UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

ASO 2280.1E
TISD
10 May 10

AIR STATION ORDER 2280.1E

From: Commanding Officer, Marine Corps Air Station, Cherry Point
To: Distribution List

Subj: SECURE TELEPHONE EQUIPMENT/KSV-21 CRYPTOGRAPHIC CARD MANAGEMENT PROCEDURES

Ref: (a) EKMS-1 (series)

1. Situation. Secure Telephone Equipment (STE) together with associated KSV-21 cryptographic cards are Communications Security (COMSEC) equipment used to protect U.S. Government transmissions of classified or sensitive unclassified information related to national security from unauthorized persons. The Electronic Key Management System (EKMS) has been established to distribute, control, and safeguard COMSEC equipment, and thus is the means for protection of vital and sensitive information moving over government communications systems.

2. Cancellation. AirStaO 2280.1D.

3. Mission. To promulgate specific guidance regarding the distribution, control, maintenance and protection of STE terminals and their associated KSV-21 cryptographic cards and assign responsibilities for their use, security, and accountability.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The protection of vital and sensitive information that moves over government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of military operations. This Order has been established to provide guidance regarding the secure distribution, control and safeguarding of STE terminals and their associated KSV-21 cryptographic cards.

(2) Concept of Operations

(a) The STE telephone is a terminal designed to serve as a standard telephone and as a secure communications terminal for sensitive unclassified and classified information up to and including TOP SECRET/Sensitive Compartmented Information (TS/SCI). New requirements for STE terminals must be submitted to the Telecommunications and Information Systems Directorate, Marine Corps Air Station Cherry Point (MCASCHERPT).

(b) Department of Defense (DoD) policy requires STE terminals with associated KSV-21 cards inserted be within reasonable proximity of potential STE users. Reasonable proximity is defined as within the office, area, room, space or other location where the potential user normally works with classified or sensitive unclassified information and routinely conducts telephone conversations related to that work. At a minimum, sensitive information includes all information which relates to operations, plans, intelligence, system acquisition, logistical support and personnel management.

b. Task

(1) MCASCHERPT TISD

(a) Will appoint an EKMS Manager per guidelines set forth in reference (a).

(b) Will appoint an EKMS Primary Alternate Manager and any additional Alternate Managers that may be required.

(2) EKMS Manager and Alternate EKMS Managers

(a) Receipt and account for STE terminals and KSV-21 cryptographic cards.

(b) Control issuance of STE terminals and associated KSV-21 cryptographic cards.

(c) Verify security clearance and access for all STE/KSV-21 users.

(d) Maintain STE/KSV-21 records and conduct inventories per reference (a).

(e) Coordinate the maintenance and repair of STE terminals.

(f) Provide training for the proper use, security, and care of each terminal to STE/KSV-21 users.

(g) Maintain physical custody of all KSV-21 Terminal Privilege Authority (TPA) cards.

(h) Ensure compliance with current directives for the storage, use and disposition of KSV-21 cryptographic cards.

(3) STE/KSV-21 Users. The STE/KSV-21 user is responsible for the proper use, care and security of the terminal and the associated KSV-21 cryptographic card as well as the security of the information transmitted via the terminal. The user's responsibilities are summarized as follows:

(a) STE/KSV-21 users must ensure that a terminal with the KSV-21 cryptographic card inserted is treated as classified material commensurate with the level of classification of the keys programmed in the card. Local controls must be instituted limiting access to the keyed terminal to those persons who have appropriate security clearance and need to know.

(b) KSV-21 cryptographic cards not inserted into their associated terminals are unclassified Controlled Cryptographic Items (CCI), requiring protection from unauthorized use with the terminal. Whenever authorized personnel are not present to protect a terminal with its card:

1. The card will be removed from the terminal and kept under the direct control of the authorized user.

2. Stored in a General Services Administration (GSA) approved container if the KSV-21 is kept in the vicinity of its associated STE terminal.

