

Department's countervailing duty questionnaire.

In accordance with section 751(a)(2)(B) of the Act and section 351.214(d) of the Department's regulations, we are initiating a new shipper review of the countervailing duty order on certain cut-to-length carbon-quality steel plate from Indonesia. In accordance with 19 CFR 351.214(h)(i), we intend to issue the preliminary results of this review not later than 180 days from the date of publication of this notice. In a countervailing duty proceeding, the standard period of review in a new shipper review is the same as that specified in 19 CFR 351.213(e)(2) for an administrative review. Although the first administrative review of this order covers July 26, 1999 through December 31, 2000, the new shipper, PT. Gunung Rajapaksi, had no shipments prior to January 1, 2000. The Department generally calculates subsidies on a calendar year basis, and PT. Gunung Rajapaksi had no shipments before 2000; therefore, we will review the subsidies received by the company only for calendar year 2000.

Countervailing duty proceeding	Period to be reviewed
Indonesia: Certain Cut-to-Length Carbon-Quality Steel Plate, C-560-806: PT. Gunung Rajapaksi .....	01/01/00-12/31/00

Concurrent with publication of this notice, and in accordance with 19 CFR 351.214(e), we will instruct the Customs Service to suspend liquidation of any unliquidated entries of the subject merchandise from the relevant exporter or producer, and to allow, at the option of the importer, the posting of a bond or security in lieu of a cash deposit for each entry of the merchandise exported by the company listed above, until the completion of the review.

Interested parties may submit applications for disclosure under administrative protective order in accordance with 19 CFR 351.305 and 351.306.

This initiation notice is in accordance with section 751(a) of the Act (19 U.S.C. 1675(a)) and 19 CFR 351.214.

Dated: March 19, 2001.

**Holly A. Kuga,**

*Acting Deputy Assistant Secretary for Import Administration, Group II.*

[FR Doc. 01-7553 Filed 3-26-01; 8:45 am]

**BILLING CODE 3510-DS-P**

**DEPARTMENT OF COMMERCE**

**National Institute of Standards and Technology**

**Public Meeting Announcing a Workshop for the Analysis of Modes of Operation for Symmetric Key Block Cipher Algorithms**

**AGENCY:** National Institute of Standards and Technology, Commerce.

**ACTION:** Notice of public workshop.

**SUMMARY:** The National Institute of Standards and Technology (NIST) announces a workshop on modes of operation for securing data using symmetric key block cipher algorithms, such as the algorithm specified in the draft Advanced Encryption Standard (AES). Interested parties may suggest ideas or submit papers for discussion at the workshop, including proposals of modes of operation, to the address below.

**DATES:** The Second Modes of Operation Workshop will be held on August 24, 2001, from 9:00 a.m. to 5:00 p.m.

**ADDRESSES:** The workshop will be held at the Holiday Inn Santa Barbara, 5650 Calle Real, Goleta, California. Details regarding workshop registration will be available at the modes home page: <http://csrc.nist.gov/encryption/aes/modes/>. Suggestions, questions, comments or submissions should be sent to Modes of Operation Workshop, Attn: Elaine Barker, NIST, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930, or to [EncryptionModes@nist.gov](mailto:EncryptionModes@nist.gov).

**FOR FURTHER INFORMATION CONTACT:** For further information, contact [EncryptionModes@nist.gov](mailto:EncryptionModes@nist.gov) or one of the following: Elaine Barker, NIST, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930; telephone 301-975-2911; fax 301-948-1233 or via e-mail at [Elaine.barker@nist.gov](mailto:Elaine.barker@nist.gov); or Morris Dworkin 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930; telephone 301-975-2354; fax 301-948-1233; or via e-mail at [morris.dworkin@nist.gov](mailto:morris.dworkin@nist.gov).

**SUPPLEMENTARY INFORMATION:** Block ciphers can be used as building blocks for encryption modes and for other modes for securing data. For example, block ciphers can be used in the construction of message authentication codes, hash algorithms, and random bit generators. With the advent of new block ciphers, such as the AES, there is an opportunity to update such modes of operation for current and future applications and technology.

The purpose of this **Federal Register** notice is to announce a workshop on

modes of operation for securing data using symmetric key block cipher algorithms, such as the algorithm specified in the draft Advanced Encryption Standard (AES). Prior to the workshop, suggestions and submissions from the public to aid NIST in planning an appropriate workshop and facilitate the comparison and analysis of block cipher modes of operation are welcome. The workshop will aid NIST in developing a standard or guideline that is secure and responsive to the needs of government, industry, and the public. NIST will consider for discussion at the workshop, at a minimum, the modes that were proposed at the October 20, 2000 public workshop on this topic. These are available at the modes home page, and NIST encourages public analysis of these modes.

The workshop may also consider other existing modes or their generalizations, or other modes that are proposed in comments and papers. It will be helpful to receive analysis and proposals for variations of counter mode, arising from alternative methods for prescribing the generation of counters. All suggestions received will be publicly available at the modes home page.

In order to encourage a common framework for comparison, a workshop approach to evaluate and analysis is available on the modes home page. NIST believes that participants in the upcoming workshop would be interested in comments that include statements regarding the intellectual property and/or licensing requirements of any proposed modes. Test vectors will also be useful, to provide analyzers of the modes a means to check the validity of their implementations. Fuller descriptions are available at the modes web site.

