require a cash deposit or posting of a bond equal to the estimated preliminary dumping margin reflected in the preliminary determination of sales at less than fair value published in the **Federal Register**. This suspension of liquidation will remain in effect until further notice.

Final Critical Circumstances Determination

We will make a final determination concerning critical circumstances for Russia when we make our final determination regarding sales at less than fair value in this investigation, which will be 75 days after the preliminary determination regarding sales at less than fair value, unless this investigation is extended.

ITC Notification

In accordance with section 733(f) of the Act, we have notified the ITC of our determination. This notice is published pursuant to section 777(i) of the Act.

Dated: November 1, 1999.

Robert S. LaRussa,

Assistant Secretary for Import Administration.

[FR Doc. 99–29062 Filed 11–4–99; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

[C–428–812]

Hot-Rolled Lead and Bismuth Carbon Steel Products From Germany: Extension of Preliminary Results of Countervailing Duty Administrative Review

AGENCY: Import Administration, International Trade Administration, Department of Commerce.

ACTION: Notice of extension of time limit for preliminary results of countervailing duty administrative review.

EFFECTIVE DATE: November 5, 1999.

FOR FURTHER INFORMATION CONTACT: Robert Copyak at 202–482–2209, Office of AD/CVD Enforcement VI, Group II, Import Administration, International Trade Administration, U.S. Department of Commerce, 14th Street and Constitution Ave, NW, Washington, DC 20230.

Time Limits

Statutory Time Limits

Section 751(a)(3)(A) of the Tariff Act of 1930, as amended (the Act), requires the Department to make a preliminary determination within 245 days after the last day of the anniversary month of an order/finding for which a review is requested and a final determination within 120 days after the date on which the preliminary determination is published. However, if it is not practicable to complete the review within the time period, section 751(a)(3)(A) of the Act allows the Department to extend these deadlines to a maximum of 365 days and 180 days, respectively.

Background

On April 30, 1999, the Department published a notice of initiation of administrative review of the countervailing duty order on hot-rolled lead and bismuth carbon steel products from Germany, covering the period January 1, 1998, through December 31, 1998, (64 FR 23269, 23280). The preliminary results are currently due no later than December 1, 1999.

Extension of Preliminary Results of Review

We determine that it is not practicable to complete the preliminary results of this review within the original time limit. Therefore the Department is extending the time limits for completion of the preliminary results until no later than March 30, 2000. *See* Decision Memorandum from Holly A. Kuga to Robert S. LaRussa, dated October 27, 1999, which is on file in the Central Records Unit. We intend to issue the final results no later than 120 days after the publication of the preliminary results notice.

This extension is in accordance with section 751(a)(3)(A) of the Act.

Dated: October 28, 1999.

Bernard T. Carreau,

Deputy Assistant Secretary, Import Administration, Group II.

[FR Doc. 99–29061 Filed 11–4–99; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 98109262–919–02]

RIN 0693–ZA 27

Announcing Approval of Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce has approved Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard, which supersedes FIPS 46–2. FIPS 46–3 provides for the use of the Triple DES as specified in American National Standard (ANSI) X9.52. NIST expects that Triple DES will provide Federal agencies with strong protective measures against associated risks until the Advanced Encryption Standard (AES) is available, probably in 2001.

EFFECTIVE DATE: This standard is effective March 25, 2000.

ADDRESSES: FIPS 46–3 is available on the NIST web page at: <http//csrc.nist.gov/publications/drafts.html>.

Copies of the ANSI X9.52 (Triple DES) standard are available from American Bankers Assoc./DC,X9 Customer Service Dept., P.O. Box 79064, Baltimore, MD 21279–0064, telephone 1–800–338–0626.

Information on the Advanced Encryption Standard under development is available at: <http://www.nist.gov/aes>.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

SUPPLEMENTARY INFORMATION: Federal Information Processing Standard 46, Data Encryption Standard (DES), first issued in 1977, specified the Data Encryption algorithm, to be implemented in hardware devices, for the cryptographic protection of computer data. The standard provided that it be reviewed within five (5) years to assess its adequacy. In 1981, the DES was adopted as an American National Standard and became widely used by the financial community. The first review of the DES was completed in 1983, and the DES was reaffirmed for Federal government use (48 FR 41062). The second review, completed in 1987, again resulted in the reaffirmation of the standard for Federal government use (52 FR 7006). The standard was re-issued as FIPS 46–1 with minor editorial updating. The third review was completed in 1993, and the standard was reaffirmed as FIPS 46–2 for Federal government use (58 FR 69347). FIPS 46–2 provided for software implementations, as well as hardware implementations, of the DES.

