Final Results of the Review

We determine the following percentage weighted-average margin exists for the period July 1, 2000 through June 30, 2001:

Manufacturer/Exporter	Weighted average margin (percentage)
TKN	3.72

Liquidation

The Department shall determine, and U.S. Customs and Border Protection (Customs) shall assess, antidumping duties on all appropriate entries. In accordance with 19 CFR 351.212(b)(1), we have calculated importer-specific assessment rates. The Department will issue appropriate assessment instructions directly to Customs within 15 days of publication of these final results of review. With respect to constructed export price sales, we divided the total dumping margins for the reviewed sales by the total entered value of those reviewed sales for each importer. We will direct Customs to assess the resulting assessment rate against the entered Customs values for the subject merchandise on each of the importer's entries during the POR.

Cash Deposit Requirements

The following deposit requirements will be effective upon publication of this notice of final results of administrative review for all shipments of stainless steel sheet and strip in coils from Germany entered, or withdrawn from warehouse, for consumption on or after the date of publication, as provided by section 751(a)(1) of the Tariff Act: (1) The cash deposit rate for the reviewed company will be the rate shown above; (2) for previously reviewed or investigated companies not listed above, 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 prior review, or the original less-than-fair-value (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 or exporters will continue to be 13.48 percent. This rate is the ''All Others'' rate from the amended final determination in the LTFV investigations. *See Stainless Steel Sheet and Strip in Coils From Germany: Amended Final Determination of Antidumping Duty Investigation*, 67 FR 15178, 15179 (March 29, 2002).

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

This notice also serves as a final reminder to importers of their responsibility under 19 CFR 351.402(f) to file a certificate regarding the reimbursement of antidumping or countervailing 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 or countervailing duties occurred and the subsequent assessment of doubled antidumping duties.

This notice also serves as a reminder to parties subject to administrative protective orders (APO) of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305. Timely written notification of the return or destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and terms of an APO is a violation which is subject to sanction.

We are issuing and publishing this determination and notice in accordance with sections 751(a)(1) and 777(i) of the Tariff Act.

Dated: February 3, 2004.

James J. Jochum,

Assistant Secretary for Import Administration.

Appendix

Comments and Responses

1. Assessment Rate Methodology
2. Interest Expenses
3. Packing Costs
4. Downstream Home Market Sales
5. Treatment of Non-Dumped Sales
6. Other Revisions to Calculation

[FR Doc. 04–2863 Filed 2–9–04; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 030429105–3270–02]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce has approved FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and has made it compulsory and binding on Federal agencies for the protection of: (i) All information within the Federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all Federal information systems other than those information systems designated as national security systems as defined in the United States Code.

The Federal Information Security Management Act (FISMA) requires all Federal agencies to develop, document, and implement agency-wide information security programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FIPS Publication 199 addresses one of the requirements specified in the FISMA. It provides security categorization standards for information and information systems.

The purpose of security categorization standards is to provide a common framework and method for expressing security and to promote effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

DATES: This standard is effective February 10, 2004.

FOR FURTHER INFORMATION CONTACT: Dr. Ron Ross, (301) 975–5390, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

A copy of FIPS Publication 199 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/*.

SUPPLEMENTARY INFORMATION: A notice was published in the **Federal Register** (68 FR 26573) on May 16, 2003, announcing the proposed FIPS Publication 199 on Standards for

Security Categorization of Federal Information and Information Systems 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 being 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 thirteen private sector organizations, individuals and groups of individuals, from eighteen federal government organizations, and from one Canadian government organization.

Many of the comments received recommended editorial changes, expressed concerns about the discussion of risk, risk assessment, threats, and security controls, and asked for clarification about the requirements of the FISMA. None of the comments opposed the adoption of this Federal Information Processing Standard. Many comments supported the concept of categorization of information and information systems and commended the clear, well-written presentation of the standard. All of the editorial and related comments were carefully reviewed, and changes were made to the standard where appropriate. Specifically, certain terminology in FIPS 199 was modified to be consistent with other NIST publications. All future publications will reflect consistent terminology.

Following is an analysis of the comments dealing with technical and implementation issues.

Comment: The major issue raised by a majority of the comments was concern about perceived errors and inconsistencies in the initial draft's discussion of risk, risk assessment, threats, and the determination of security controls. Some of the comments suggested that NIST consider using the term ''level of impact'' instead of ''level of risk'' to apply to the categorization process.

