India; Final Results of Antidumping Duty Administrative Review and Partial Rescission of Administrative Review, 65 FR 48965, 48968 (Aug. 10, 2000)). In this review, there are no circumstances indicating that this margin is inappropriate as facts available. There are no calculated margins in this review. Therefore, we find that the 19.54 percent rate is corroborated to the greatest extent practicable in accordance with section 776(c) of the Act.

Preliminary Results of the Reviews

We preliminarily determine the following weighted-average dumping margin:

Manufacturer/ exporter	Period	Margin (percent)
Panchmahal	2/1/98–1/31/99	19.54

Any interested party may request a hearing within 30 days of publication of this notice. A hearing, if requested, will be held 37 days after the publication of this notice, or the first business day thereafter. Interested parties may submit case briefs within 30 days of the date of publication of this notice. Rebuttal briefs, which must be limited to issues raised in the case briefs, may be filed not later than 35 days after the date of publication of this notice. The Department will issue the final results of this administrative review, which will include the results of its analysis of issues raised in any such comments, within 120 days of publication of these preliminary results.

Upon completion of this administrative review, the Department shall determine, and the Customs Service shall assess, antidumping duties on all appropriate entries. The Department will issue appraisement instructions directly to the Customs Service.

The following deposit requirements will be effective upon publication of the final results of this administrative review for all shipments of stainless steel bar from India entered, or withdrawn from warehouse, for consumption on or after the publication date, as provided for by section 751(a)(1) of the Act: (1) The cash deposit rate for the reviewed company will be the rate established in the final results of this review; (2) if the exporter is not a firm covered in this review, but was covered in a previous review or the original LTFV investigation, the cash deposit rate will continue to be the company-specific rate published for the most recent period; (3) if the exporter is not a firm covered in this review, a previous review, or the original LTFV 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 (4) the cash deposit rate for all other manufacturers and/or exporters of this merchandise, shall be 12.45 percent, the ''all others'' rate established in the LTFV investigation (59 FR 66915, December 28, 1994).

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

This notice also serves as a preliminary reminder to importers of their responsibility under 19 CFR 351.402(f) 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 administrative review and notice are in accordance with sections 751(a)(1) and 777(i)(1) of the Act.

Dated: January 29, 2001.

Bernard T. Carreau,

Fulfilling the duties of Assistant Secretary for Import Administration.

[FR Doc. 01–2980 Filed 2–2–01; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of a Government-Industry IT Security Forum To Discuss Strategies for the Development of Security Requirements and Specifications for Computing and Real-Time Control Systems

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice of public meeting.

SUMMARY: The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), partners in the National Information Assurance Partnership (NIAP), invite interested parties to attend a government-industry IT security forum to discuss potential public and private sector strategies for the development of security requirements and specifications needed for the protection of government, business and personal computing and real-time control systems.

The primary purpose of the IT security forum is to bring national attention to the concept of security requirements definition and its importance in developing a more secure information infrastructure within the United States. Leaders from government, industry, and academia will have an opportunity to share their views on the role of security requirements in the development, testing and acquisition of commercial products and systems. There will also be discussion on prospective approaches to security requirements development, the importance of national and international standards, cost-effective and timely testing strategies, and the use of state-of-the-art tools and techniques in this area.

The Government-Industry IT Security Forum will follow the First Symposium on Requirements Engineering for Information Security (SREIS) hosted by the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS) in cooperation with the North Carolina State University (NCSU) E-commerce program and the Association for Computing Machinery (ACM).

DATES: The IT Security Forum will take place on March 7, 2001 from 9:00 a.m. until 5:00 p.m.

ADDRESSES: University Place Conference Center and Hotel, IUPUI (Indiana University-Purdue University at Indianapolis), 850 West Michigan Street, Indianapolis, IN 46202–5198.

FOR FURTHER INFORMATION CONTACT: Forum Coordinator, Dr. Ron Ross, Information Technology Laboratory, NIST, 100 Bureau Drive, Mailstop 8930, Gaithersburg, MD 20899–8930; Telephone: (301) 975–5390; E-mail: *rross@nist.gov*; World wide web: *http://niap.nist.gov.* Comments and suggestions on the proposed forum agenda are welcomed and appreciated.

Forum Registration: To register for the Government-Industry IT Security Forum, visit the NIAP web site at *http://niap.nist.gov* or the Purdue CERIAS web site at *http://www.cerias.purdue.edu/sreis.html.*

Registrations must be received by February 24, 2001. For additional registration or logistics information, please contact Mr. John Wellman, Business Office, Conference Division, Purdue University; Telephone: (800) 359–2968 or (765) 494–0243; Fax: (765) 494–0567; E-mail: *jmw@purdue.edu.*

SUPPLEMENTARY INFORMATION: For over a decade, NIST and NSA have worked cooperatively with government agencies, industry, and academia on the development of testing and evaluation

programs to assess the security features in commercial information technology (IT) products. There have also been extensive efforts, both nationally and internationally, to develop IT security evaluation criteria to support these assessment programs. During that period, few products were tested and there were continuing questions about the cost and timeliness of the evaluations. Additionally, due to operational considerations, many consumers did not use the products in their evaluated configurations.

