Dated: January 6, 2005.

Jeffrey Anspacher,

Director, Export Trading Company Affairs.

[FR Doc. E5–88 Filed 1–11–05; 8:45 am]

BILLING CODE 3510–DR–F

DEPARTMENT OF COMMERCE

International Trade Administration

AGENCY: International Trade Administration, U.S. Department of Commerce.

ACTION: Notice of invitation to energy industry event—Norwegian offshore opportunities forum.

DATE: March 3, 2005.

TIME: 8 a.m.

LOCATION: The Houstonian Hotel, Houston, Texas.

SUMMARY: As part of the U.S.-Norway Oil and Gas Industry Summit in Houston, the Royal Norwegian Ministry of Petroleum and Energy and the U.S. Department of Commerce are pleased to invite you, or a representative you designate from your company, to a breakfast briefing on opportunities on the Norwegian Continental Shelf (NCS). The briefing will provide offshore exploration and production companies with an overview of the resource potential and the framework conditions on the NCS.

Although Norway is the third largest oil exporter in the world, only about ¼ of the total estimated petroleum resources on the NCS have been produced. With the large quantities of petroleum that remain to be discovered, the NCS offers a variety of oil and gas opportunities in both established and frontier basins. Norway also has a well established and competitive petroleum industry, predictable and transparent framework conditions, and an approachable and skilled public administration.

8 a.m.—Breakfast.

8:15 a.m.—Welcome and Opening Remarks.

Ms. Thorild Widvey, Norwegian Minister of Petroleum and Energy Official from the U.S. Department of Commerce.

8:30 a.m.—The Resource Potential on the NCS.

Ms. Bente Nyland, Director, Norwegian Petroleum Directorate.

8:45 a.m.—The Framework Conditions on the NCS.

Mr. Gunnar Gjerde, Director General, Norwegian Ministry of Petroleum and Energy.

9:15 a.m.—Experiences of a U.S. Entrant to the NCS.

Steven B. Hinchman, Senior Vice President of Worldwide Production, Marathon Oil Corporation.

9:35 a.m.—Question and Answer Period.

9:55 a.m.—Closing Remarks.

Official from the U.S. Department of Commerce.

10 a.m.—Adjourn.

Please RSVP by February 18, 2005 to Patterson Brown, U.S. Department of Commerce, 202/482.4950, 202/482.0170 (fax), or *pbrown@ita.doc.gov;* or to Erik Just Olsen, Norwegian Ministry of Petroleum and Energy, +47 22 24 61 94 or *erik-just.olsen@oed.dep.no.*

Dated: January 6, 2004.

Patterson W. Brown,

International Trade Specialist, Office of Energy and Environmental Industries.

[FR Doc. E5–71 Filed 1–11–05; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 041217352–4352–01]

Announcing Development of Federal Information Processing Standard (FIPS) 140–3, a Revision of FIPS 140–2, Security Requirements for Cryptographic Modules

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology announces that it plans to develop Federal Information Processing Standard (FIPS) 140–3, which will supersede FIPS 140–2, Security Requirements for Cryptographic Modules. FIPS 140–2, approved by the Secretary of Commerce and announced in the **Federal Register** (June 27, 2001, Volume 66, Number 124, Pages 34154–34155), identifies requirements for four levels of security for cryptographic modules that are utilized by Federal agencies to protect the security of Federal information systems. The Federal Information Security Management Act (FISMA) (Public Law 107–347) requires that all Federal agencies and their contractors use only those cryptographic-based security systems that were validated to FIPS 140–2 or to its predecessor, FIPS 140–1.

DATES: Comments on new and revised requirements for FIPS 140–3 must be received on or before Febrary 28, 2005.

ADDRESSES: Comments may be sent electronically to *FIPS140–3@nist.gov,* or may be mailed to Information Technology Laboratory, ATTN: Development of FIPS 140–3, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930. All comments received will be available on the NIST Web site at: *http://csrc.nist.gov/cryptval/*

FOR FURTHER INFORMATION CONTACT: Mr. Allen Roginsky (301) 975–3603, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930. E-mail: *allen.roginsky@nist.gov.*

A copy of FIPS 140–2 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/fips/index.html.*

SUPPLEMENTARY INFORMATION: FIPS 140–2, Security Requirements for Cryptographic Modules, superseded FIPS 140–1, which had been issued in 1994. FIPS 140–1 specified that the standard be reviewed within five years to consider its continued usefulness and to determine whether new or revised requirements should be added. NIST conducted a review of FIPS 140–1 in 1998–99, and the standard was reaffirmed as FIPS 140–2 in 2001 with technical modifications to address technological advances that had occurred since FIPS 140–1 had been issued.

FIPS 140–2 identifies requirements for four increasing, qualitative levels of security for cryptographic modules. The four security levels cover a wide range of potential applications and a wide spectrum of information types, including data with the potential to cause low, moderate and serious impacts on organizations should there be a loss of confidentiality, integrity or availability of the data. In 1995, NIST and the Communications Security Establishment (CSE) of the Government of Canada established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to FIPS 140–1 and other cryptography-based standards. Nearly 500 cryptographic modules and many implementations of cryptographic algorithms have been tested by National Voluntary Laboratory Accreditation Program (NVLAP) accredited, independent third-party laboratories and have been validated. Products validated by this program are used in Canada, the U.S., and many other countries. Federal government agencies are required to acquire products that have been validated under the CMVP when they use cryptographic-based security systems to protect their information. The CMVP enables vendors of cryptographic products to use a common standard and a common testing