When the DES was reaffirmed in 1993, NIST stated that it would ''consider alternatives which offer a higher level of security'' at the next review in 1998. There was concern that the DES 56–bit key was not long enough to prevent an attack by trying all of the possible keys. NIST believed that the key was sufficiently long for the

expected life of the standard and that the security could be increased, when needed, by using the DES for three sequential encryption operations with different keys. This approach is called Triple DES. In 1997, NIST advised Federal organizations that they could use Triple DES if they needed security beyond that provided by the DES.

Since 1998, there have been reports that the DES could be attacked through an exhaustion attack whereby possible keys are tested one at a time until the correct key is found. Because of this, NIST proposed to replace FIPS 46–2 with FIPS 46–3 to specify use of Triple DES. Triple DES was documented and specified as an American National Standard (ANSI X9.52) by Accredited Standards Committee X9 for Financial Services, which develops cryptography and public key infrastructure standards. Triple DES was developed by the private sector with NIST assistance and is used by many government and private sector organizations, particularly in the financial services industry.

Public comments were solicited on the draft of FIPS 46–3 in the **Federal Register** (January 15, 1999, Volume 64, Number 10, pp. 2625–2628). The draft standard was also made available on NIST's web page. NIST received comments from three industry organizations and individuals and one Canadian government organization. The comments supported revision of the standard; minor technical and editorial changes were recommended and have been incorporated into FIPS 46–3.

Related to FIPS 46–3 is NIST's project to develop an Advanced Encryption Standard (AES), anticipated for completion in 2001. It is anticipated that Triple DES and the Advanced Encryption Standard (AES) will coexist as FIPS approved algorithms allowing for a gradual transition to AES. (The AES is a new symmetric-based encryption standard under development by NIST. AES is intended to provide strong cryptographic security for the protection of sensitive information well into the 21st century.) NIST is working with industry and the cryptographic community to develop the AES, which will offer improved security and efficiency over Triple DES, and provide needed cryptographic protection will into the next century. Information on the AES is available at <http://www.nist.gov/aes>.

Authority: This work effort is being conducted pursuant to NIST's responsibilities for the development of security standards and guidelines for the protection of sensitive federal information technology systems under the Computer Security Act of 1987, the Information Technology Management Reform Act of 1996, Executive Order 13011, and Appendix III to Office of Management and Budget (OMB) Circular A–130.

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 (Public Law 104–106), and Computer Security Act of 1987 (Public Law 100–235).

1. *Name of Standard.* Data Encryption Standard (DES).

2. *Catgegory of Standard.* Computer Security, Cryptography.

3. *Explanation.* The Data Encryption Standard (DES) specifies two FIPS approved cryptographic algorithms as required by FIPS 140–1. When used in conjunction with the American National Standards Institute (ANSI) X9.52 standard, this publication provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specify both enciphering and deciphering operations that are based on a binary number called a key.

A DES key consists of 64 binary digits (''0''s or ''1''s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, *i.e., t*here is an odd number of ''1''s in each 8-bit byte.[1] A TDEA key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force ''exhaustion attack.'' Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. A risk analysis should be performed under the direction of a responsible authority to determine potential threats. The costs of providing cryptographic protection using this standard as well as alternative methods of providing this protection and their respective costs should be projected. A responsible authority then should make a decision, based on these analyses, whether or not to use cryptographic protection and this standard.

4. *Approving Authority.* Secretary of Commerce.

5. *Maintenance Agency.* U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory.

6. *Applicability.* This standard may be used by Federal departments and agencies when the following conditions apply:

1. An authorized official or manager responsible for data security or the security of any computer system decides that cryptographic protection is required; and

2. The data is not classified according to the National Security Act of 1947, as amended, or the Atomic Energy Act of 1954, as amended.

Federal agencies or departments, which use cryptographic devices for protecting data classified according to either of these acts, can use those devices for protecting sensitive data in lieu of the standard.

Other FIPS approved crytographic algorithms may be used in addition to or in lieu of this standard when implemented in accordance with FIPS 140–1.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use in encouraged when it provides the desired security for commercial and private organizations.

