

an Export Market or Markets, or to distributors, buyers and/or sales representatives who directly or indirectly market or sell to an Export Market or Markets;

15. Sell, or offer to sell Products at different prices for direct or indirect sale to an Export Market or Markets as compared to prices for direct or indirect sale to domestic markets; and

16. Affix labels or other forms of identification to Products which identify the Products and indicate whether such Products are for direct or indirect sale only in an Export Market or Markets.

Terms and Conditions of Certificate

1. In engaging in Export Trade Activities and Methods of Operation, DecoArt, Inc. 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. DecoArt, Inc. 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.

Definitions

1. "Export Intermediary" means a person who acts as a distributor, sales representative, sales or marketing agent, or broker, or who performs similar functions including providing or arranging for the provision of Export Trade Facilitation Services.

2. "Supplier" means a person who produces, provides, or sells any Product and/or a Service.

A copy of this Certificate will be kept in the International Trade Administration's Freedom of Information Records Inspection Facility Room 4102, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230.

Dated: June 30, 1999.

Morton Schnabel,

Director, Office of Export Trading Company Affairs.

[FR Doc. 99-17103 Filed 7-6-99; 8:45 am]

BILLING CODE 3510-DR-P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 990608155-9155-01]

RIN 0693-ZA31]

Technical Advisory Committee Report: Requirements for Key Recovery Products

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

ACTION: Notice; request for comments.

SUMMARY: The Department of Commerce seeks public comment on "Requirements for Key Recovery Product," encompassing technical recommendations prepared by the "Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure." The Committee was established by the Department to provide technical advice on an encryption key recovery standard for use by Federal agencies to provide for the continued government access to encrypted information in the event of the unavailability (e.g., loss due to unavailability of critical personnel) of the encryption/decryption key(s). The Committee held its final meeting in November, 1998, and subsequently delivered its work to the Secretary of Commerce. Notwithstanding the availability of opportunities for public input to the Committee's activities, the Committee's technical report and significance makes them worthy of additional public discussion and comment. Comments are also sought as to actions that the Department may wish to take as it contemplates using this report as the basis for a Federal key recovery standard.

DATES: Comments should be submitted no later than November 4, 1999.

REPORT AVAILABILITY AND ADDRESSES:

The report is available electronically from the Committee's homepage at <<http://csrc.nist.gov/tacdifipsfkm/>>. Electronic comments on the report may be sent to Key-recovery@nist.gov.

A hard copy of the report is available by request from NIST, Information Technology Laboratory, Attention: Review of Key Recovery Committee Report, 100 Bureau Drive, Stop 8930,

Gaithersburg, MD 20899-8930. Written comments may also be sent to this address.

FOR FURTHER INFORMATION CONTACT:

Edward Roback, Executive Secretary, Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, telephone 301-975-3696.

SUPPLEMENTARY INFORMATION:

The "Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure" was chartered by the Department of Commerce in 1996 to seek industry recommendations on technical specifications for accomplishing the recovery of keys used for encryption (as opposed to keys used solely for digital signatures, which should not be recoverable, since a new signature key pair is normally created in event of loss). The Committee was comprised of 24 members drawn from the private sector with expertise in computer systems, telecommunications, banking, security, research and other pertinent areas. Its activities were augmented by liaisons from various Federal agencies, who provided input and perspective to the Committee as to the security and functional key recovery requirements of Federal agencies. Twelve meetings of the Committee were held between December 1996 and November 1998. The progress that the Committee made on various drafts of its report may be seen on the Committee's electronic homepage at <<http://csrc.nist.gov/tacdifipsfkm/>>.

In June 1998, the Committee delivered an interim work product to the Secretary, requested additional time to complete its work, and suggested that work on detailed implementation guidance be initiated, noting that such guidance will be essential to the successful deployment of any key recovery system (since many aspects of key recovery system security [e.g., integration of key recovery products into an application/operational system or usage policy] were outside the scope of the Committee's work). The Committee also urged pursuit of conformance testing based upon the model employed for Federal Information Processing Standard (FIPS) 140.1, Security of Cryptographic Modules. In response to the request for additional time, the Department extended the charter of the Committee through the end of 1998 and urged the Committee to use the remaining time to complete its review of the document,

resolve inconsistencies and address any remaining issues.

Because this technical input was requested in anticipation of developing a FIPS on key recovery, the format of the Committee's report parallels that of a FIPS. However, since the Committee was chartered only to address technical issues, some areas (e.g., "applicability" and "waiver process") contained in a FIPS were not addressed by the Committee. The Committee noted in their draft that text for these sections would have to be supplied at a later date by the government.

In delivering its report to the Secretary, the Committee noted that its members did not "have time to verify the consistency and completeness of the document as a whole" and stated that these are crucial. Therefore, the submission of public comments on the consistency and completeness of the document is particularly encouraged.

The Committee's report is divided into two major sections, an "announcement section" and a "specifications section." The first section is fairly pro forma and contains, among other items, a brief explanation of the document, an index, list of appropriate applications, notes on implementations, and a glossary. Qualifications on the use of conforming products are also discussed. The second section contains the detailed specifications of the document and is divided into four chapters: (1) Overview, (2) Key Recovery Model, (3) Security Requirements, and (4) Assurance Requirement. Four appendices are included: (A) Key Recovery Technique (B) Examples, (C) Key Recovery Block, and (D) Certificate Extensions.

