DEFENSE SECURITY COOPERATION AGENCY
201 12TH STREET SOUTH, STE 203
ARLINGTON, VA 22202-5408

AUG 1 1 2009

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Communications Security (COMSEC) Equipment and Embedded Cryptographic Modules (DSCA Policy 09-36) [SAMM E-Change 141]

This memorandum updates the Security Assistance Management Manual (SAMM) by providing additional information regarding the required procedures for the release and approval to offer COMSEC equipment and embedded cryptographic modules. Chapter 3, paragraph C3.3.6. and Chapter 4, paragraph C4.3.4. of the SAMM are updated as attached.

This change will be included in the automated version of the SAMM found on the DSCA Web Page as SAMM E-Change 141. If you have any questions concerning this policy, please contact Mr. Kent Bell, DSCA/STR-POL, at 703-604-6612 or e-mail: kent.bell@dsca.mil.

Scott R. Schless
Principal Director
Strategy

Attachment:
As Stated

Security Assistance Management Manual (SAMM), E-Change 141

1. Delete references (an) and (ao) from the reference list.

2. Chapter 3, paragraph C3.3.6. has been replaced in its entirety as follows:

C3.3.6. INFOSEC LOAs. The Director, National Security Agency, (DIRNSA) is the National Manager for INFOSEC products to include both external Communications Security (COMSEC) equipment and embedded cryptographic modules. The Implementing Agency for COMSEC and embedded cryptographic modules is determined by the Acquisition Manager of a particular device. DIRNSA may allow some NSA managed INFOSEC materiel to be included on other Implementing Agency managed LOAs due to urgent operational requirements, end of fiscal year funding issues, etc. Requests for exceptions to allow NSA-managed INFOSEC materiel on other Implementing Agency LOAs will not be granted due to the lack of an existing NSA LOA or to avoid the Small Case Management Line. Special Purpose INFOSEC equipment ("S" Type COMSEC) shall be provided to Non-NATO Nations on NSA-managed FMS cases only. Requests to allow "S" Type COMSEC equipment on other Implementing Agency LOAs will not be granted.

C3.3.6.1. INFOSEC Validation/Authorization. All Implementing Agencies must request DIRNSA determination as to whether INFOSEC equipment and embedded cryptographic modules are releasable, and whether the releasable equipment/modules can be included on an LOA written by an Implementing Agency other than NSA. DIRNSA authorization is required even when the Implementing Agency is responsible for the acquisition of the INFOSEC equipment and embedded cryptographic modules. Requests must include a copy of the purchaser's LOR, nomenclature of the INFOSEC and/or embedded cryptographic modules, quantities, and identify the weapon system or platform in which the INFOSEC equipment will be integrated. DIRNSA will provide a written response to the Implementing Agency within 30 days of the request. Some responses may include special instructions for INFOSEC materiel that requires special handling.

C3.3.6.2 Classification of INFOSEC. The association of a specific INFOSEC product with a foreign government may be classified; however, classifying the entire FMS case will be avoided, when possible. See Chapter 5, C5.4.11. for more information on classified FMS cases.

3. Chapter 4, paragraph C4.3.4. has been replaced in its entirety as follows:

C4.3.4. Communications Security (COMSEC) Equipment. Combatant Commanders' requirements to communicate with foreign governments via secure transmissions will necessitate a requirement for release and delivery of U.S. COMSEC. Transfer of U.S. COMSEC must be done in conjunction with a Combatant Command's interoperability requirement or otherwise support a U.S. policy objective. See Chapter 3, C3.3.1. and C3.3.2. for information on the technology transfer process. See Chapter 3, C3.3.6. for information on INFOSEC case processing.

4. Renumber current and subsequent sections as required to accommodate above changes.