3. If not kept in the vicinity of its associated STE terminal, locked in an appropriate container per paragraph 535n of the reference which states, "Unkeyed CCI and/or CCI keyed with unclassified key marked or designated CRYPTO must be stored in a manner that affords protection against pilferage, theft, sabotage, or tampering, and ensures that access and accounting integrity are maintained."

(c) A STE/KSV-21 user must ensure prior to making a secure call that his immediate physical area is secure, e.g., that personnel in the immediate area have security clearances and a need to know commensurate with the level of the planned conversation. Personnel in outside offices should be isolated from the sensitive or classified conversations by appropriate physical barriers or supervision of cleared personnel.

(d) When operationally required, STE/KSV-21 users may permit others to use their terminals; however, the call must be placed by the STE/KSV-21 user. Once the call has been placed and before turning the hand receiver over to the other party, the STE/KSV-21 user must identify the party on whose behalf the call is being made, indicating their level of clearance.

(e) A STE terminal with its associated KSV-21 cryptographic card removed is unclassified. However, the STE terminal is sensitive, high value equipment requiring strict security controls and accountability.

(f) At least annually, STE/KSV-21 users will reassess their STE/KSV-21 requirements and turn-in any terminals that are no longer required to the EKMS Manager.

c. Coordinating Instructions

(1) Accountability. KSV-21 cryptographic cards are serialized and accountable to the Naval Communications Security Material System (NMCS) through the EKMS Manager. The EKMS Manager will be responsible for ensuring that STE and associated KSV-21 cryptographic cards are utilized, maintained and accounted for per reference (a).

(a) STE Terminals. Terminals may not be moved from their initial placement area without approval. Requests for moving STE terminals should be addressed to Director, TISD, MCASCHPT (Attn: EKMS Manager) and forwarded via the appropriate chain of command.

(b) KSV-21 Cryptographic Cards. The EKMS Manager and an Alternate Manager, when directed by NCMS, will inventory all KSV-21 cryptographic cards per reference (a).

(2) Emergency Protection Procedures. Emergency protection procedures dictate actions to be taken during emergencies to

prevent the unauthorized use of STE terminals and KSV-21 cryptographic cards.

(a) Local Elements will ensure that emergency action procedures for STE terminals and associated KSV-21 cryptographic cards are included in local emergency action plans.

(b) STE/KSV-21 users will be familiar with the actions to be taken during emergencies as directed by local authority.

(3) COMSEC Incidents. A COMSEC incident is any occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information. STE/KSV-21 users must immediately report all known or suspected COMSEC incidents to the EKMS Manager. The EKMS Manager will be responsible to ensure accurate and timely submission of COMSEC Incident Reports (CIRs) to the Director NSA, in accordance with procedures outlined in Chapter 9 of reference (a). The following are COMSEC incidents pertaining to the STE/KSV-21:

(a) Whenever the user identification or authentication information displayed during a secure call is not representative of the distant terminal. Authentication information includes:

1. Classification level authorized by the key for the particular terminal.

2. Authorization for access to sensitive compartmented information (SCI) when common to both terminals.

3. Identification of the using organization (e.g.; US Navy, US Marine Corps).

4. Foreign access to a keyed terminal, when approved (e.g., CANADA) identifies terminals supporting Canadian operations, (US/CAN) identifies terminals supporting US/CAN operations.

(b) Any instance in which the display indicates that the distant terminal contains compromised key.

(c) Known or suspected tampering of a KSV-21 card.

(d) Loss of a TPA card that has not yet been associated with a STE.

(e) Loss of a TPA card may impact local information security because a TPA card can be used to change the security settings of all the STEs under its control.

(f) Loss of a fill card.

(g) Loss of a card when the card can be identified with a particular secure voice or data terminal and it was not disassociated from its terminal.

(h) Loss of a user card with its associated STE or with its associated carry card.

