

**Authority:** Pub. L. 94-582, 90 Stat. 2867, as amended (7 U.S.C. 71 *et seq.*).

**James E. Link,**

*Administrator, Grain Inspection, Packers and Stockyards Administration.*

[FR Doc. E6-3501 Filed 3-10-06; 8:45 am]

**BILLING CODE 3410-EN-P**

## DEPARTMENT OF COMMERCE

### Foreign-Trade Zones Board

(Docket 8-2006)

#### Foreign-Trade Zone 202—Los Angeles, CA, Application for Subzone, Sharp Electronics Corporation, (Office and Consumer Electronics/Home Products/Solar Panels Distribution), Huntington Beach, California

An application has been submitted to the Foreign-Trade Zones Board (the Board) by the Board of Harbor Commissioners of the City of Los Angeles, grantee of FTZ 202, requesting special-purpose subzone status for the office and consumer electronics/home products/solar panels warehousing and distribution facility of Sharp Electronics Corporation (Sharp), in Huntington Beach, California. The application was submitted pursuant to the provisions of the Foreign-Trade Zones Act, as amended (19 U.S.C. 81a-81u), and the regulations of the Board (15 CFR part 400). It was formally filed on February 27, 2006.

The Sharp facility (939,800 sq. ft. of enclosed space on 23.4 acres) is located at 5901 Bolsa Avenue, Huntington Beach, California. The facility (97 employees) may be used under FTZ procedures for the testing, packaging, warehousing and distribution of consumer electronics/home products/solar panels. Sharp's application indicates that 5 percent of the merchandise handled at the facility is domestically-sourced and includes products manufactured at and transferred from Subzone No. 77A, Sharp Manufacturing Company of America's manufacturing facility in Memphis, Tennessee.

Zone procedures would exempt Sharp from Customs duty payments on foreign products that are re-exported. On domestic sales, the company would be able to defer payments until merchandise is shipped from the plant. The company would be able to avoid duty on foreign merchandise which becomes scrap/waste. Sharp also anticipates realizing significant logistical/procedural benefits. The application indicates that all of the above-cited savings from FTZ

procedures would help improve the facility's international competitiveness.

In accordance with the Board's regulations, a member of the FTZ Staff has been designated examiner to investigate the application and report to the Board.

Public comment is invited from interested parties. Submissions (original and 3 copies) shall be addressed to the Board's Executive Secretary at one of the following addresses:

1. *Submissions Via Express/Package Delivery Services:* Foreign-Trade-Zones Board, U.S. Department of Commerce, Franklin Court Building - Suite 4100W, 1099 14th St. NW, Washington, D.C. 20005; or
2. *Submissions Via the U.S. Postal Service:* Foreign-Trade-Zones Board, U.S. Department of Commerce, FCB - Suite 4100W, 1401 Constitution Ave. NW, Washington, D.C. 20230.

The closing period for their receipt is May 12, 2006. Rebuttal comments in response to material submitted during the foregoing period may be submitted during the subsequent 15-day period (to May 30, 2006).

A copy of the application and accompanying exhibits will be available for public inspection at the Office of the Foreign-Trade Zones Board's Executive Secretary at address Number 1 listed above, and at the U.S. Department of Commerce Export Assistance Center, 3300 Irvine Avenue, Suite 305, Newport Beach, CA 92660.

Dated: March 3, 2006.

**Dennis Puccinelli,**

*Executive Secretary.*

[FR Doc. E6-3535 Filed 3-10-06; 8:45 am]

**BILLING CODE 3510-DS-S**

## DEPARTMENT OF COMMERCE

### Foreign-Trade Zones Board

Order No. 1439

#### Approval of Manufacturing Authority—Subzone 61I, Shell Chemicals Yabucoa, Inc., (Oil Refinery), Yabucoa, Puerto Rico

Pursuant to its authority under the Foreign-Trade Zones Act of June 18, 1934, as amended (19 U.S.C. 81a-81u), the Foreign-Trade Zones Board (the Board) adopts the following Order:

*Whereas*, the Puerto Rico Trade and Exports Company, grantee of FTZ 61, has requested manufacturing authority on behalf of Shell Chemicals Yabucoa, Inc. (Shell), within Subzone 61I at the Shell refinery in Yabucoa, Puerto Rico (FTZ Docket 8-2005, filed 2/11/2005);

*Whereas*, notice inviting public comment has been given in the **Federal Register** (70 FR 9615, 2/28/2005);