Response: NIST recognizes that some of the initial discussion about risk, risk assessment, threats and the determination of security controls was abbreviated and concise, and that the discussion could have been misinterpreted. The original discussion described three potential levels of risk (low, moderate and high) for each of three security objectives (confidentiality, integrity and availability of information and information systems, which were defined in the FISMA). The levels of risk considered both impact of adverse events and threats to systems, but were more heavily weighted toward impact. The categorization process involves matching the agency's assessment of levels of potential risk to each security objective, considering the occurrence of events that could jeopardize the information and information systems of the agency.

As some of the comments pointed out, risk assessment is part of a well-defined management process conducted by agencies to identify and evaluate risks and risk impacts, and to recommend risk-reducing measures that balance costs and organizational requirements. NIST agrees that the issues of determining levels of risk and conducting risk assessments are part of a structured management process. These issues are covered comprehensively in other NIST publications. Therefore, the focus of the categorization process should be on ''level of impact'' that undesired events could have on information and information systems.

The text of FIPS Publication 199 was changed to describe three levels of potential impact (low, moderate and high) on organizations or individuals if any of the security objectives of confidentiality, integrity and availability of information and information systems were compromised. The security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to the agency. This change responds to the many comments received on this issue, and clarifies the text for agency users. Terms and definitions relating to risk and risk assessments that had been included in the initial draft were removed from the final standard.

Comment: Some comments expressed confusion about the information included in the initial draft about the Federal Information Security Management Act (FISMA) and its requirements, particularly those requirements that are addressed by FIPS Publication 199.

Response: NIST agrees that some of the original discussion in draft FIPS Publication 199 could have been misinterpreted. Therefore, the text was revised to delete extraneous material and to clarify the purpose of FIPS Publication 199. FIPS Publication 199 now clearly defines the impact levels to be used in categorizing information and information systems, and indicates that the standard addresses one of the tasks assigned to NIST by the FISMA. That task is the development of standards to be used by all Federal agencies to categorize information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. Other requirements of the FISMA, such as determination of the types of information and information to be included in each category, will be addressed in future NIST standards and guidelines.

Comment: Some comments suggested changes to Table 1 in the original draft, and asked for an explanation of the use of the table. Examples of impacts for each impact definition were requested.

Response: FIPS Publication 199 was revised to clarify the text and to provide examples of impacts for each definition of impact for each security objective.

Comment: There are no provisions for the use of new technologies or updating of legacy systems.

Response: The provisions of FIPS Publication 199 are independent of the technology used, and can be applied to electronic and non-electronic information.

Comment: An objective for privacy should be added to the objectives of confidentiality, integrity and availability. The loss of privacy and identity theft should be added to the impact definitions.

Response: FIPS Publication 199 was revised to clarify the issue of privacy by specifying that loss of privacy and identify theft are examples of impacts on individuals. The objective of confidentiality, as defined in the FISMA (44 USC, Sec. 3542), encompasses privacy: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Comment: The definition of availability should be modified. Other security objectives (non-repudiation and authentication) should be added

Response: The definition of availability is taken directly from the FISMA legislation and thus, cannot be modified. However, the security objectives mentioned in the public comment, namely nonrepudiation and authenticity are specifically covered in FIPS Publication 199 under the definition of integrity. FISMA's definition of integrity includes the security objectives of nonrepudiation and authenticity so there is no need to modify the definition of availability to include those objectives. Adding additional security objectives independently would make the simple three by three matrix more complex for federal agencies during implementation and not add any appreciable value in

helping to assess the potential impact of loss of information systems supporting those agencies.

Comment: An impact level of ''none'' should be added to the levels of low, moderate and high.

Response: A note was added that an impact level of ''none'' was appropriate only for confidentiality of some information (such as public information). Impact levels of ''none'' are not appropriate for the security objectives of availability and integrity since all agency information and information systems should be protected for availability and integrity.

Comment: The category of information designation should be separate from the category of system designation.

Response: FIPS Publication 199 treats systems categorization separately from information categorization.

Comment: The security objectives of confidentiality, integrity, and availability could be expanded.

Response: FIPS Publication 199 allows agencies to develop and use additional security designators.

Comment: Only two impact levels are needed for non-national security information and systems.

