

steels; (7) tool steels; and (8) silicon manganese steel or silicon electric steel.

The products covered by this review are provided for under the following HTSUS item numbers: 7208.40.3030, 7208.40.3060, 7208.51.0030, 7208.51.0045, 7208.51.0060, 7208.52.0000, 7208.53.0000, 7208.90.0000, 7210.70.3000, 7210.90.9000, 7211.13.0000, 7211.14.0030, 7211.14.0045, 7211.90.0000, 7212.40.1000, 7212.40.5000, 7212.50.0000, 7225.40.3050, 7225.40.7000, 7225.50.6000, 7225.99.0090, 7226.91.5000, 7226.91.7000, 7226.91.8000, 7226.99.0000.

Although the HTSUS subheadings are provided for convenience and Customs purposes, the written description of the scope of this proceeding is dispositive.

#### Rescission of Review

In their February 11, 2003, request that the Department rescind the review, petitioners asserted that the Department's consistent practice has been to rescind an administrative review upon learning that no shipments of subject merchandise occurred during the relevant POR. They cited to several notices in which the Department rescinded antidumping administrative reviews on the basis of lack of shipments. Petitioners also cited to the preliminary results of *Carbon Steel Wire Rod from New Zealand*, 56 FR 33253 (July 19, 1991) and the preliminary results of *Brass Sheet and Strip from Brazil*, 56 FR 33252 (July 19, 1991) as the only two instances they could locate where the Department decided to complete administrative reviews of countervailing duty (CVD) orders for a POR during which no shipments of the subject merchandise occurred. However, they asserted that both of these reviews preceded the Uruguay Round Agreements Act (URAA) and involved a program-wide change in which the subsidy programs to be reviewed had been terminated. Given the post-URAA regulations and practice and the lack of a program-wide change, petitioners argued that the Department should promptly rescind the instant review.

On March 7, 2003, Siderar confirmed that it did not have any shipments of subject merchandise to the United States during the POR. However, Siderar submitted that the Department has the discretion to conduct an administrative review in this case for the purpose of adjusting Siderar's deposit rate. Siderar stated that it requested this administrative review for the sole purpose of having the Department's determination in the recently completed investigation of cold rolled products

from Argentina<sup>1</sup> extended to this case and having the CVD deposit adjusted accordingly. Siderar stated that the factual circumstances of this case are clear and not in dispute.

In support of its position that the Department has the discretion to conduct a CVD administrative review for the purpose of adjusting the cash deposit rate even in the absence of shipments during the review period, Siderar pointed out that the Department has done so in the past. Siderar cited *Carbon Steel Wire Rod From New Zealand*,<sup>2</sup> where a program-wide change involving the termination of two government programs took place, and to precedent.<sup>3</sup> Siderar asserted that, in that case, the Department concluded that Section 751 of the Tariff Act of 1930, as amended (the Act) (19 U.S.C. § 1675 (a)(1)) authorizes it to conduct annual administrative reviews to determine the amount of any net countervailing subsidy and estimated duty to be deposited, even in the absence of entries, shipments, or exports. Siderar acknowledged that the issue in this review does not involve a "program-wide change." However, it argued that the Department's determination in *Cold Rolled* has the same effect as a program-wide change in that it removes the legal and factual basis for the collection of deposits at the rate previously established. See the letter from Siderar to the Department dated March 7, 2003, which is on file in the CRU.

We agree with petitioners that it has been the Department's practice to rescind administrative reviews when we find a lack of exports. See *Certain Hot-Rolled Lead and Bismuth Carbon Steel Products From Germany: Notice of Termination of Countervailing Duty Administrative Review*, 64 FR 44489 (August 16, 1999), and *Final Results and Partial Rescission of Countervailing Duty Administrative Review: Stainless Steel Sheet and Strip From the Republic of Korea*, 68 FR 13267 (March 19, 2003).

In accordance with the Department's regulations, and consistent with its practice, the Department intends to

<sup>1</sup> See *Final Negative Countervailing Duty Determination: Certain Cold-Rolled Carbon Steel Flat Products From Argentina*, 67 FR 62106 (October 3, 2002) (*Cold Rolled*); Issues and Decision Memorandum of September 23, 2002 from Richard W. Moreland to Faryar Shirzad.

<sup>2</sup> *Carbon Steel Wire Rod From New Zealand: Final Results of Countervailing Duty Administrative Review (Carbon Steel Wire from New Zealand)*, 56 FR 28863 (June 25, 1991).

<sup>3</sup> See *Certain Electrical Aluminum Redraw Rod from Venezuela: Final Results of Countervailing Duty Administrative Review*, 56 FR at 14232 (April 8, 1991) ("where the Department Conducted a review and changed the case deposit rate as a result of a program-wide change despite no entries or exports") 56 FR at 28864.

rescind the administrative review of hot-rolled products from Argentina for the period January 1, 2001 to December 31, 2001 due to no shipments during the POR. See 19 CFR section 351.213(d)(3), which states in pertinent part: "The Secretary may rescind an administrative review under this section, in whole or only with respect to a particular exporter or producer, if during the POR, there were no entries, exports, or sales of the subject merchandise."

This notice is in accordance with section 751(a)(1) of the Act, and section 351.213(d) of the Department's regulations.

Dated: May 9, 2003.