*Whereas*, the Board adopts the findings and recommendations of the examiner's report, and finds that the requirements of the FTZ Act and Board's regulations would be satisfied, and that approval of the application would be in the public interest if approval is subject to the conditions listed below;

*Now, therefore*, the Board hereby orders:

The application for manufacturing authority under zone procedures within Subzone 61I, is approved, subject to the FTZ Act and the Board's regulations, including § 400.28, and subject to the following conditions:

1. Foreign status (19 CFR § 146.41, 146.42) products consumed as fuel for the petrochemical complex shall be subject to the applicable duty rate.
2. Privileged foreign status (19 CFR § 146.41) shall be elected on all foreign merchandise admitted to the subzone, except that non-privileged foreign (NPF) status (19 CFR § 146.42) may be elected on refinery inputs covered under HTSUS Subheadings #2709.00.10, #2709.00.20, #2710.11.25, #2710.11.45, #2710.19.05, #2710.19.10, #2710.19.45, #2710.91.00, #2710.99.05, #2710.99.10, #2710.99.16, #2710.99.21 and #2710.99.45 which are used in the production of:
  - petrochemical feedstocks (examiners report, Appendix "C");
  - products for export;
  - and, products eligible for entry under HTSUS # 9808.00.30 and # 9808.00.40 (U.S. Government purchases).

Signed at Washington, DC, this 28th day of February 2006.

**David M. Spooner,**

*Assistant Secretary of Commerce for Import Administration, Alternate Chairman, Foreign-Trade Zones Board.*

Attest:

**Dennis Puccinelli,**

*Executive Secretary.*

[FR Doc. E6-3536 Filed 3-10-06; 8:45 am]

**BILLING CODE 3510-DS-S**

## DEPARTMENT OF COMMERCE

### Bureau of Industry and Security

#### Action Affecting Export Privileges; Oriental Trading Corporation

*In the Matters of:* Oriental Trading Corporation, 1st Floor, Masco Plaza, Blue

Area, P.O. Box 2879, Islamabad, Pakistan, Respondent; *Order Renewing Temporary Denial Order as to Oriental Trading Corporation.*

Pursuant to Section 766.24 of the Export Administration Regulations (“EAR”), the Bureau of Industry and Security (“BIS”), U.S. Department of Commerce, through its Office of Export Enforcement (“OEE”), has requested that I renew for 180 days an Order temporarily denying export privileges of Oriental Trading Corporation, 1st Floor, Masco Plaza, Blue Area, P.O. Box 2879, Islamabad, Pakistan.

On March 8, 2005, the Acting Assistant Secretary of Commerce for Export Enforcement found that the Respondent<sup>1</sup> had conspired to undertake acts that violated the EAR, that such violations had been deliberate and covert, and that there was a strong likelihood of future violations, particularly given the nature of the transactions and the elaborate steps that had been taken by the Respondent to avoid detection by the U.S. Government while knowing that its actions were in violation of the EAR. 70 FR 12442 (Mar. 14, 2005). This finding was based on evidence presented by BIS that indicated that the Respondent had conspired with others, known and unknown, to cause items subject to the EAR to be illegally exported to Pakistan, that it caused exports of items controlled for nuclear non-proliferation reasons to Pakistan with knowledge that violations of the EAR would occur, and that it took actions intending to violate the EAR.

BIS continues to investigate this matter and believes that all of the facts found in the original Order continue to justify the renewal of the Order, especially given the nature of the transactions and the steps that have been taken by the Respondent to avoid detection by the U.S. Government while knowing its actions were in violation of the EAR. BIS believes evidence

described in the initial request for the Order supports this renewal.

Based on the evidence submitted by BIS, I find that renewal of the Order naming the Respondent is necessary, in the public interest, to prevent an imminent violation of the EAR. A copy of the request for renewal of this Order was served upon the Respondent in accordance with the requirements of 15 CFR 766.24 of the EAR, and no response was received in opposition to this request within the applicable time period described in that section.

*It is therefore ordered:*

First, that the Respondent, at the address listed above, and its successors and assigns and when acting on behalf of the Respondent, its officers, employees, agents or representatives, (collectively, the “Denied Persons”) may not, directly or indirectly, participate in any way in any transaction involving any commodity, software or technology (hereinafter collectively referred to as “item”) exported or to be exported from the United States that is subject to the Export Administration Regulations (“EAR”), or in any other activity subject to the EAR including, but not limited to:

A. Applying for, obtaining, or using any license, License Exception, or export control document;

B. Carrying on negotiations concerning, or ordering, buying, receiving, using, selling, delivering, storing, disposing of, forwarding, transporting, financing, or otherwise servicing in any way, any transaction involving any item exported or to be exported from the United States that is subject to the EAR, or in any other activity subject to the EAR; or

C. Benefitting in any way from any transaction involving any item exported or to be exported from the United States that is subject to the EAR, or in any other activity subject to the EAR.

