Notification to Interested Parties

This notice serves as a preliminary reminder to importers of their responsibility under 19 CFR 351.402(f)(2) to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in the Secretary's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

We are issuing and publishing this determination in accordance with sections section 751(a)(1) and 777(i)(1) of the Act.

Dated: December 30, 2004.

Joseph A. Spetrini,

Acting Assistant Secretary for Import Administration.

[FR Doc. 05–604 Filed 1–11–05; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

International Trade Administration

Export Trade Certificate of Review

ACTION: Notice of issuance of an Export Trade Certificate of Review, Application No. 04–00004.

SUMMARY: The Department of Commerce has issued an Export Trade Certificate of Review to AmRus Ventures, Inc. (''AMRUS''). This notice summarizes the conduct for which certification has been granted.

FOR FURTHER INFORMATION CONTACT: Jeffrey Anspacher, Director, Export Trading Company Affairs, International Trade Administration, by telephone at (202) 482–5131 (this is not a toll-free number), or by e-mail at *oetca@ita.doc.gov.*

SUPPLEMENTARY INFORMATION: Title III of the Export Trading Company Act of 1982 (15 U.S.C. 400l-21) authorizes the Secretary of Commerce to issue Export Trade Certificates of Review. The regulations implementing Title III are found at 15 CFR part 325 (2004).

Export Trading Company Affairs is issuing this notice pursuant to 15 CFR 325.6(b), which requires the Department of Commerce to publish a summary of the Certificate in the **Federal Register**.Under Section 305 (a) of the Act and 15 CFR 325.ll(a), any person aggrieved by the Secretary's determination may, within 30 days of the date of this notice, bring an action in any appropriate district court of the United States to set aside the determination on the ground that the determination is erroneous.

Description of Certified Conduct:

I. Export Trade

A. Products

All products.

B. Services

All services.

C. Technology Rights

Technology Rights, including, but not limited to, patents, trademarks, copyrights, and trade secrets that relate to Products and Services.

D. Export Trade Facilitation Services (as they Relate to the Export of Products, Services, and Technology Rights)

Export Trade Facilitation Services, including, but not limited to, professional services and assistance relating to: government relations; state and federal export programs; foreign trade and business protocol; consulting; market research and analysis; collection of information on trade opportunities; marketing; negotiations; joint ventures; shipping and export management; export licensing; advertising; documentation and services related to compliance with customs requirements; insurance and financing; trade show exhibitions; organizational development; management and labor strategies; transfer of technology; transportation services; and the formation of shippers' associations.

II. Export Markets

The Export Markets include all parts of the world except the United States (the fifty states of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the Trust Territory of the Pacific Islands).

III. Export Trade Activities and Methods of Operation

AMRUS may:

1. Provide and/or arrange for the provision of Export Trade Facilitation Services;
2. Engage in promotional and marketing activities and collect information on trade opportunities in the Export Markets and distribute such information to clients;
3. Enter into exclusive and/or non-exclusive licensing and/or sales agreements with Suppliers for the export of Products, Services, and/or Technology Rights in Export Markets;
4. Enter into exclusive or non-exclusive agreements with distributors and/or sales representatives in Export Markets;
5. Allocate export sales or divide Export Markets among Suppliers for the sale and/or licensing of Products, Services, and/or Technology Rights;
6. Allocate export orders among Suppliers;
7. Establish the price of Products, Services, and/or Technology Rights for sale and/or licensing in Export Markets;
8. Negotiate, enter into, and/or manage licensing agreements for the export of Technology Rights;
9. Enter into contracts for shipping; and
10. Exchange information on a one-to-one basis with individual Suppliers regarding inventories and near-term production schedules for the purpose of determining the availability of Products for export and coordinating export with distributors.

IV. Terms and Conditions of Certificate

1. In engaging in Export Trade Activities and Methods of Operation, AMRUS will not intentionally disclose, directly or indirectly, to any Supplier any information about any other Supplier's costs, production, capacity, inventories, domestic prices, domestic sales, or U.S. business plans, strategies, or methods that is not already generally available to the trade or public.
2. AMRUS will comply with requests made by the Secretary of Commerce on behalf of the Secretary of Commerce or the Attorney General for information or documents relevant to conduct under the Certificate. The Secretary of Commerce will request such information or documents when either the Attorney General or the Secretary of Commerce believes that the information or documents are required to determine that the Export Trade, Export Trade Activities, and Methods of Operation of a person protected by this Certificate of Review continue to comply with the standards of Section 303(a) of the Act.

V. Members

AMRUS has named no members (other than itself as Applicant) that are seeking protection under the Export Trade Certificate of Review.

VI. Definitions

1. ''Supplier'' means a person who produces, provides, or sells Products, Services and/or Technology Rights.

A copy of this certificate will be kept in the International Trade Administration's Freedom of Information Records Inspection Facility, Room 4001, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW., Washington, DC 20230.

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