Response: NIST believes that three levels of impact are needed for non-national security systems. Two levels of impact do not provide sufficient granularity to describe the range of potential impacts on federal agency missions resulting from the loss of confidentiality, integrity, or availability of information and information systems. Three impact levels are necessary to adequately describe the potential impact of loss to agency operations and assets ranging from routine administrative support systems at the low end to the most critical systems that are a part of the nation's critical information infrastructure at the high end. The moderate impact level provides another important category to address those systems that are deemed significantly more important than routine support systems, but not critical to the operations of the U.S. government. Three impact levels strike an adequate balance between providing too many categories and making the categorization process too complex and providing too few categories which forces agencies to either undervalue or overvalue the potential impact of loss to their operations and assets.

Comment: FIPS Publication 199 could define what level of risk is to be associated with a security objective required by law. More explicit information is needed to categorize systems. FIPS Publication 199 should present definitive guidance on vulnerabilities, impact and risk management methodology.

Response: These issues are discussed in current NIST publications, or will be addressed in future NIST publications.

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

Dated: February 4, 2004.

Arden L. Bement, Jr.,

Director.

[FR Doc. 04–2885 Filed 2–9–04; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of the American Petroleum Institute's Standards Activities

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice.

SUMMARY: The American Petroleum Institute (API), with the assistance of other interested parties, continues to develop standards, both national and international, in several areas. This notice lists the standardization efforts currently being conducted by API committees. The publication of this notice by the National Institute of Standards and Technology (NIST) on behalf of API is being undertaken as a public service. NIST does not necessarily endorse, approve, or recommend the standards referenced.

ADDRESSES: American Petroleum Institute, 1220 L Street, NW., Washington, DC 20005; telephone (202) 682–8000, *http://www.api.org.*

FOR FURTHER INFORMATION CONTACT: All contact individuals listed in the **SUPPLEMENTARY INFORMATION** section of this notice may be reached at the American Petroleum Institute.

SUPPLEMENTARY INFORMATION:

Background

The American Petroleum Institute develops and publishes voluntary standards for equipment, materials, operations, and processes for the petroleum and natural gas industry. These standards are used by both private industry and by governmental agencies. All interested persons should contact the appropriate source as listed for further information.

Pipeline Committee

New Std 1163 ILI Systems Qualification
New Std 1164 SCADA Security
New Std 1165 SCADA Display

For Further Information Contact: Andrea Johnson, Standards Department, e-mail: *johnsona@api.org.*

Committee on Marketing

Std 2610 Design, Construction, Operation, Maintenance, and Inspection of Terminal and Tank Facilities
NEW API/IP RP 1540, Design Construction, Modification and Maintenance of Aircraft Fueling Facilities
New API/IP Std 1529 Aviation Fueling Hose
RP 1626 Recommended Practice for Storing and Handling Ethanol and Gasoline-ethanol Blends at Distribution Terminals and Service Stations.

For Further Information Contact: David Soffrin, Standards Department, e-mail: *soffrind@api.org.*

Committee on Refining

Corrosion & Materials:

RP 651 Cathodic Protection of Aboveground Petroleum Storage Tanks
RP 652 Lining of Aboveground Petroleum Storage Tanks
New RP 938–C Use of Duplex Stainless Steels in the Oil Refining Industry

Inspection:

Std 510 Pressure Vessel Inspection Code
RP 575 Inspection of Atmospheric and Low Pressure Storage Tanks

Pressure Vessel and Tanks:

Std 620 Design & Construction of Large, Welded, Low-Pressure Storage Tanks
Std 650 Welded Tanks for Oil Storage
Std 653 Tank Inspection, Repair, Alteration, and Reconstruction

Electrical Equipment:

New Std 547 General Purpose Form-wound Squirrel-cage Induction Motors larger than 250 HP
Std 541 Form-Wound Squirrel-cage Induction Motors 500 HP and Larger

Mechanical Equipment:

Std 672 Packaged, Integrally Geared Centrifugal Air Compressors for Petroleum, Chemical, and Gas Industry Services
Std 618 Reciprocating Compressors for Petroleum, Chemical, and Gas Industry Services
Std 619 Rotary Type Positive Displacement Compressors
Std 677 General Purpose Gear Units
Std 684 Tutorial on Rotor Dynamics and Balancing
Std 686 Machinery Installation and Installation Design
Std 610, National Adoption of ISO 13709, Centrifugal Pumps for