The results of the workshop will aid NIST's efforts to develop a complete "suite" of modes of operation from which individual modes can be selected to fit the needs of a wide range of applications and environments. The recommended modes are expected to support the eventual Advanced Encryption Standard (AES) and other block ciphers.

Submissions for discussion at the workshop should be made early enough to provide time to prepare the meeting agenda. Papers proposing new modes of operation are requested as soon as possible, to provide time for the analysis of the new proposals.

**Authority:** NIST's activities to develop computer security standards to protect sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST in section

5131 of the Information Technology Management Reform Act of 1996 (P.L. 104-106), the Computer Security Act of 1987 (Pub. L. 100-235), and Appendix III to Office of Business Management Circular A-130.

Dated: March 19, 2001.

**Karen Brown,**

*Acting Director, NIST.*

[FR Doc. 01-7497 Filed 3-26-01; 8:45 am]

**BILLING CODE 3510-CN-M**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

[I.D. 032101D]

#### 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 (Council) will convene a public meeting of the Red Drum Stock Assessment Panel (RDSAP).

**DATES:** The Council's RDSAP will meet on Monday, April 10, 2001 from 9:30 a.m. to 5:00 p.m.

**ADDRESSES:** The meeting will be held at the New Orleans Airport Hilton, 901 Airline Highway, Kenner, LA 70062; (504)465-1157.

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

**FOR FURTHER INFORMATION CONTACT:** Peter B. Hood, Biologist, Gulf of Mexico Fishery Management Council; telephone: (813) 228-2815.

**SUPPLEMENTARY INFORMATION:** The RDSAP will convene to develop a standardized stock assessment methodology that can accept area (state)-specific data and work with these within the context of a Gulf stock assessment. In addition, the RDSAP will hear about new life history research conducted by Louisiana State University personnel and will consider available data on shrimp-trawl bycatch mortality and historic length composition of the commercial catch that may have not been used in the last stock assessment conducted by NMFS. A copy of the agenda can be obtained by calling the Council office at (813)228-2815.

Although other issues not on the agenda may come before the RDSAP for discussion, in accordance with the Magnuson-Stevens Fishery Conservation and Management Act,

those issues may not be the subject of formal action by the RDSAP during this meeting. The RDSAP's actions will be restricted to those issues specifically identified in the agenda listed as available by this notice.

#### Special Accommodations

The meeting is open to the public and is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to the Council office (see **ADDRESSES**) by April 3, 2001.

Dated: March 21, 2001.

**Richard W. Surdi,**

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

[FR Doc. 01-7543 Filed 3-26-01; 8:45 am]

**BILLING CODE 3510-22-S**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

[I.D. 032101B]

#### Mid-Atlantic 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 Mid-Atlantic Fishery Management Council's (Council) Comprehensive Management Committee (CMC) will hold a public meeting.

**DATES:** The meeting will be held on Tuesday, April 10, 2001, from 10 a.m. until 5 p.m.

**ADDRESSES:** This meeting will be held at the Embassy Suites Hotel Philadelphia Airport, 9000 Bartram Avenue, Philadelphia, PA; (610) 561-1776.

*Council address:* Mid-Atlantic Fishery Management Council, 300 South New Street, Room 2115, Dover, DE 19904.

**FOR FURTHER INFORMATION CONTACT:** Daniel T. Furlong, Executive Director, Mid-Atlantic Fishery Management Council; (302) 674-2331, ext. 19.

**SUPPLEMENTARY INFORMATION:** The purpose of this meeting is to address the development of future committee activities and actions, and provide priority recommendations to the Council regarding its future activities and actions. For purposes of establishing Council priorities, the committee will review and discuss the following items:

1. Consider utility of ecosystem management;

2. Address implications of Marine Protected Areas (sea mapping data review);

3. Identify possible effort management scenarios;

4. Consider economic impacts of management measures (highest and best use of the resource);

5. Address managing a recovering fishery;

6. Analyze and redesign the fishery management infrastructure;

7. Address economic and social impacts of fishery management;

8. Achieve maximum harvest while minimizing impacts;

9. Achieve maximum harvest while using minimum fuel;

10. Manage harvest for the maximum economic benefit to the nation;

11. Develop a stable year-round infrastructure;

12. Resolve dilemma whereby fishery management can't support all traditional entities and/or communities;

13. Address utility of Individual Transferable Quota applications;

14. Consider conducting a management experiment whereby a selected number of boats fish under a particular format to test fundamental changes in management approaches;

15. Consider fishing as farming and manage activity accordingly;

16. Evaluate the extent and scope of the Mid-Atlantic fishery as to actual and potential capacity in terms of number of boats, number of permits, landings, etc.; and

17. Explore the notion of cumulative trip limits and associated impact on bycatch

Other issues and items that arise during this meeting can become part of the rating and ranking process that will ultimately be reduced to writing as a set of priorities to be recommended to the Council for its consideration and action.

Although other issues not contained in this agenda may come before this Council for discussion, in accordance with the Magnuson-Stevens Fishery Conservation and Management Act, those issues may not be the subject of formal Council action during this meeting. Council action will be restricted to those issues specifically identified in the agenda listed in this notice.

#### Special Accommodations

This meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Joanna Davis at the Council Office (see **ADDRESSES**) at least 5 days prior to the meeting date.