With all of the focus on criteria and testing programs, there has been very little attention paid to helping consumers define and create their IT security requirements. There has also been insufficient effort to bring consumers and producers of products and systems together to build a better understanding of what customers need in the realm of security and what industry is able to deliver in a cost-effective manner.

Consumers of IT products from a variety of public and private sector communities of interest, *e.g.,* healthcare, banking and finance, defense, national security, insurance, legal, manufacturing, process control, telecommunications, etc., continue to express interest in obtaining better ways to convey their security requirements to industry in an effort to build more secure systems for their respective enterprises. New and innovative approaches to developing security requirements for commercial products and systems are being explored in many venues. One such effort, led by NIST, NSA, and other standards and security organizations worldwide, has been the development of the Common Criteria for Information Technology Security Evaluation.

The Common Criteria provides a mechanism for consumers to articulate their IT security requirements and a common structure by which consumers and producers can exchange perspectives on what security features are needed and what security features can be provided. The Common Criteria became an international standard (ISO/IEC 15408) in 1999 and now serves as the foundation for a formal fourteen-nation arrangement recognizing the results of security evaluations conducted in participating nations.

Consumers and producers of IT products and systems can now use the Common Criteria to produce well-defined sets of security requirements in many areas such as operating systems, database management systems, smart cards, telecommunications and networks devices, and applications. There is also an opportunity to address the ''realistic configuration'' and ''timeliness of evaluation'' problems by allowing producers and consumers of products to agree on a set of security requirements (for both features and assurances) that meet the consumer's real needs.

Without consumer involvement in helping to shape the demand for evaluated products through the security requirements definition process, the ultimate goal of improving the confidence consumers have in the products they purchase, may be more difficult to achieve. Greater confidence in the security features of the individual component products will facilitate the development of more secure systems for Federal agencies and private sector enterprises, and ultimately, result in a more secure information infrastructure for the United States.

The sponsors of the forum hope to obtain answers to the following questions:

- What are the important information technology areas for general purpose products, *e.g.* operating systems, database systems, firewalls, intrusion detection systems, etc., that could benefit from the development of stable sets of security requirements?
- How are the security requirements for general-purpose products best developed?
- What specific security requirements are needed to address highly reliable, real time systems?
- Are there additional needs for IT security requirements tailored to specific consumer communities (*e.g.,* healthcare, banking, manufacturing, process control)?
- If so, how should these security requirements be developed (process and organization question) and how do they interact with the security requirements for general-purpose products (technical question)?
- What value do consumers, government security experts, and the insurance and audit industries see in third party testing and evaluation of commercial products?
- How much value do consumers place on the assurances received from IT product testing and evaluation and how much product currency are they willing to give up to get it?
- How can the results from component product testing and evaluation be used to increase the level of confidence consumers have in their systems and networks?
- What role should the U.S. Government play in the development of security requirements for key information technology areas that affect the U.S. information infrastructure?
- Should the U.S. Government mandate for Federal agencies, the use of evaluated and validated information technology products built to specific security requirements, *e.g.,* Common Criteria Protection Profiles?

Preliminary Agenda

—Introduction and Forum Overview (NIAP Director)
—Keynote Address (U.S. IT Industry CEO)
—Panel 1: Consumer's Perspective (Invited Participants)
—Panel 2: Insurance, Audit, and Testing Industry Perspectives (Invited Participants)
—Panel 3: IT Industry's Perspective (Invited Participants)
—Panel 4: Research and Development Activities: A Perspective from Academia (Invited Participants)
—Approaches for Developing Requirements: Bringing the Communities Together (Invited Participants)
—Summary and Conclusions (NIAP Director)

Dated: January 29, 2001.

Karen Brown,

Acting Director, NIST.

[FR Doc. 01–2977 Filed 2–2–01; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Call for Applications for Alternate Representatives to the Coral Reef Ecosystem Reserve Council for the Northwestern Hawaiian Islands Coral Reef Ecosystem Reserve

AGENCY: National Marine Sanctuary Program (NMSP), National Ocean Service (NOS), National Oceanic and Atmospheric Administration, Department of Commerce (DOC).

ACTION: Notice and request for applications.

SUMMARY: On December 4, 2000, Executive Order 13178 established the Northwestern Hawaiian Islands Coral Reef Ecosystem Reserve (Reserve). The Executive Order requires the Secretary of Commerce or his or her designee (hereafter ''Secretary'') to establish a Coral Reef Ecosystem Reserve Council (Reserve Council) to provide advice and recommendations on the development of the Reserve Operations Plan and the designation and management of a Northwestern Hawaiian Islands