The key recovery model utilized by the Committee throughout its document describes five key recovery functions: (1) Key Recovery Information Generation, (2) Key Recovery Information Delivery, (3) Function Key Recovery Information Validation, (4) Key Recovery Requestor and (5) Key Recovery Agent. For each of these functions, one or more security levels is defined and functional and security requirements provided. For each security level(s) of a function, a corresponding assurance level is then specified with appropriate requirements.

Dated: June 30, 1999.

Karen H. Brown,
Deputy Director.

[FR Doc. 99-17234 Filed 7-6-99; 8:45 am]

BILLING CODE 3510-CN-M

DEPARTMENT OF DEFENSE

Department of the Navy

Public Hearings for Draft Environmental Impact Statement (DEIS) for the Introduction of the V-22 to the Second Marine Aircraft Wing

AGENCY: Department of the Navy, DOD.

ACTION: Notice of public hearing.

SUMMARY: The Department of the Navy, United States Marine Corps has prepared and filed with the U.S. Environmental Protection Agency a Draft Environmental Impact Statement (DEIS) to evaluate the introduction of the V-22 aircraft to the Second Marine Aircraft Wing in eastern North Carolina. In accordance with the National Environmental Policy Act (NEPA) and the Council on Environmental Quality regulations, this notice announces the dates and locations of public hearings for the DEIS.

DATES: Comments must be postmarked by August 9, 1999.

The meeting dates are:

1. July 19, 1999, 3:00p.m. to 8:00p.m., Jacksonville, NC.
2. July 20, 1999, 3:00p.m. to 8:00p.m., Havelock, NC.
3. July 21, 1999, 3:00p.m. to 8:00p.m., Atlantic, NC.
4. July 22, 1999, 3:00p.m. to 8:00p.m., Pollocksville, NC.

ADDRESSES: Address written comments to Commander, Atlantic Division, Naval Facilities Engineering Command, Attn: Mr. James Haluska (Code 2033JH), 1510 Gilbert Street, Norfolk, Virginia 23511; Fax: (757) 322-4894.

The meeting locations are:

1. Jacksonville, NC—Jacksonville City Hall, Meeting Room A, 211 Johnson Boulevard, Jacksonville, NC;
2. Havelock, NC—Havelock City Hall, 1 Hatteras Avenue, Havelock, NC;
3. Atlantic, NC—Marine Corps Outlying Landing Field Atlantic, Building 7017, Administration & Housing, Airfield Road, Atlantic, NC;
4. Pollocksville, NC—Pollocksville Elementary School, 300 Trent Street, Pollocksville, NC.

FOR FURTHER INFORMATION CONTACT:

Additional information concerning this notice may be obtained by contacting Mr. James Haluska, (757) 322-4889 or Lt. Col. Blackiston, Community Plans and Liaison Officer, MCAS Cherry Point, (919) 466-4196.

SUPPLEMENTARY INFORMATION: Pursuant to Section 102(2) of the National Environmental Policy Act (NEPA) of 1969 as implemented by the Council on Environmental Quality regulations (40

CFR 1500-1508), the Department of the Navy, United States Marine Corps has prepared a Draft Environmental Impact Statement (DEIS) to assess the potential environmental effects of introducing the V-22 "Osprey," a new type of tiltrotor aircraft, to the Second Marine Aircraft Wing (2d MAW) which operates from several Marine Corps air stations located along the East Coast of the United States. The DEIS has been distributed to various Federal, state, and local agencies, as well as other interested individuals and organizations. In addition, copies of the DEIS have been distributed to the following libraries for public review: Carteret County Public Library, 210 Turner Street, Beaufort, NC; Craven-Pamlico-Carteret Regional Library, 400 Johnson Street, New Bern, NC; Godwin Memorial Library, College Street, New Bern, NC; Havelock-Craven County Public Library, 300 Miller Boulevard, Havelock, NC; Onslow County Public Library, 58 Doris Avenue East, Jacksonville, NC; and Pamlico County Library, Bayboro, NC. A limited number of single copies of the DEIS are available upon request by contacting Mr. James Haluska at (757) 322-4889.

The introduction of the V-22 to the 2d MAW is part of a Corps-wide process of replacing two existing weapons systems, the CH-46E and CH-53D medium-lift helicopters currently used by the USMC MAWs, with a new weapon system. The USMC relies on a veteran fleet of CH-46Es and CH-53Ds for medium-lift operations, such as the delivery of troops and equipment in amphibious assault operations. These aircraft are nearing the end of their lifecycle, cannot travel great distances, and are not well equipped for night or adverse weather operations. The V-22 is capable of vertical/short takeoffs and landings, significantly greater flight distances at a faster speed, and with a greater payload than the helicopters it would replace. The proposed action, therefore, is to replace the CH-46 assets of the 2d MAW with the V-22 on a one-to-one basis. (Currently, the 2d MAW has no CH-53D assets. These are all located in MCB Hawaii.) Replacement of a weapons system such as the CH-46 involves more than just a substitution of a new system for an old one. It includes replacement or renovation of the facilities used to house and maintain the system. It also includes development within the USMC of the skills needed to employ the new weapons system during wartime.

The CH-46E aircraft are near the end of their operating life. The USMC must continue to have the capability of supporting combat forces, by lifting personnel and equipment into and out