consumer goods products, and to share ideas on ways to strengthen this relationship.

Timetable

November 7—Arrive in Beijing (individual travel plans to be determined by participants); activities open.

November 8—Briefing for mission delegates with Beijing consultative staff. Delegation participants expect to meet with officials from the National Development and Reform Commission (NDRC), the Ministry of Commerce (MOFCOM), the Ministry of Information (MII), and the State Administration for Quality Supervision and Inspection and Quarantine (AQSIQ).

November 9 ''Delegation will continue meetings with officials from the aforementioned government agencies.

November 10—Mission delegation will depart for the United States, or other destinations.

V. Criteria for Participation

- Relevance of the company's business line to mission goals. Participants must be U.S. citizens representing U.S. manufacturing or service firms in the consumer goods industry (exclusive of automobiles, consumer electronics, computers and accessories, and cosmetics).
- Participating firms must be incorporated or otherwise organized under the laws of the United States, and demonstrate that they are at least 51 percent U.S.-owned.
- Representatives of participating firms must have experience in dealing with China trade policy issues on behalf of their firms.
- Potential for expanding business in the Chinese market.
- Minimum of 8 and maximum of 20 participating in the mission.
- Provision of adequate information on the company's products and/or services and communication of the company's primary objectives to facilitate appropriate matching with government officials.

Mission recruitment will be conducted in an open and public manner, including publication in the **Federal Register**, posting on the Commerce Department's trade missions calendar—*http://www.ita.doc.gov/doctm/tmcal.html*—and other Internet Web sites, press releases to the general and trade media, direct mail and broadcast fax, notices by industry trade associations and other multiplier groups, and at industry meetings, symposia, conferences, trade shows.

Recruitment for the mission will begin no later than July 2004 and conclude no later than September 10, 2004.

Participants in the Mission must agree to represent the interests of their firms only, and they may not represent the policies of the U.S. government.

Any partisan political activities (including political contributions) of an applicant are entirely irrelevant to the selection process.

Costs

$950 per participant. Budget breakdown available upon request.

Contacts Information: John Vanderwolf, Charlie Rast, U.S. Department of Commerce, International Trade Administration, Office of Consumer Goods, ITA/TD/TACGI/OCG, Room 3013, Fax: 202–482–1388, John Vanderwolf—Tel: 202–482–0348; E-mail: *john_vanderwolf@ita.doc.gov*, Charlie Rast—Tel: 202–482–4034; E-mail: *charlie_rast@ita.doc.gov*.

Dated: July 20, 2004.

Nancy Hesser,

Industry Sector Manager, Export Promotion Services.

[FR Doc. 04–16909 Filed 7–23–04; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 040602169–4169–01]

Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the 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), currently specified in Federal Information Processing Standard (FIPS) 46–3, was evaluated pursuant to its scheduled review. At the conclusion of this review, NIST determined that the strength of the DES algorithm is no longer sufficient to adequately protect Federal government information. As a result, NIST proposes to withdraw FIPS 46–3, and the associated FIPS 74 and FIPS 81.

Future use of DES by Federal agencies is to be permitted only as a component function of the Triple Data Encryption Algorithm (TDEA). TDEA may be used for the protection of Federal information; however, NIST encourages agencies to implement the faster and stronger algorithm specified by FIPS 197, Advanced Encryption Standard (AES) instead. NIST proposes issuing TDEA implementation guidance as a NIST Recommendation via its ''Special Publication'' series (rather than as a FIPS) as Special Publication 800–67, Recommendation for Implementation of the Triple Data Encryption Algorithm (TDEA).

DATES: Comments on the proposed withdrawal of DES must be received on or before September 9, 2004.

ADDRESSES: Official comments on the proposed withdrawal of DES may either be sent electronically to *DEScomments@nist.gov* or by regular mail to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Proposed Withdrawal of DES, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930.

FOR FURTHER INFORMATION CONTACT: Mr. William Barker (301) 975–8443, *wbarker@nist.gov,* National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

SUPPLEMENTARY INFORMATION: In 1977, the Federal government determined that, while the DES algorithm was adequate to protect against any practical attack for the anticipated 15-year life of the standard, DES would be reviewed for adequacy every five years. DES is now vulnerable to key exhaustion using massive, parallel computations.

The current Data Encryption Standard (FIPS 46–3) still permits the use of DES to protect Federal government information. Since the strength of the original DES algorithm is no longer sufficient to adequately protect Federal government information, it is necessary to withdraw the standard.

In addition, NIST proposes the simultaneous withdrawal of FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard and FIPS 81, DES Modes of Operation. FIPS 74 is an implementation guideline specific to the DES. An updated NIST Special Publication 800–21, Guideline for Implementing Cryptography in the Federal Government, will provide generic implementation and use guidance for NIST-approved block cipher algorithms (*e.g.*, TDEA and AES). Because it is DES-specific, and DES is being withdrawn, the simultaneous withdrawal of FIPS 74 is proposed.

FIPS 81 defines four modes of operation for the DES that have been used in a wide variety of applications. The modes specify how data is to be encrypted (cryptographically protected)

and decrypted (returned to original form) using DES. The modes included in FIPS 81 are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode. NIST Special Publication 800–38A, Recommendation for Block Cipher Modes of Operation, specifies modes of operation for generic block ciphers. Together with an upcoming message authentication code recommendation, SP 800–38B, SP 800–38A is a functional replacement for FIPS 81. FIPS 81 is DES-specific and is proposed for withdrawal along with FIPS 46–3 and FIPS 74.