[1] Sometimes keys are generated in an encrypted form. A random 64-bit number is generated and defined to be the cipher formed by the encryption of a key using a key encrypting key. In this case the parity bits of the encrypted key cannot be set until after the key is decrypted.

7. *Applications.* Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DES and TDEA [2] will be based on many factors particular to the computer system and its associated components. In general, crytography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period. FIPS 171 provides approved methods for managing the keys used by the algorithms specified in this standard. Public-key based protocols may also be used (*e.g.*, ANSI X9.42).

8. *Implementations.* Crytographic modules that implement this standard shall conform to the requirements of FIPS 140–1. The algorithms specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such at the application, the environment, the technology used, *etc.* Implementations which may comply with this standard include electronic devices (*e.g.*, VLSI chip packages), micro-processors using Read Only Memory (ROM), Programmable Read Only Memory (PROM), or Electronically Erasable Read Only Memory (EEROM), and mainframe computers using Random Access Memory (RAM). When an algorithm is implemented in software or firmware, the processor on which the algorithm runs must be specified as part of the validation process. Implementations of an algorithm that are tested and validated by NIST will be considered as complying with the standard. Note that FIPS 140–1 places additional requirements on crytographic modules for Government use. Information about devices that have been validated and procedures for testing and validating equipment for conformance with this standard and FIPS 140–1 are available from the National Institute of Standards and Technology, Information Technology Laboratory, 100 Bureau Dr. Stop 8930, Gaithersburg, MD 20899–8930.

9. *Export Control.* Cryptographic devices and technical data regarding them are subject to Federal Government export controls and exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce.

10. *Patents.* Cryptographic devices implementing this standard may be covered by U.S. and foreign patents, including patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus that complies with the standard. The terms, conditions and scope of the licenses are set out in notices published in the May 13, 1975, and August 31, 1976, issues of the Official Gazette of the United States Patent and Trademark Office (934 O.G. 452 and 949 O.G. 1717).

11. *Alternative Modes of Using the DES and TDEA.* FIPS PUB 81, DES Modes of Operation, describes four different modes for using DES described in this standard. These four modes are called the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode. ECB is a direct application of the DES algorithm to encrypt and decrypt data; CBC is an enhanced mode of ECB which chains together blocks of cipher text; CFB uses previously generated cipher text as input to the DES to generate pseudorandom outputs which are combined with the plain text to produce cipher, thereby chaining together the resulting cipher; OFB is identical to CFB except that the previous output of the DES is used as input in OFB while the previous cipher is used as imput in CFB. OFB does not chain the cipher.

The ANSI X9.52 standard, ''Triple Data Encryption Algorithm Modes of Operation'' describes seven different modes for using TDEA described in this standard. These seven modes are called the TDEA Electronic Codebook Mode of Operation (TECB) mode, the TDEA Cipher Block Chaining Mode of Operation (TCBC), the TDEA Cipher Block Chaining Mode of Operation—Interleaved (TCBC–I), the TDEA Cipher Feedback Mode of Operation (TCFB), the TDEA Cipher Feedback Mode of Operation—Pipelined (TCFB–P), the TDEA Output Feedback Mode of Operation (TOFB), and the TDEA Output Feedback Mode of Operation—Interleaved (TOFB–I). The TECB, TCBC, TCFB and TOBF modes are based upon the ECB, CBC, CFB and OFB modes, respectively, obtained by substituting the DES encryption/decryption operation with the TDEA encryption/decryption operation.

12. *Implementation of this standard.* FIPS 46–3 supersedes FIPS 46–2 on March 25, 2000. It applies to all Federal agencies, contractors of Federal agencies, or other organizations that process information (using a computer or telecommunications system) on behalf of the Federal Government to accomplish a Federal function. Each Federal agency or department may issues internal directives for the use of this standard by their operating units based on their data security requirement determinations.

a. Triple DES (*i.e.*, TDEA), as specified in ANSI X9.52, is recognized as a FIPS approved algorithm.

b. Triple DES is the FIPS approved symmetric encryption algorithm of choice.

c. Single DES (*i.e.*, DES) is permitted for legacy systems only. New procurements to support legacy systems should, where feasible, use Triple DES products running in the single DES configuration.

d. Government organizations with legacy DES systems are encouraged to transition to Triple DES based on a prudent strategy that matches the strength of the protective measures against the associated risk.

