withdrawal of its request for an administrative review.

FOR FURTHER INFORMATION CONTACT: Constance Handley, Office of AD/CVD Enforcement, Group I, Import Administration, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230, telephone: (202) 482–0631.

SUPPLEMENTARY INFORMATION:

Background

On October 30, 1998, Cray Research, Inc., the petitioner, requested an administrative review of the antidumping duty order on vector supercomputers from Japan in accordance with 19 CFR 351.213(b). On November 30, 1998, in accordance with 19 CFR 351.221(c)(1)(i), we initiated an administrative review of this order for the period October 16, 1997, through September 30, 1998. On December 1, 1998, Cray Research, Inc., withdrew its request for this review.

Pursuant to 19 CFR 351.213(d)(1), the Department may allow a party that requests an administrative review to withdraw such request within 90 days of the date of publication of the notice of initiation of the requested review. Because Cray Research, Inc.'s request for termination was submitted within the 90-day time limit and there were no requests for review from other interested parties, we are rescinding this review. We will issue appropriate appraisement instructions directly to the U.S. Customs Service.

This determination is issued and published in accordance with section 751 of the Tariff Act of 1930, as amended (19 U.S.C. 1675), and 19 CFR 351.213(d)(4).

Dated: January 11, 1999.

Laurie Parkhill,

Acting Deputy Assistant Secretary for Import Administration.

[FR Doc. 99–999 Filed 1–14–99; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 981019262–8262–01]

RIN 0693–ZA27

Announcing Draft Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES), and Request for Comments

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

ACTION: Notice: request for comments.

SUMMARY: The Data Encryption Standard (DES) provides specifications for the Data Encryption Algorithm and is used by federal agencies (and others outside the government) for the protection of sensitive information. This standard, first issued in 1977, is reviewed every five years. The DES, currently specified in Federal Information Processing Standard (FIPS) 46–2, is due for review in December 1998. NIST is proposing to replace FIPS 46–2 with FIPS 46–3 to provide for the use of Triple DES as specified in the American National Standards Institute (ANSI) X9.52 standard. Comments are sought from industry, government agencies, and the public on the draft of FIPS 46–3.

DATES: Comments must be received on or before April 15, 1999.

ADDRESSES: Written comments concerning this standard should be sent to: Information Technology Laboratory, Attention: Review of Draft FIPS 46–3, National Institute of Standards and Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899–8970. Comments may also be sent via e-mail to ''desreview@nist.gov''.

Interested parties may order a copy of FIPS 46–2 from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161. Telephone (703) 487–1650. Copies of FIPS 46–2 and its proposed replacement (Draft FIPS 46–3) may also be downloaded from <http://csrc.nist.gov/fips>.

Ordering information for the ANSI X9.52 (Triple DES) standard is available from American Bankers Assoc./DC, X9 Customer Service Dept., PO Box 79064, Baltimore, MD 21279–0064, telephone 1–800–338–0626.

FOR FURTHER INFORMATION CONTACT: Mr. Miles Smid (301) 975–2938, 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, first issued in 1977, specifies the Data Encryption Algorithm for the cryptographic protection of computer data. The standard provided that it be reviewed within five (5) years to assess its adequacy. The first review was completed in 1983, and the standard was reaffirmed for Federal government use (48 FR 41062). The second review was completed in 1987, and was again reaffirmed for Federal government use (52 FR 7006) and 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). In addition to hardware implementations, FIPS 46–2 provided for software implementations of the DES. We are now proposing to replace FIPS 46–2 with FIPS 46–3 to also allow for the use of Triple DES as described in ANSI X9.52.

When DES was reaffirmed in 1993, NIST stated in the announcement that NIST would ''consider alternatives which offer a higher level of security'' at the next review in 1998. After the first exhaustion of a DES key, NIST advised Federal organizations that DES, properly used, still provided adequate security for many applications. At the time, NIST also stated that organizations needing security beyond that provided by the DES could use Triple DES as specified in ANSI X9.52. NIST worked with the financial community to develop this standard. Triple DES is a method for using the DES algorithm in three operations, developed by the private sector and used in many government and private sector organizations, particularly in the financial services industry. These operations have been 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. The American Bankers Association is the secretariat for X9. Ordering information for the X.52 standard is contained in the **ADDRESSES** section.

Additionally, knowing that the DES' security life was nearing an end, NIST has been working with industry and the cryptographic community to develop an Advanced Encryption Standard (AES) for the 21st century. On January 2, 1997, NIST announced the initiation of an effort to develop the AES (62 FR 93). It is intended that the AES will specify an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well in the next century. Unfortunately, since it takes a substantial amount of time to gain confidence in a new encryption algorithm, the AES is not expected to be a fully developed FIPS for some time to come. Information on NIST's multi-year effort to develop the AES can be obtained at <http://www.nist.gov/aes >.

Recently claims have been made of a special-purpose hardware based attack on the DES. In light of this most recent attack, NIST can no longer support the use of the DES for many applications. As with other security tools, encryption must balance cost against risk. The recent brute force exhaustion attack by a ''cracking machine'' costing $250,000 took 56 hours to crack a single message.