NIST invites public comments on the proposed withdrawal of FIPS 46–3, FIPS 74 and FIPS 81. After the comment period closes, NIST will analyze the comments and make appropriate recommendations for action to the Secretary of Commerce.

Future use of FIPS 46–3 by Federal agencies is proposed to be permitted only as a component function of the Triple Data Encryption Algorithm or ''TDEA.'' TDEA encrypts each block three times with the DES algorithm, using either two or three different 56-bit keys. This approach yields effective key lengths of 112 or 168 bits. TDEA is considered a very strong algorithm. The original 56-bit DES algorithm can be modified to be interoperable with TDEA.

Though TDEA may be used for several more years to encourage widespread interoperability, NIST instead encourages agencies to implement the stronger and more efficient algorithm specified by FIPS 197, Advanced Encryption Standard (AES) when building new systems. TDEA implementation guidance will be issued as a NIST Recommendation rather than as a FIPS. NIST plans to issue TDEA as Special Publication 800–67, Recommendation for Implementation of the Triple Data Encryption Algorithm (TDEA).

Authority: 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 and the Federal Information Security Management Act of 2002, Public Law 107–347.

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

Dated: July 18, 2004.

Hratch Semerjian,

Acting Director, NIST.

[FR Doc. 04–16894 Filed 7–23–04; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 040709204–4204–01]

Opportunity for Public To View Fire Test of Floor System as Part of the Federal Building and Fire Safety Investigation of the World Trade Center Disaster

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Opportunity for public to view fire test of World Trade Center floor system.

SUMMARY: The National Institute of Standards and Technology announces the opportunity for the public to view the fire test of a floor system as part of the federal building and fire safety investigation of the World Trade Center disaster. The test will be conducted by Underwriters Laboratories, Northbrook, Illinois, on August 25, 2004.

DATES: The test is scheduled to be conducted on August 25, 2004, at Underwriters Laboratories in Northbrook, Illinois. A preliminary briefing will be given at 9 a.m., followed by a viewing of the test furnace and floor specimen. A conference room has been set up to view the test remotely, including video and temperature data. The test is scheduled to be completed by 5 p.m. Members of the public wishing to view the test will need to submit their request to attend by 5 p.m. e.d.t. on Wednesday, August 4, 2004, per the instructions under the **SUPPLEMENTARY INFORMATION** section of this notice. NIST will inform selected attendees if the test is re-scheduled for a later date.

ADDRESSES: The test will be conducted at the facilities of Underwriters Laboratories in Northbrook, Illinois. Requests to attend the test must be submitted to Mr. Stephen Cauffman, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8611, Gaithersburg, MD 20899–8611, or via e-mail (*WTC@NIST.gov*) or fax (301–975–4052).

FOR FURTHER INFORMATION CONTACT: Mr. Stephen Cauffman. Mr. Cauffman's e-mail address is *cauffman@nist.gov,* and his phone is 301–975–6051.

SUPPLEMENTARY INFORMATION: The National Institute of Standards and Technology (NIST) began its building and fire safety investigation of the World Trade Center (WTC) disaster in September 2002. This WTC Investigation, led by NIST, is conducted under the authority of the National Construction Safety Team Act (Pub. L. 107–231, codified at 15 U.S.C. 7301 *et seq.*).

Objectives of the WTC Investigation

The objectives of the NIST-led Investigation are to:

1. Determine why and how WTC 1 and WTC 2 collapsed following the initial impacts of the aircraft and why and how WTC 7 collapsed.

2. Determine why the injuries and fatalities were so high or low depending on location, including all technical aspects of fire protection, occupant behavior, evacuation, and emergency response.

3. Determine what procedures and practices were used in the design, construction, operation, and maintenance of WTC 1, 2, and 7.

4. Identify, as specifically as possible, areas in current building and fire codes, standards, and practices that warrant revision.

Resistance-to-Fire Testing

To aid in the analysis of the response of the WTC towers to fires, Underwriters Laboratories, under a contract from NIST, is carrying out fire endurance testing of a typical floor system and individual steel members under the fire conditions prescribed in the ASTM E119 standard test. There will be an opportunity for interested individuals to view the fire test scheduled to be conducted August 25, 2004, at Underwriters Laboratories in Northbrook, IL.

A preliminary briefing will be given at 9 a.m., followed by a viewing of the test furnace and floor specimen. A conference room has been set up to view the test remotely, including video and temperature data. The test is scheduled to be completed by 5 p.m. NIST will inform selected attendees if the test is re-scheduled for a later date.

Requests To Attend

Up to thirty people will be selected to attend the resistance-to-fire floor system test based upon the following factors:

- Balanced representation of a broad group of interests, including the engineering profession, public interest groups and families of victims, emergency responders, standards and code making organizations, and media outlets; and
- Time of receipt of request within each group.

To request an opportunity to attend, NIST must receive the following information via mail to Mr. Stephen Cauffman, National Institute of Standards and Technology, 100 Bureau