**Holly A. Kuga,**

*Acting Deputy Assistant Secretary for Import Administration.*

[FR Doc. 03-12313 Filed 5-15-03; 8:45 am]

BILLING CODE 3510-DS-S

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

[Docket No. 030429105-3105-01]

#### Announcing Draft Federal Information Processing Standard (FIPS) 199 on Standards for Security Categorization of Federal Information and Information Systems; and Request for Comments

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

**ACTION:** Notice; request for comments.

**SUMMARY:** Draft FIPS 199 defines requirements to be used by Federal agencies to categorize information and information systems, and to provide appropriate levels of information security according to a range of risk levels. This draft standard establishes three potential levels of risk (low, moderate, and high) for each of the security objectives of confidentiality, integrity, and availability. The levels of risk are based on what is known about the potential impact or harm. Harmful events can impact agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy). The levels of risk consider both impact and threat, but are more heavily weighted toward impact. Federal information systems, which are often interconnected and interdependent, are vulnerable to a variety of threats (both malicious and unintentional) that could compromise the security of information and information systems.

NIST invites public comments on the Draft FIPS on Standards for Security Categorization of Federal Information

and Information Systems. After the comment period closes, NIST will analyze the comments, make appropriate changes to the document, and then propose the draft standard to the Secretary of Commerce for approval as FIPS PUB 199.

**DATES:** Comments on the Draft FIPS on Standards for Security Categorization of Federal Information and Information Systems must be received on or before August 14, 2003.

**ADDRESSES:** Written comments concerning the Draft FIPS on Standards for Security Categorization of Federal Information and Information Systems may be sent by regular mail to: Information Technology Laboratory, ATTN: Draft FIPS 199, Mail Stop 8930, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. Electronic comments should be sent to: [fips.comments@nist.gov](mailto:fips.comments@nist.gov).

Comments received in response to this notice will be published electronically at: <http://csrc.nist.gov/publications/>.

**Specifications:** Specifications for the Draft FIPS on Standards for Security Categorization of Federal Information and Information Systems are available through the Computer Security Resource Center: <http://csrc.nist.gov/publications/>.

**FOR FURTHER INFORMATION CONTACT:** Dr. Ron S. Ross (301) 975-5390, National Institute of Standards and Technology, Attn: Computer Security Division 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930, Email: [rross@nist.gov](mailto:rross@nist.gov).

**SUPPLEMENTARY INFORMATION:** Under section 5131 of the Information Technology Management Reform Act of 1996 and sections 302-3 of the Federal Information Security Management Act of 2002 (Pub. L. 107-347), the Secretary of Commerce is authorized to approve standards and guidelines for Federal information systems and to make standards compulsory and binding for Federal agencies as necessary to improve the efficiency or security of Federal information systems. The National Institute of Standards and Technology is authorized to develop standards, guidelines, and associated methods and techniques for information systems, other than national security systems, to provide for adequate information security for agency operations and assets.

The Federal Information Security Management Act (FISMA) requires each Federal agency to develop, document, and implement an agency-wide information security program that will

provide information security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

To enable agencies to carry out this responsibility, the FISMA specifically tasked NIST to develop a standard to categorize information and information systems. In addition, NIST was tasked to develop guidelines recommending the types of information to be included in each category, and to develop minimum information security requirements (*i.e.*, management, operational, and technical security controls) for the information and information systems in each category.

In response to the mandate, NIST developed FIPS 199. Draft FIPS 199 defines requirements to be used by Federal agencies to categorize information and information systems, and to provide appropriate levels of information security according to a range of risk levels. This draft standard establishes three potential levels of risk (low, moderate, and high) for each of the security objectives of confidentiality, integrity, and availability. The levels of risk are based on what is known about the potential impact or harm. Harmful events can impact agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy). The levels of risk consider both impact and threat, but are more heavily weighted toward impact. Federal information systems, which are often interconnected and interdependent, are vulnerable to a variety of threats (both malicious and unintentional) that could compromise the security of information and information systems.

This standard for categorizing information and information systems supports the implementation of a common framework that will promote the effective government-wide management and oversight of Federal agency information security programs. The common framework will facilitate the coordination of information security efforts throughout the civilian, national, security, and law enforcement communities, and will enable consistent reporting by agencies to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

NIST is in the process of developing guidance documents for the second and third tasks mandated by the FISMA and will make these documents available for public comment when they are finalized. For the second assigned task,

NIST plans guidelines to help agencies identify, in a consistent manner, the types of information and information systems, (*e.g.*, privacy, medical, proprietary, financial, contractor sensitive, mission critical) appropriate for each category of information and information system. For the third task, NIST plans to develop standards that will describe the minimum sets of security controls for each defined category of information and information system.

**Authority:** Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce, pursuant to section 5131 of the Information Technology Management Reform Act of 1996 (Pub. L. 104-106), the Federal Information Security Management Act of 2002 (Pub. L. 107-347), and Appendix III to Office of Management and Budget Circular A-130.

Executive Order 12866: This notice has been determined to be not significant under Executive Order 12866.

Dated: May 9, 2003.

**Karen H. Brown,**  
Deputy Director, NIST.

[FR Doc. 03-12319 Filed 5-15-03; 8:45 am]

**BILLING CODE 3510-13-P**

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

#### Judges Panel of the Malcolm Baldrige National Quality Award

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

**ACTION:** Notice of closed meeting.

**SUMMARY:** Pursuant to the Federal Advisory Committee Act, 5 U.S.C. app. 2, notice is hereby given that the Judges Panel of the Malcolm Baldrige National Quality Award will meet Wednesday, June 4, 2003. The Judges Panel is composed of nine members prominent in the field of quality management and appointed by the Secretary of Commerce. The purpose of this meeting is to Review the 2003 Baldrige Award Cycle; Discussion of Senior Examiner Training for Site Visits and Final Judging Interaction; Judges' Survey of Applicants; and Judging Process Improvement for Final Judges' Meeting Preparation. The applications under review contain trade secrets and proprietary commercial information