With this special-purpose technology, the average time of cracking per message would be twice that, since only a quarter of all keys were tested. In some cases this kind of attack may not pose an immediate or significant threat—for example where short-term protection of perishable information is desired. However, advances in technology are likely to further reduce the average cracking time. Therefore, NIST recommends the following:

—For existing systems, develop a prudent transition strategy to move to Triple DES. This strategy should match the strength of the protective measures against the associated risk. Critical systems should receive priority

—When building new systems, use Triple DES to protect sensitive, unclassified data

These recommendations are reflected in the proposed draft FIPS 46–3 (see below) by recognizing Triple DES, as described in ANSIX9.52, as a FIPS approved algorithm. Comments are sought on the proposed draft of FIPS 46–3.

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

DRAFT Federal Information Processing Standards Publication 46–3; 1999 (Approval Date) Announcing the Data Encryption Standard

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), and the Computer Security Act of 1987 (Pub. L. 100–235).

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

2. Category 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 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 specifies both enciphering and deciphering operations which are based on a binary number called a key.

A DEA key consists of 64 binary digits (''O''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., there is an odd number of ''1''s in each 8-bit byte [1]. A TDEA key consists of three DEA 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 cryptographic 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 is encouraged when it provides the desired security for commercial and private organizations.

7. Applications. Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DEA and TDEA will be based on many factors particular to the computer system and its associated components. In general, cryptography 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. DEA forms the basis for TDEA. 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.

[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.

Public-key based protocols may also be used (e.g., ANSI X9.42).

8. Implementations. Cryptographic modules which 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 as 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 which are tested and validated by NIST will be considered as complying with the standard. Note that FIPS 140–1 places additional requirements on cryptographic 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, Gaithersburg, MD 20899.

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 which 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 DEA and TDEA. FIPS PUB 81, DES Modes of Operation, describes four different modes for using DEA 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 plaintext 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 input in CFB. OFB does not chain the cipher.

The X9.52 standard, ''Triples 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–1). 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 DEA encryption/decryption operation with the TDEA encryption/decryption operation.

12. Implementation of this standard. This standard became effective July 1977. It was reaffirmed in 1983, 1988, 1993, and 1999 (if approved). 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 issue internal directives for the use of this standard by their operating units based on their data security requirement determinations.

With this modification of the FIPS 46–2 standard:

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

(2) Triple DES will be the FIPS approved symmetric encryption algorithm of choice.

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

(4) 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 coexit 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.

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 Diffie-Hellman and MQV Algorithms.

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 revaluate 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. Therefore, Government agencies with legacy single DES systems are encouraged to transition to Triple DES. Agencies are advised to implement Triple DES when building new systems.

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, Gaithersburg, MD 20899.

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 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 which 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 which 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 8970, Gaithersburg, MD 20899–8970.

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 an 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, review 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.

(Note that the technical specifications of the DES encryption algorithm are not reproduced in this **Federal Register** Notice. They are available in FIPS 46–2 and the draft of FIPS 46–3. No technical changes are being proposed in the DES algorithm itself from the specifications in FIPS 46–2.)

Triple Data Encryption Algorithm

Let $E_K(I)$ and $D_K(I)$ represent the DEA encryption and decryption of I using DEA key K respectively. Each TDEA encryption/decryption operation (as specified in ANSI X9.52) is a compound operation of DEA encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block) that is defined as follows: $O=E_{K3}(D_{K2}(E_{K1}(I)))$

2. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: $O = D_{K1}(E_{K2}(D_{K3}(I)))$

The standard species the following keying options for bundle (K_1, K_2, K_3)

1. Keying Option 1: K_1, K_2 and K_3 are independent keys;

2. Keying option 2: K_1 and K_2 and independent keys and $K_3 = K_1$;

3. Keying Option 3: $K_1 = K_2 = K_3$.

A TDEA mode of operation is backward compatible with its single DEA counterpart if, with compatible keying options for TDEA operation,

1. An encrypted plaintext computed using a single DEA mode of operation can be decrypted correctly by a corresponding TDEA mode of operation; and

2. An encrypted plaintext computed using a TDEA mode of operation can be decrypted correctly by a corresponding single DEA mode of operation.

When using keying Option 3 ($K_1 = K_2 = K_3$), TECB, TCBC, TCFB, amd TOFB modes are backward compatible with single DEA modes of operation ECB, CBC, CFB, OFB respectively.

The diagram in Appendix 2 illustrates TDEA encryption an TDEA decrytion.

(Note that the two appendices to FIPS 46–3 are not reproduced in this **Federal Register** notice. They are available in the complete draft of FIPS 46–3.)

Dated: January 8, 1999.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 99–898 Filed 1–14–99; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of Meeting of National Conference on Weights and Measures

AGENCY: National Institute of Standards and Technology.

ACTION: Notice of meeting.

SUMMARY: Notice is hereby given that the Interim Meeting of the National Conference on Weights and Measures will be held January 31 through February 4, 1999, at the Sheraton Old Town Hotel, Albuquerque, New Mexico. The meeting is open to the public.

The National Conference on Weights and Measures is an organization of weights and measures enforcement officials of the States, counties, and cities of the United States, and private sector representatives. The interim meeting of the conference, as well as the annual meeting to be held next July (a notice will be published in the **Federal Register** prior to such meeting), brings together enforcement officials, other government officials, and representatives of business, industry, trade associations, and consumer