Second, that no person may, directly or indirectly, do any of the following:

A. Export or reexport to or on behalf of the Denied Persons any item subject to the EAR;

B. Take any action that facilitates the acquisition or attempted acquisition by the Denied Person of the ownership, possession, or control of any item subject to the EAR that has been or will be exported from the United States, including financial or other support activities related to a transaction whereby the Denied Persons acquire or attempt to acquire such ownership, possession or control;

C. Take any action to acquire from or to facilitate the acquisition or attempted acquisition from the Denied Persons of

any item subject to the EAR that has been exported from the United States;

D. Obtain from the Denied Persons in the United States any item subject to the EAR with knowledge or reason to know that the item will be, or is intended to be, exported from the United States; or

E. Engage in any transaction to service any item subject to the EAR that has been or will be exported from the United States and which is owned, possessed or controlled by the Denied Persons, or service any item, of whatever origin, that is owned, possessed or controlled by the Denied Persons if such service involves the use of any item subject to the EAR that has been or will be exported from the United States. For purposes of this paragraph, servicing means installation, maintenance, repair, modification or testing.

Third, that after notice and opportunity for comment as provided in section 766.23 of the EAR, any other person, firm, corporation, or business organization related to the Respondent by affiliation, ownership, control, or position of responsibility in the conduct of trade or related services may also be made subject to the provisions of this Order.

Fourth, that this Order does not prohibit any export, reexport, or other transaction subject to the EAR where the only items involved that are subject to the EAR are the foreign-produced direct product of U.S.-origin technology.

In accordance with the provisions of Section 766.24(e) of the EAR, the Respondent may, at any time, appeal this Order by filing a full written statement in support of the appeal with the Office of the Administrative Law Judge, U.S. Coast Guard ALJ Docketing Center, 40 South Gay Street, Baltimore, Maryland 21202–4022.

In accordance with the provisions of Section 766.24(d) of the EAR, BIS may seek renewal of this Order by filing a written request not later than 20 days before the expiration date. The Respondent may oppose a request to renew this Order by filing a written submission with the Assistant Secretary for Export Enforcement, which must be received no later than seven days before the expiration date of the Order.

A copy of this Order shall be served on the Respondent, and shall be published in the **Federal Register**.

This Order is effective on March 10, 2006 and shall remain in effect for 180 days.

<sup>1</sup> The original order applied to Gold Technology Limited, Flat 23C, 97 High Street, Hong Kong; Hero Peak Limited, Flat C, Block 4, 11/F Golden Bldg, 145 Fuk Wa Street, Sham Shui Po, Kowloon, Hong Kong and Room D, 11/F, Fui Nam Building, 48–51 Connaught Road West, Hong Kong; Joanna Liu, Flat 23C, 97 High Street, Hong Kong; Portson Trading Limited, Room D, 8/F, 217–223 Tung Choi Street, Mongkok, Kowloon, Hong Kong and Room 709 Wing Shan Tower, 173 Des Voeux Road Central, Hong Kong, and Room 2208, 22/F, 118 Connaught Road West, Hong Kong; Sunford Trading Limited, Room 2208 22/F, 118 Connaught Road West, Hong Kong; and Zhenke International Trading Co. Ltd. Tianjin Port Free Trade Zone, Room 801, Gold Beauty Building No. 88, Haibain 8 Road, TPFTZ, Tianjin, Peoples Republic of China. The Office of Export Enforcement is not seeking to renew this temporary denial order against any party other than Oriental Trading Corporation.

Entered this 3rd day of March, 2006.

**Darryl W. Jackson,**

*Assistant Secretary of Commerce for Export Enforcement.*

[FR Doc. 06-2359 Filed 3-10-06; 8:45 am]

BILLING CODE 3510-DT-M

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

[Docket No. 051114299-5299-01]

#### Announcing Draft Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard (DSS), and Request for Comments

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

**ACTION:** Notice; Request for Comments.

**SUMMARY:** This notice announces Draft Federal Information Processing Standard 186-3, Digital Signature Standard, for public review and comment. The draft standard, designated "Draft FIPS 186-3," is proposed to revise and supersede FIPS 186-2.

