf of Mexico and to discuss structural components and potential alternatives. The goal is to get input from various stakeholders early in this process. A public comment session will be scheduled from 1 p.m. to 3 p.m. These meetings are being coordinated by the Council's Consultant (MRAG Americas) that is developing the PEIS. These will not be the only workshops scheduled; other opportunities for public and stakeholders involvement exist through the PEIS development process and will be noticed accordingly. Interested participants/attendees should contact Heidi Lovett.

A copy of the agenda and related materials can be obtained by calling the Council office at 813-228-2815.

Although non-emergency issues not contained in this agenda may come before this group for discussion, those issues may not be the subject of formal action during this meeting. Action will be restricted to those issues specifically identified in this notice and any issues arising after publication of this notice that require emergency action under section 305(c) of the Magnuson-Stevens Fishery Conservation and Management Act, provided the public has been notified of the Council's intent to take final action to address the emergency.

Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Anne Alford at the Council (see **ADDRESSES**) by April 9, 2002.

Dated: March 27, 2002.

Theophilus R. Brainerd,

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

[FR Doc. 02–7932 Filed 4–1–02; 8:45 am]

BILLING CODE 3510–22–S

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 032602E]

Pacific Fishery Management Council; Public Meeting

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

ACTION: Notice of public meeting.

SUMMARY: The Pacific Fishery Management Council's (Council) Highly Migratory Species Plan Development Team (HMSPDT) will hold a work session, which is open to the public.

DATES: The HMSPDT will meet on Wednesday, April 17, 2002; Thursday, April 18, 2002; and Friday, April 19, 2002. The HMSPDT will meet each day from 8 a.m. until 5 p.m., except for Friday, when the HMSPDT will meet from 8 a.m. until business for the day is completed.

ADDRESSES: The work session will be held in the large conference room at the NMFS Southwest Fisheries Science Center, 8604 La Jolla Shores Drive, Room D-203, La Jolla, CA 92037; telephone: (858) 546–7000.

Council address: Pacific Fishery Management Council, 7700 NE Ambassador Place, Suite 200, Portland, OR 97220–1384.

FOR FURTHER INFORMATION CONTACT: Dan Waldeck, Pacific Fishery Management Council; (503) 326–6352.

SUPPLEMENTARY INFORMATION: The primary purpose of the work session is to scope and review revisions to the draft fishery management plan for West Coast highly migratory species fisheries per Council guidance from the March 2002 Council meeting.

Although nonemergency issues not contained in the HMSPDT meeting agenda may come before the HMSPDT for discussion, those issues may not be the subject of formal HMSPDT action during this meeting. HMSPDT action will be restricted to those issues specifically listed in this document and any issues arising after publication of this document that require emergency action under section 305(c) of the Magnuson-Stevens Fishery Conservation and Management Act, provided the public has been notified of the HMSPDT's intent to take final action to address the emergency.

Special Accommodations

The meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Ms. Carolyn Porter at (503) 326–6352 at least 5 days prior to the meeting date.

Dated: March 27, 2002.

Theophilus R. Brainerd,

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

[FR Doc. 02–7933 Filed 4–1–02; 8:45 am]

BILLING CODE 3510–22–S

COMMITTEE FOR THE IMPLEMENTATION OF TEXTILE AGREEMENTS

Adjustment of Import Limits for Certain Cotton Textile Products Produced or Manufactured in Macau

March 26, 2002.

AGENCY: Committee for the Implementation of Textile Agreements (CITA).

ACTION: Issuing a directive to the Commissioner of Customs adjusting limits.

EFFECTIVE DATE: April 2, 2002.

FOR FURTHER INFORMATION CONTACT: Ross Arnold, International Trade Specialist, Office of Textiles and Apparel, U.S. Department of Commerce, (202) 482–4212. For information on the quota status of these limits, refer to the Quota Status Reports posted on the bulletin boards of each Customs port, call (202) 927–5850, or refer to the U.S. Customs website at http://www.customs.gov. For information on embargoes and quota re-openings, refer to the Office of Textiles and Apparel website at http://otexa.ita.doc.gov.

SUPPLEMENTARY INFORMATION:

Authority: Section 204 of the Agricultural Act of 1956, as amended (7 U.S.C. 1854); Executive Order 11651 of March 3, 1972, as amended.

The current limits for certain categories are being reduced for carryforward used.

A description of the textile and apparel categories in terms of HTS numbers is available in the CORRELATION: Textile and Apparel Categories with the Harmonized Tariff Schedule of the United States (see **Federal Register** notice 66 FR 65178, published on December 18, 2001). Also