(4) Practices Dangerous to Security (PDSs). PDSs, while not reportable to NSA, are practices which have the potential to jeopardize the security of COMSEC material if allowed to perpetuate. The following are non-reportable PDSs pertaining to the STE/KSV-21:

(a) Discovery of a tampered or unauthorized modification/repair of a STE. The STE is not a COMSEC device and this is not considered a COMSEC incident. However, the integrity of the STE must be verified prior to installation for operational use. Users must contact their EKMS Manager for specific guidance. The EKMS Manager will contact the STE program office at NSA for further assistance upon discovery of unauthorized repair or modification of a STE.

(b) Loss of a user card or carry card that has been associated with the STE is not a COMSEC incident. However, users are required to notify the EKMS Manager when a user card or carry card is lost so that its association with the STE can be removed at the earliest opportunity to prevent unauthorized access to the STE.

(5) STE Rekey. Rekey calls can be made at any time. However, rekey must be performed at least annually prior to the STE/KSV-21 key's expiration. The EKMS Central Facility will make the new STE/KSV-21 key available on the rekey server, usually within 60 days of the end of the annual cryptoperiod. Rekey is automatically performed by simply making a call to the rekey server while the KSV-21 cryptocard is inserted into the STE. Once

the rekey call is complete, the STE/KSV-21 user must verify that the key expiration date has been extended. The following are procedures for viewing the STE/KSV-21 key expiration date and performing rekey:

(a) Viewing the STE/KSV-21 key expiration date:

1. Press "Menu", terminal displays "Terminal Management".

2. Press "Scroll", terminal displays "Crypto Card Management".

3. Press "Select", terminal displays "Card Management Privileges."

4. Press "User", terminal displays "Rekey Functions".

5. Press "Scroll", terminal displays "View Card Key Data".

6. Press "Select", terminal displays "SDNS 1 Key Data - Key ID: XXXXXXX".

7. Press "Scroll" three times, terminal displays STE/KSV-21 key expiration date.

(b) Performing a STE Rekey:

1. Press "Menu", terminal displays "Terminal Management".

2. Press "Scroll", terminal displays "Crypto Card Management".

3. Press "Select", terminal displays "Card Management Privileges".

4. Press "User", terminal displays "Rekey Functions".

5. Press "Select", terminal displays "Update Rekey Phone Number/Perform Rekey".

6. Press "Rekey", terminal displays "Perform Rekey STU-III: NONE -- SDNS: OK".

7. Press "SDNS", terminal displays "SDNS Rekey Mode -- Select Type".

8. Press "SCIP", terminal displays "SDNS Rekey Mode SCIP -- Dial: 9918006333971."

9. Press "Go". The rekey server will be dialed. Note: If the rekey server is busy or if you are disconnected, repeat steps (b) 1 through 9.

10. The terminal displays "Going Secure To:" followed by "SECRET Rekey in Progress, Please Stand By". When the rekey call is complete, the terminal will display "SDNS Rekey Complete". Press "Continue".

11. If performing annual rekey, follow steps (a) 1 through 7 to verify that the key expiration date has been extended.

(6) Troubles and Repairs.

(a) Troubles or repairs involving processing of telephone calls on equipment will be handled by calling the Joint Help Desk at extension 114 for assistance.

(b) Difficulty with using a STE/KSV-21 in the secure mode should be addressed directly to the EKMS Manager for determination of further required action.

(c) If any terminal requires removal for repair, further action will be coordinated with the EKMS Manager. The terminal removed for repair will be reinstalled upon completion of repairs. A standard telephone will be installed, when requested from the Station Telephone Department, while the terminal is in the repair cycle. A replacement STE terminal may be installed, if available.

5. Administration and Logistics. The Commanding General, 2d MAW and tenant organization Commanding Officers concur with the contents of this Order insofar as it pertains to members of their command.

6. Command and Signal

a. Command. This Order is applicable to the Marines, Sailors, and Civilian employees aboard MCASCHERPT. The EKMS Manager and EKMS Alternate Managers are located in the TISD, building 4397.

b. Signal. This Order is effective the date signed.

ROBERT D. CLINTON
Executive Officer

DISTRIBUTION: A