''Exclusions'' section of the notice, we are excluding the following companies: Armand Duhamel et fils Inc., Bardeaux et Cedres, Beaubois Coaticook Inc., Busque & Laflamme Inc., Carrier & Begin Inc., Clermond Hamel, J.D. Irving, Ltd., Les Produits. Forestiers. D.G., Ltee, Marcel Lauzon Inc., Mobilier Rustique, Paul Vallee Inc., Rene Bernard, Inc., Roland Boulanger & Cite., Ltee, Scierie Alexandre Lemay, Scierie La Patrie, Inc., Scierie Tech, Inc., Wilfrid Paquet et fils, Ltee, B. Luken Logging Ltd., Frontier Lumber, and Sault Forest Products Ltd. Therefore, we are directing the U.S. Customs Service to exempt from the suspension of liquidation only entries of softwood lumber products from Canada which are accompanied by an original Certificate of Origin issued by the Maritime Lumber Bureau (MLB), and those of the excluded companies listed above. The MLB certificate will specifically state that the corresponding entries cover softwood lumber products produced in the Maritime Provinces from logs originating in Nova Scotia, New Brunswick, Prince Edward Island, Newfoundland and the state of Maine.

ITC Notification

In accordance with section 705(d) of the Act, we will notify the ITC of our determination. In addition, we are making available to the ITC all non-privileged and non-proprietary information related to this investigation. We will allow the ITC access to all privileged and business proprietary information in our files, provided that the ITC confirms that it will not disclose such information, either publicly or under an administrative protective order (APO), without the written consent of the Assistant Secretary for Import Administration.

If the ITC determines that material injury, or threat of material injury, does not exist, this proceeding will be terminated. If however, the ITC determines that such injury does exist, we will issue a countervailing duty order.

Return or Destruction of Proprietary Information

In the event that the ITC issues a final negative injury determination, this notice will serve as the only reminder to parties subject to APO of their responsibility concerning the destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3). Failure to comply is a violation of the APO.

This determination is published pursuant to sections 705(d) and 777(i) of the Act.

Dated: March 21, 2002.

Faryar Shirzad,

Assistant Secretary for Import Administration.

Appendix I—Issues and Decision Memorandum

[FR Doc. 02–7849 Filed 4–1–02; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 000929279–1219–02]

RIN 0693–ZA41

Announcing Approval of Federal Information Processing Standard (FIPS) 198, The Keyed-Hash Message Authentication Code (HMAC)

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce approves FIPS 198, The Keyed-Hash Message Authentication Code (HMAC), and makes it compulsory and binding on Federal agencies for the protection of sensitive, unclassified information. FIPS 198 is an essential component of a comprehensive group of cryptographic techniques that government agencies need to protect data, communications, and operations. The Key-Hashed Message Authentication Code specifies a cryptographic process for protecting

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.