FIPS 186, first published in 1994, specifies a digital signature algorithm (DSA) to generate and verify digital signatures. Later revisions (FIPS 186-1 and FIPS 186-2, adopted in 1998 and 1999, respectively) adopt two additional algorithms specified in American National Standards (ANS) X9.31 (Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)), and X9.62 (The Elliptic Curve Digital Signature Algorithm (ECDSA)).

The original DSA algorithm, as specified in FIPS 186, 186-1 and 186-2, allows key sizes of 512 to 1024 bits. With advances in technology, it is prudent to consider larger key sizes. Draft FIPS 186-3 allows the use of 1024, 2048 and 3072-bit keys. Other requirements have also been added concerning the use of ANS X9.31 and ANS X9.62. In addition, the use of the RSA algorithm as specified in Public Key Cryptography Standard (PKCS) #1 (RSA Cryptography Standard) is allowed.

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration is given to the needs and views of the public, users, the information technology industry, and Federal, State and local government organizations. The purpose of this notice is to solicit such views.

**DATES:** Comments must be received on or before June 12, 2006.

**ADDRESSES:** Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS 186-3, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

Electronic comments may also be sent to: [elaine.barker@nist.gov](mailto:elaine.barker@nist.gov).

The current FIPS 186-2 and its proposed replacement, Draft FIPS 186-3, are available electronically at <http://csrc.nist.gov/publications/fips/index.html> and <http://csrc.nist.gov/publications/drafts.html>, respectively. Comments received in response to this notice will be published electronically at <http://csrc.nist.gov/CryptoToolkit/tkdigsigs.html>.

**FOR FURTHER INFORMATION CONTACT:**

Elaine Barker, Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, telephone (301) 975-2911.

**SUPPLEMENTARY INFORMATION:** FIPS 186, Digital Signature Standard (DSS), first issued in 1994, specified a single technique for the generation and verification of digital signatures. FIPS 186-1 adopted a second technique that was approved as ANS X9.31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), by the American National Standards Institute (ANSI). FIPS 186-2 adopted a third technique that computed digital signatures using elliptic curve technology as specified in another ANSI standard, ANS X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

Digital signature algorithms require keys to generate secure signatures. With advances in technology, the size of these keys must be increased to provide adequate security. rDSA and ECDSA have been specified with sufficient flexibility to use various key sizes. DSA was specified for key sizes between 512 and 1024 bits. Key sizes below 1024 bits are currently not considered adequate. Therefore, the requirements for key sizes for DSA, as specified in FIPS 186-3, have been revised to include key sizes of 2048 and 3072 bits, in addition to the previously allowed 1024-bit key size. These key sizes provide security that is equivalent to the 80, 112 and 128-bit key sizes of symmetric key encryption algorithms such as TDEA (Triple Data Encryption Algorithm), as specified in NIST Special Publication 800-67, and AES (Advanced Encryption Standard), as specified in FIPS 197.

ANS X9.31, published in 1998, specifies the generation of keys and digital signatures for only an 80-bit

security level. Draft FIPS 186-3 specifies criteria for the generation of keys and digital signatures for additional security levels.

Many cryptographic applications use the RSA algorithm that was specified in PKCS #1 and that was developed by RSA Security. PKCS #1 is considered to provide adequate security for Federal Government applications. Therefore, in the interests of providing interoperability, Draft FIPS 186-3 allows implementations of PKCS #1 in addition to that of ANS X9.31 and specifies criteria for the generation of keys for PKCS #1 digital signature applications; no provision is currently provided in PKCS #1 for the generation of digital signature keys.

ANS X9.62 was published in 1998 and is currently under revision. Other requirements have been added in Draft FIPS 186-3 to address deficiencies present in the current ANS X9.62; these additional requirements are consistent with the proposed ANS X9.62 revision.

FIPS 186-2 included several methods for random number generation for the 80-bit security level. Draft FIPS 186-3 includes a new random number generator that can be used to provide random numbers at multiple security levels. This random number generator is based on the Approved hash functions specified in FIPS 180-2, Secure Hash Standard.

Draft FIPS 186-3 includes methods for the generation of domain parameters and digital signature keys. These methods are referenced by NIST Special Publication 800-56, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, for the generation of domain parameters and keys for key establishment.

Draft FIPS 186-3 requires that parties have various assurances when generating and verifying digital signatures. Methods for obtaining these assurances will be specified in a future publication to be issued in the NIST Special Publication (SP) series, SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications.

**Authority:** NIST's activities to develop computer security standards to protect Federal sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST in Section 5131 of the Information Technology Management Reform Act of 1996 (Pub. L. 104-106) and the Federal Information Security Management Act of 2002 (Pub. L. 107-347).

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