

Deletion

I certify that the following action will not have a significant impact on a substantial number of small entities. The major factors considered for this certification were:

1. The action will not result in any additional reporting, recordkeeping or other compliance requirements for small entities.

2. The action will result in authorizing small entities to furnish the commodity to the Government.

3. There are no known regulatory alternatives which would accomplish the objectives of the Javits-Wagner-O'Day Act (41 U.S.C. 46-48c) in connection with the commodity proposed for deletion from the Procurement List.

The following commodity has been proposed for deletion from the Procurement List:

Pillowcase, Cotton/Cotton Polyester
7210-00-054-7910

Beverly L. Milkman,

Executive Director.

[FR Doc. 99-984 Filed 1-14-99; 8:45 am]

BILLING CODE 6353-01-P

COMMITTEE FOR PURCHASE FROM PEOPLE WHO ARE BLIND OR SEVERELY DISABLED

Procurement List; Additions and Deletions

AGENCY: Committee for Purchase From People Who Are Blind or Severely Disabled.

ACTION: Additions to and deletions from the Procurement List.

SUMMARY: This action adds to the Procurement List a commodity and services to be furnished by nonprofit agencies employing persons who are blind or have other severe disabilities, and deletes from the Procurement List commodities previously furnished by such agencies.

EFFECTIVE DATE: February 16, 1999.

ADDRESS: Committee for Purchase From People Who Are Blind or Severely Disabled, Crystal Gateway 3, Suite 310, 1215 Jefferson Davis Highway, Arlington, Virginia 22202-4302.

FOR FURTHER INFORMATION CONTACT: Beverly Milkman (703) 603-7740.

SUPPLEMENTARY INFORMATION: On November 16 and 30, 1998, the Committee for Purchase From People Who Are Blind or Severely Disabled published notices (63 F.R. 63670, 65746 and 65747) of proposed additions to and deletions from the Procurement List:

Additions

After consideration of the material presented to it concerning capability of qualified nonprofit agencies to provide the commodity and services and impact of the additions on the current or most recent contractors, the Committee has determined that the commodity and services listed below are suitable for procurement by the Federal Government under 41 U.S.C. 46-48c and 41 CFR 51-2.4.

I certify that the following action will not have a significant impact on a substantial number of small entities. The major factors considered for this certification were:

1. The action will not result in any additional reporting, recordkeeping or other compliance requirements for small entities other than the small organizations that will furnish the commodity and services to the Government.

2. The action will not have a severe economic impact on current contractors for the commodity and services.

3. The action will result in authorizing small entities to furnish the commodity and services to the Government.

4. There are no known regulatory alternatives which would accomplish the objectives of the Javits-Wagner-O'Day Act (41 U.S.C. 46-48c) in connection with the commodity and services proposed for addition to the Procurement List.

Accordingly, the following commodity and services are hereby added to the Procurement List:

Commodity

Jack, Scissors, Hand
5120-00-106-7598

Services

Commissary Shelf Stocking, Custodial and Warehousing, Naval Air Station, Key West, Florida

Commissary Shelf Stocking, Custodial and Warehousing, Fort Detrick, Maryland
Commissary Shelf Stocking, Custodial and Warehousing, Dahlgren Naval Surface Warfare Center, Dahlgren, Virginia
Commissary Shelf Stocking, Custodial and Warehousing, Fort McCoy, Wisconsin

This action does not affect current contracts awarded prior to the effective date of this addition or options that may be exercised under those contracts.

Deletions

I certify that the following action will not have a significant impact on a substantial number of small entities. The major factors considered for this certification were:

1. The action may result in any additional reporting, recordkeeping or

other compliance requirements for small entities.

2. The action will not have a severe economic impact on future contractors for the commodities.

3. The action may result in authorizing small entities to furnish the commodities to the Government.

4. There are no known regulatory alternatives which would accomplish the objectives of the Javits-Wagner-O'Day Act (41 U.S.C. 46-48c) in connection with the commodities deleted from the Procurement List.

After consideration of the relevant matter presented, the Committee has determined that the commodities listed below are no longer suitable for procurement by the Federal Government under 41 U.S.C. 46-48c and 41 CFR 51-2.4.

Accordingly, the following commodities are hereby deleted from the Procurement List:

Broom, Upright
7920-00-291-8305
7920-00-292-4371
7920-00-292-4372
7920-00-292-4375

Beverly L. Milkman,

Executive Director.

[FR Doc. 99-985 Filed 1-14-99; 8:45 am]

BILLING CODE 6353-01-P

DEPARTMENT OF COMMERCE

International Trade Administration

[A-588-841]

Vector Supercomputers From Japan: Notice of Recission of Antidumping Duty Administrative Review

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

ACTION: Notice of recission of antidumping duty administrative review.

EFFECTIVE DATE: January 15, 1999.

SUMMARY: On November 30, 1998, the Department of Commerce (the Department) published in the **Federal Register** (63 FR 65748) a notice announcing the initiation of an administrative review of the antidumping duty order on vector supercomputers, covering the period October 16, 1997, through September 30, 1998, and two manufacturers/exporters of the subject merchandise, Fujitsu Limited and NEC Corporation. The Department initiated this review based on a request from Cray Research, Inc. We are now rescinding this review as a result of Cray Research, Inc.'s

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 appraisal 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.