Note: It is anticipated that triple DES and the Advanced Encryption Standard (AES) will coexist as FIPS approved algorithms allowing for a gradual transition to AES. (The AES is a new symmetric-based encryption standard under development by NIST. AES is intended to provide strong cryptographic security for the protection of sensitive information well into the 21st century.)

NIST provides technical assistance to Federal agencies in implementing data encryption through the issuance of standards, guidelines and through individual reimbursable projects.

13. *Specifications.* Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES) (affixed).

14. *Cross Index.*

a. FIPS PUB 31, Guidelines to ADP Physical Security and Risk Management.

b. FIPS PUB 39, Glossary for Computer Systems Security.

c. FIPS PUB 73, Guidelines for Security of Computer Applications.

d. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.

e. FIPS PUB 81, DES Modes of Operation.

[2] DES forms the basis for TDEA.

f. FIPS PUB 87, Guidelines for ADP Contingency Planning.

g. FIPS PUB 112, Password Usage.

h. FIPS PUB 113, Computer Data Authentication.

i. FIPS PUB 140–1, Security Requirements for Cryptographic Modules.

j. FIPS PUB 171, Key Management Using ANSI X9.17.

k. ANSI X9.42, Agreement of Symmetric Keys on Using Discrete Logarithm Cryptography.©

l. ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.

15. *Qualifications.* Both this standard and possible threats reducing the security provided through the use of this standard will undergo review by NIST as appropriate, taking into account newly available technology. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NIST to reevaluate this standard and provide necessary revisions.

With regard to the use of single DES, exhaustion of the DES (*i.e.,* breaking a DES encrypted ciphertext by trying all possible keys) has become increasingly more feasible with technology advances. Following a recent hardware based DES key exhaustion attack, NIST can no longer support the use of single DES for many applications.

16. *Comments.* Comments and suggestions regarding this standard and its use are welcomed and should be addressed to the National Institute of Standards and Technology, Attn: Director, Information Technology Laboratory, 100 Bureau Dr., Stop 8900, Gaithersburg, MD 20899–8900.

17. *Waiver Procedure.* Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or

b. Compliance with a standard would cause a major adverse financial impact on the operator that is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision that explains the basis on which the agency head made the required finding(s). A copy of each decision, with procurement sensitive or classified portions clearly identified, shall be sent to National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the **Federal Register**.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any accompanying documents, with such deletions as the agency is authorized and decides to make under 5 United States Code Section 552(b), shall be part of the procurement documentation and retained by the agency.

18. *Special Information.* In accordance with the Qualifications Section of this standard, reviews of this standard have been conducted every 5 years since its adoption in 1977. The standard was reaffirmed during each of those reviews. This revision to the text of the standard contains changes which allow software implementations of the algorithm, permit the use of other FIPS approved cryptographic algorithms, and designate Triple DES (i.e., TDEA) as a FIPS approved cryptographic algorithm.

19. *Where to Obtain Copies of the Standard.* Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 46–3 (FIPSPUB46–3), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

Dated: October 29, 1999.

Karen H. Brown,

Deputy Director, NIST

[FR Doc. 99–28947 Filed 11–4–99; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 991101293–9293–01]

Public Meeting, Digital Divide Summit

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

ACTION: Notice.

SUMMARY: The Secretary of Commerce, William M. Daley, will host a Digital Divide Summit, focused on expanding access to new technologies for underserved populations and areas. Secretary Daley will lead the dialogue among participants from the U.S. Government, technology industry, civil rights and non-profit communities, grass-roots community organizations, and the general public.

DATES: The Digital Divide Summit will be held on December 9, 1999 from 8:00 a.m. to 1:00 p.m.

ADDRESSES: The Digital Divide Summit will be held at the U.S. Department of Commerce, Main Auditorium, 1401 Constitution Avenue, NW, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Jeffrey Joyner, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4713, Washington, D.C. 20230; telephone (202) 482–1816; facsimile (202) 501–8013; or electronic mail <digitaldivide@ntia.doc.gov>.

MEDIA INQUIRIES: Please contact the Office of Public Affairs, U.S. Department of Commerce, at (202) 482–7002.

SUPPLEMENTARY INFORMATION: Information tools, such as the personal computer and the Internet, are increasingly critical to economic success and personal advancement. On July 8, 1999, the National Telecommunications and Information Administration (NTIA) issued a report, Falling Through the Net: Defining the Digital Divide, that found a growing gap between those with access to these tools and those without. As information technology plays an ever-increasing role in Americans' economic and social lives, the prospect that some will be left behind in the information age can have