made to the Tariff Act of 1930 (''the Act'') by the Uruguay Round Agreements Act. In addition, unless otherwise indicated, all citations to the Department's regulations are to the regulations at 19 CFR part 351 (April 2001).

Scope of Investigation

The product covered by this investigation is certain welded carbon and alloy line pipe, of circular cross section and with an outside diameter greater than 16 inches, but less than 64 inches, in diameter, whether or not stencilled. This product is normally produced according to American Petroleum Institute (API) specifications, including Grades A25, A, B, and X grades ranging from X42 to X80, but can also be produced to other specifications. The product currently is classified under U.S. Harmonized Tariff Schedule (HTSUS) item numbers 7305.11.10.30, 7305.11.10.60, 7305.11.50.00, 7305.12.10.30, 7305.12.10.60, 7305.12.50.00, 7305.19.10.30. 7305.19.10.60, and 7305.19.50.00. Although the HTSUS item numbers are provided for convenience and customs purposes, the written description of the scope is dispositive. Specifically not included within the scope of this investigation is American Water Works Association (AWWA) specification water and sewage pipe and the following size/grade combinations; of line pipe:

- Having an outside diameter greater than or equal to 18 inches and less than or equal to 22 inches, with a wall thickness measuring 0.750 inch or greater, regardless of grade.
- Having an outside diameter greater than or equal to 24 inches and less than 30 inches, with wall thickness measuring greater than 0.875 inches in grades A, B, and X42, with wall thickness measuring greater than 0.750 inches in grades X52 through X56, and with wall thickness measuring greater than 0.688 inches in grades X60 or greater.
- Having an outside diameter greater than or equal to 30 inches and less than 36 inches, with wall thickness measuring greater than 1.250 inches in grades A, B, and X42, with wall thickness measuring greater than 1.000 inches in grades X52 through X56, and with wall thickness measuring greater than 0.875 inches in grades X60 or greater.
- Having an outside diameter greater than or equal to 36 inches and less than 42 inches, with wall thickness measuring greater than 1.375 inches in grades A, B, and X42, with wall thickness measuring greater than 1.250 inches in grades X52 through X56, and with wall thickness measuring greater than 1.125 inches in grades X60 or greater.
- Having an outside diameter greater than or equal to 42 inches and less than 64 inches, with a wall thickness measuring greater than 1.500 inches in grades A, B, and X42, with wall thickness measuring greater than 1.375 inches in grades X52 through X56, and with wall thickness measuring greater than 1.250 inches in grades X60 or greater.
- Having an outside diameter equal to 48 inches, with a wall thickness measuring 1.0 inch or greater, in grades X–80 or greater.

Antidumping Duty Order

In accordance with section 735(a) of the Act, the Department made its final determination that welded large diameter line pipe from Japan is being sold at less than fair value. *See Notice of Final Determination of Sales at Less Than Fair Value: Welded Large Diameter Line Pipe from Japan,* 66 FR 47172 (September 11, 2001).

On October 25, 2001, in accordance with section 735(d) of the Act, the U.S. International Trade Commission (''ITC'') notified the Department that a U.S. industry is ''materially injured,'' within the meaning of section 735(b)(1)(A)(i) of the Act, by reason of less-than-fair-value imports of welded large diameter line pipe from Japan.

Therefore, in accordance with section 736(a)(1) of the Act, the Department will direct U.S. Customs to assess, upon further advice by the Department, antidumping duties equal to the amount by which the normal value of the merchandise exceeds the export price of the merchandise for all relevant entries of welded large diameter line pipe from Japan. These antidumping duties will be assessed on all imports of the subject merchandise that are entered, or withdrawn from warehouse, for consumption on or after June 27, 2001, the date of publication of the preliminary determination in the **Federal Register** (*see Notice of Preliminary Determination of Sales at Less Than Fair Value: Welded Large Diameter Line Pipe From Japan,* 66 FR 34151). On or after the date of publication of this notice in the **Federal Register**, Customs officers must require, at the same time as importers normally would deposit estimated duties, cash deposits based on the rates listed below. The ''All Others'' rate applies to all exporters of subject merchandise not specifically listed. The weighted-average dumping margins are as follows:

Manufacturer/Exporter	Margin (percent)
Nippon Steel Corporation (Nippon)	30.80
Kawasaki Steel Corporation (Kawasaki)	30.80
All Others	30.80

This notice constitutes the antidumping duty order with respect to welded large diameter line pipe from Japan. Interested parties may contact the Department's Central Records Unit, Room B–099 of the main Commerce building, for copies of an updated list of antidumping duty orders currently in effect.

This order is published in accordance with section 736(a) of the Act.

