publication of this notice of final results of review for all shipments of certain stainless steel wire rods from France entered, or withdrawn from warehouse, for consumption on or after the publication date, as provided for by section 751(a)(1) of the Act: (1) the cash deposit rates for the reviewed companies will be the rates for those firms as stated above; (2) if the exporter is not a firm covered in this review, or the original investigation, but the manufacturer is, the cash deposit rate will be the rate established for the most recent period for the manufacturer of the merchandise; and (3) the cash deposit rate for all other manufacturers or exporters will continue to be 24.51 percent for stainless steel wire rods, the all others rate established in the LTFV investigation. See *Amended Final Determination and Antidumping Duty Order: Certain Stainless Steel Wire Rods from France* (59 FR 4022, January 28, 1994).

These deposit requirements, when imposed, shall remain in effect until publication of the final results of the next administrative review.

This notice serves as a final reminder to importers of their responsibility under 19 CFR 353.26 to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in the Secretary's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

This notice also serves as the only reminder to parties subject to administrative protective order (APO) of their responsibility concerning the disposition of proprietary information disclosed under APO in accordance with section 353.34(d) of the Department's regulations. Timely notification of return/destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and the terms of an APO is a sanctionable violation.

This administrative review and notice are in accordance with section 751(a)(1) of the Act (19 U.S.C. 1675(a)(1)) and 19 CFR 353.22.

Dated: February 7, 1997.

Robert S. LaRussa,

Acting Assistant Secretary for Import Administration.

[FR Doc. 97–3913 Filed 2–14–97; 8:45 am]

BILLING CODE 3510–DS–P

National Institute of Standards and Technology

[Docket No. 950420110–6167–02]

RIN 0693–XX06

Approval of Federal Information Processing Standards Publication (FIPS) 196, Entity Authentication Using Public Key Cryptography

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

ACTION: The purpose of this notice is to announce that the Secretary of Commerce has approved a new standard, which will be published as FIPS Publication 196, Entity Authentication Using Public Key Cryptography.

SUMMARY: On June 6, 1995, notice was published in the Federal Register (60 FR 29830–29832) that a Federal Information Processing Standard for Public Key Cryptographic Entity Authentication mechanisms was being proposed for Federal use.

The written comments submitted by interested parties and other material available to the Department relevant to this standard were reviewed by NIST. On the basis of this review, NIST recommended that the Secretary approve the standard as a Federal Information Processing Standards Publication, and prepared a detailed justification document for the Secretary's review in support of that recommendation.

The detailed justification document which was presented to the Secretary, and which includes an analysis of the written comments received, is part of the public record and is available for inspection and copying in the Department's Central Reference and Records Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW, Washington, DC 20230.

This FIPS contains two sections: (1) an announcement section which provides information concerning the applicability, implementation, and maintenance of the standard; and (2) a specifications section, which deals with the technical requirements of the standard. Only the announcement section of the standard is provided in this notice.

EFFECTIVE DATE: This standard becomes effective April 6, 1997.

ADDRESSES: Interested parties may purchase copies of this standard, including the technical specifications section, from the National Technical Information Service (NTIS). Specific ordering information from NTIS for this standard is set out in the Where to Obtain Copies Section of the announcement section of the standard.

FOR FURTHER INFORMATION CONTACT: Mr. James Foti, telephone (301) 975–5237, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Dated: January 30, 1997.

Elaine Bunten-Mines,

Director, Program Office.

Federal Information Processing Standards Publication 196

February 18, 1997.

Announcing—Entity Authentication Using Public Key Cryptography

Federal Information Processing Standards (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100–235.

1. Name of Standard. Entity Authentication Using Public Key Cryptography (FIPS PUB 196).

2. Category of Standard. Computer Security, *Subcategory* Access Control.

3. Explanation. This standard specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These protocols may be used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

Authentication based on public key cryptography has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. A user (claimant) attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

6. Cross Index.

a. FIPS PUB 140–1, Security Requirements for Cryptographic Modules.

b. FIPS PUB 171, Key Management Using ANSI X9.17.

c. FIPS PUB 180–1, Secure Hash Standard.

d. FIPS PUB 186, Digital Signature Standard.

e. FIPS PUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives.

f. ANSI X9.17–1985, Financial Institution Key Management (Wholesale).

g. ISO/IEC 9798–1:1991, Information technology—Security techniques—Entity authentication mechanisms—Part 1: General model.

h. ISO/IEC 9798–3:1993, Information technology—Security techniques—Entity authentication mechanisms—Part 3: Entity authentication using a public key algorithm.

Other NIST publications maybe applicable to the implementation and use of this standard. A list (NIST Publications List 91) of currently available computer security publications, including ordering information, can be obtained from NIST.

7. Applicability. This standard is applicable to all Federal departments and agencies that use pubic key based authentication systems to protect unclassified information within computer and digital telecommunications systems that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. This standard shall be used by all Federal departments and agencies in designing, acquiring and implementing public key based, challenge-response authentication systems at the application layer within computer and digital telecommunications systems. This includes all systems that Federal departments and agencies operate or that are operated for them under contact. In addition, this standard may be used at other layers within computer and digital telecommunications systems.

This standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it is either cost effective or provides interoperability for commercial and private organizations.

8. Applications. Numerous applications can benefit from the incorporation of entity authentication based on public key cryptography, when the implementation of such technology is considered cost-effective. Networking applications that require remote login will be able to authenticate clients who have not previously registered with the host, since secret material (e.g., a password) does not have to be exchanged beforehand. Also, point-to-point authentication can take place between users who are unknown to one another. The authentication protocols in this standard may be used in conjunction with other pubic key-based systems (e.g., a public key infrastructure that uses public key certificates) to enhance the security of a computer system.

9. Specifications. Federal Information Processing Standard (FIPS) 196, Entity Authentication Using Public Key Cryptography (affixed).

10. Implementations. The authentication protocols described in this standard may be implemented in software, firmware, hardware, or any combination thereof.

11. Export Control. Implementations of this standard are subject to Federal Government export controls as specified in Title 15, Code of Federal Regulations, Parts 768 through 799. Exporters are advised to contact the Department of Commerce, Bureau of Export Administration, for more information.

12. Implementation Schedule. This standard becomes effective April 6, 1997.

13. Qualifications. The authentication technology described in this standard is based upon information provided by sources within the Federal Government and private industry. Authentication systems are designed to protect against adversaries (e.g., hackers, organized crime, economic competitors) mounting cost-effective attacks on unclassified government or commercial data. The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff.

While specifications in this standard are intended to maintain the security of an authentication protocol, conformance to this standard does not guarantee that a particular implementation is secure. It is the responsibility of the manufacturer to build the implementation of an authentication protocol in a secure manner. This standard will be reviewed every five years in order to assess its adequacy.

14. Waivers. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may re-delegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or

b. Cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive classified portions clearly identified, shall be sent to: National Institute of Standards and Technology, ATTN: FIPS Waiver Decisions, Building 820, Room 509, Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the *Commerce Business Daily* as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.

15. Where to Obtain Copies. Copies of this publication are available for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 196 (FIPS PUB 196), and identify the title. When microfiche is desired, this should be specified. Payment may be made by check, money order, credit card, or deposit account.

[FR Doc. 97–3824 Filed 2–14–97; 8:45 am]

BILLING CODE 3510–CN–M

National Oceanic and Atmospheric Administration

[I.D. 020797A]

Gulf of Mexico Fishery Management Council; Public Meetings

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 will convene public meetings.

DATES: The meetings will be held on March 10–13,1997.

ADDRESSES: These meetings will be held at the Holiday Inn on the Beach, 365 East Beach Boulevard, Gulf Shores, Alabama; telephone: 334–948–6191.

Council address: Gulf of Mexico Fishery Management Council, 3018 U.S. Highway 301 North, Suite 1000, Tampa, FL 33619.

FOR FURTHER INFORMATION CONTACT: Wayne E. Swingle, Executive Director, Gulf of Mexico Fishery Management Council; telephone: (813) 228–2815.

SUPPLEMENTARY INFORMATION:

Council

March 12

8:30 a.m.—Convene.

8:45 a.m. - 11:30 a.m.—Receive public testimony on Vermilion Snapper Total Allocable Catch (TAC).

1:00 p.m. - 2:30 p.m.—Receive a report of the Reef Fish Management Committee.

2:30 p.m. - 3:30 p.m.—Receive a report of the Scientific and Statistical (SSC) Selection Committee. (CLOSED SESSION).

3:30 p.m. - 5:00 p.m.—Receive a report of the Advisory Panel (AP) Selection Committee. (CLOSED SESSION).

March 13

8:30 a.m. - 9:30 a.m.—Receive a report of the Shrimp Management Committee.