Dated: November 30, 2001.

Richard W. Moreland,

Acting Assistant Secretary for Import Administration.

[FR Doc. 01–30288 Filed 12–5–01; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 000929280–1201–01]

RIN 0693–ZA42

Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce approves FIPS 197, Advanced Encryption Standard (AES), and makes it compulsory and binding on Federal agencies for the protection of sensitive, unclassified information. A new robust encryption algorithm was needed to replace the aging Data Encryption Standard (FIPS 46–3), which had been developed in the 1970s. In September 1997, NIST issued a **Federal Register** notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free worldwide. Following the submission of 15 candidate algorithms and three publicly held conferences to discuss and analyze the candidates, the field was narrowed to five candidates. NIST continued to study all available information and analyses about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to propose for the AES.

EFFECTIVE DATE: This standard is effective May 26, 2002.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 10 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

A copy of FIPS 197 is available electronically from the NIST web site at: *<http://csrc.nist.gov/encryption/aes/index.html/>*.

SUPPLEMENTARY INFORMATION: A notice was published in the **Federal Register** (Volume 66, Number 40, pp. 12762–3) on February 28, 2001, announcing the proposed FIPS for Advanced Encryption Standard 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 be 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 21 private sector organizations, individuals, and groups of individuals, and from one federal government organization. None of the comments opposed the adoption of the AES as a Federal Information Processing Standard. Comments supported the selection of the algorithm and commended the clear, well-written presentation of the standard. Some comments offered editorial suggestions, pointed out perceived inconsistencies in the text, and requested clarifications. All of the editorial recommendations were carefully reviewed, and changes were made to the standard where appropriate.

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

Comment: The FIPS for AES should include support for additional block and key sizes. This would take advantage of the AES algorithm's built-in flexibility, making it better suited for use in a hashing mode and with communications applications that require minimal overhead (padding).

Response: NIST recognizes that one of the AES algorithm's strengths is its inherent support for additional block and key sizes. However, other block and key sizes have not been subjected to the same public analyses as those sizes that are provided for in the recommended FIPS. As a result, NIST believes that it would not be appropriate to include the additional sizes at this time. The block and key sizes are specified as parameters in the recommended FIPS, and could be modified to include other block and key sizes in the future if needed. The recommended standard explains that the use of parameters in the specification is intended to encourage AES implementers to build their applications and systems with future flexibility and adaptability in mind. NIST will monitor future developments, and will consider adding more parameters to the specification if needed in the future.

Comment: For added security, and to meet the needs for extremely long-term security, NIST should increase the number of rounds that are specified by the AES algorithm (i.e., the amount of processing used for encryption and decryption). Since new techniques to break the algorithm may evolve, the margin of security offered by the algorithm should be increased.

Response: Prior to its evaluation of the five finalist candidate algorithms, NIST's AES selection team discussed the issue of whether the number of rounds should be changed for one or more of the algorithms; the selection team decided to consider only the algorithms as initially submitted. Changing the number of prescribed rounds would change the way that the algorithm was defined (e.g., its key schedule), and the process of proposing, reviewing, and evaluating an algorithm would have to start over from the beginning. If the number of rounds were changed, many of the security and performance analyses that had already been performed on the candidate algorithms would no longer be useful.

Furthermore, throughout the development and review of the recommended FIPS, there was little agreement on which key sizes should have more rounds, and less agreement on how many rounds to add. Some who commented on the Draft FIPS proposed adding just two rounds, while another comment suggested adding 114 rounds.

NIST is not aware of advances in cryptographic techniques that would threaten the security provided by the recommended FIPS, but will continue to follow developments, to reevaluate the standard, and to consider changes or additions that might be needed. As with its other cryptographic standards, NIST will review the recommended FIPS every five years to consider whether the standard should be reaffirmed, amended, or withdrawn.

Comment: Since the AES algorithm allows three different key sizes, NIST should provide guidance to users regarding how and for what purpose(s) the different keys should be used.

Response: NIST is currently developing a guideline that will address numerous key management issues, including considerations for selecting from among multiple key sizes. Details on the content and development of that guideline are available on NIST's web pages http://csrc.nist.gov/encryption/kms/white-paper.pdf.

Comment: Statements in the FIPS are unclear and ambiguous regarding validation requirements for AES implementations. Additionally, many of these statements refer to FIPS 140–2, which has not been approved and which has a transition period when both FIPS 140–1 and FIPS 140–2 are in effect.

Response: FIPS 140–2 was approved in May 2001, and became effective on November 25, 2001. However, references to FIPS 140–2 have been removed in order to limit any misunderstandings.

Following approval of this recommended FIPS, vendors may request that their AES implementation be tested and validated either for conference to the AES specification or in conjunction with a cryptographic module validation test (i.e., validation testing for FIPS 140–2). The process is the same for all testing of implementations of FIPS-approved algorithms under the Cryptographic Module Validation Program.

Comment: Comments indicated concern about the padding to be used when the length of the data to be encrypted was not an even multiple of the block size. Other comments proposed more optimal specifications of the algorithm.

Response: NIST considers padding and optimization to be outside the scope of this standard. Padding will be addressed in a standard or recommendation to be developed on the modes of operation for the AES, and in the applications and protocols that use the AES.

It is expected that many optimization of the AES will be developed over time. NIST plans to post information that it receives on optimization issues on its web pages with the permission of the submitter.

Comment: One comment recommended the selections of a different algorithm, one that had not been submitted during the AES development process.

Response: NIST conducted an open process to solicit and evaluate algorithms for consideration for the AES. All candidate algorithms have been thoroughly reviewed and analyzed by the international cryptographic community.

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.

Executive Order 12866: This notice has been determined not to be significant for the purposes of E. O. 12866.

Dated: November 28, 2001.

Karen H. Brown,

Acting Director, National Institute of Standards and Technology.

[FR Doc. 01–30232 Filed 12–5–01; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 120301A]

Proposed Information Collection; Comment Request; Economic Data Collection for the Atlantic Wreckfish Fishery

AGENCY: National Oceanic and Atmospheric Administration (NOAA).

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995, Pub. L. 104–13 (44 U.S.C. 3506 (c)(2)(A)).

DATES: Written comments must be submitted on or before February 4, 2002.

ADDRESSES: Direct all written comments to Madeleine Clayton, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6086, 14th and Constitution Avenue NW, Washington DC 20230 (or via Internet at MClayton@doc.gov).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument(s) and instructions should be directed to Jim Waters, Department of Commerce, NOAA, National Marine Fisheries Service, 101 Pivers Island Road, Beaufort, NC 28516–9722, (252–7288710).

SUPPLEMENTARY INFORMATION:

I. Abstract

The National Marine Fisheries Service (NMFS) proposes to collect to conduct a one-time census to collect economic, sociocultural, and demographic data about commercial fishing for wreckfish (*Polyprion americanus*) along the U.S. south Atlantic coast. The wreckfish fishery has been managed with individual transferable quotas (ITQs) since 1992. Few shareholders currently fish for wreckfish, yet they have not sold or leased their shares. This project will address why shareholders chose not to participate in the wreckfish fishery, where and for what species they did fish, and why they did not sell or lease their unused quota to generate revenue even though they did not fish for wreckfish. Equally important is to determine if the process of developing an ITQ system contributed to the rapid increase in fishing effort in the early 1990s. The results of this inquiry could offer important lessons for economists, fishery managers and others researching the appropriateness of applying ITQ systems in other fisheries in the southeast.

II. Method of Collection

Data will be collected through personal interviews with approximately 50 past and current shareholders in the ITQ management system for the wreckfish fishery. Interviews will include open-ended questions so that respondents can put into their own words their thoughts, interpretations and experiences with the fishery and the ITQ management program. All interviews will be tape-recorded and transcribed. Results of the study will be made available both through publications and on a National Marine Fisheries Community Impacts web page. Participation in the study will be voluntary.

III. Data

OMB Number: None.

Form Number: None.

Type of Review: Regular submission.

Affected Public: Business or other for-profit organizations.

Estimated Number of Respondents: 50.

Estimated Time Per Response: 2 hours.

Estimated Total Annual Burden Hours: 100.

Estimated Total Annual Cost to Public: $0.

IV. Request for Comments

Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: November 29, 2001.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Office of the Chief Information Officer.

[FR Doc. 01–30291 Filed 12–5–01; 8:45 am]

BILLING CODE 3510–22–S

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 120301C]

Proposed Information Collection; Comment Request; Highly Migratory Species Logbooks

AGENCY: National Oceanic and Atmospheric Administration (NOAA).

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995, Pub. L. 104–13 (44 U.S.C. 3506 (c)(2)(A)).

DATES: Written comments must be submitted on or before February 4, 2002.

ADDRESSES: Direct all written comments to Madeleine Clayton, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6086, 14th and Constitution Avenue NW, Washington DC 20230 (or via Internet at MClayton@doc.gov).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument(s) and instructions should be directed to Jill Stevenson at the National Marine Fisheries Service (NMFS) Highly Migratory Species Division, 1315 East-West Highway, Silver Spring, MD 20910, or by email at *jill.stevenson@noaa.gov*or phone at 301–713–2347.

SUPPLEMENTARY INFORMATION: