



DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS, MARYLAND 21402-1300

USNAINST 2210.1B
6/Msg Br

20 SEP 2006

USNA INSTRUCTION 2210.1B

From: Superintendent

Subj: SECURE TELEPHONE UNIT VERSION III (STU-III) TYPE 1 TERMINAL

Ref: (a) EKMS-1

Encl: (1) STU III Local Custody Document

1. Purpose. To publish policy, guidance, and instructions concerning the use and security of the STU-III, Type 1 secure telephone as required by reference (a).

2. Cancellation. USNAINST 2210.1A

3. Background. Due to the unique capabilities of the STU-III, specific handling and operating instructions are required. This instruction establishes policy for the use and security of the STU-III. The STU-III is a "state-of-the-art" phone that has the added capability to operate in a secure mode for the discussion of classified information at all levels of classification.

4. Action. All U.S. Naval Academy (USNA) and contingent staff personnel who are/will be authorized STU-III users will familiarize themselves and comply with the contents of this instruction.

5. Definitions

a. Command Authority. The individual responsible for the appointment of user representatives for a department, agency, or organization and key ordering privileges. The command authority for USNA is the Message Branch.

b. Crypto Ignition Key (CIK). A storage device that contains information used to electronically lock and unlock a STU-III telephone's secure mode. The secure mode is usable when the CIK is inserted and disabled when it is removed. The CIK is unclassified when not inserted in a STU-III.

c. Authentication Information (Key ID). The information which identifies a STU-III telephone. Authentication information is specified for each STU-III key ordered and is embedded as part of the key. Each terminal's authentication information is displayed on the distant telephone during a secure call. Authentication information includes:

(1) Classification Level. The highest classification level authorized by the key for an individual STU-III. During a secure call, the clearance level displayed on each terminal is the highest level common to both terminals and is the authorized level for the call.

(2) Authorization for Access to Sensitive Compartmented Information (SCI). Compartments are displayed only when they are common to both terminals.

(3) Identification of the using organization or individual (e.g., "USNA ANNAPOLIS").

(4) A five digit KEY ID number.

(5) Expiration date of the terminal's key.

20 SEP 2006

d. Keyed Terminal. A keyed terminal is one in which the crypto has been loaded and the associated CIK is inserted. These terminals are classified based on the classification level of the filled crypto material.

e. Unkeyed Terminal. A terminal that contains no crypto or one which has been filled but the CIK is not inserted. These terminals are unclassified.

6. Physical Security

a. Keyed Terminal. When the terminal is keyed, it must be afforded protection commensurate with the classification of the key it contains. When personnel in an area are not cleared to the level of the keyed terminal, it must be under the operation control and within view of at least one appropriately cleared, authorized person.

b. Unkeyed Terminal. An unkeyed terminal should be provided the protection of any high value item (i.e., computer).

c. CIK Management. When authorized persons are not present, or when offices are vacated upon completion of working hours, the CIK must be removed from the terminal and properly protected. The CIK may be locked in an appropriate security container or kept in the possession of the authorized users(s). CIKs kept in the personal possession of authorized users should be treated as valuable personal property. The loss of a CIK must be reported immediately to the Message Branch, ext 31575. Master CIKs are only created by the Message Branch who will retain and store the Master CIK to preclude unauthorized creation of CIKs.

d. Terminal/CIK Chain of Custody. To provide a chain of custody, the user, upon receipt of the STU-III or CIK, will be required to sign enclosure (1). The custody document will be retained by the Message Branch. When the user is transferred or relieved, the user will notify the Message Branch. A new custody document will be issued by the Message Branch to reflect the custody change before the member departs.

7. User Responsibilities

a. Users must pay close attention to the authentication displayed on the terminal during each secure call. When two terminals communicate in the secure mode, each terminal automatically displays the highest classification level common to both terminals. The information displayed indicates the approved level for the call; however, it does not authenticate the person using the terminal. Therefore, users must use judgment in determining "need-to-know" when communicating classified information. The crypto period for the STU-III key is one year. The expiration date of a user's key is embedded in the authentication information and may be viewed by following instructions furnished in the STU-III user's manual. In the event of an expired key (STU-III will indicate "Key Expired" or "Call Key Management Center"), the crypto period can be extended an additional year by dialing the Electronic Key Management System (EKMS) at 1-800-635-6301. This process is user friendly and completely automated after connectivity with EKMS.

b. Classified information must not be transmitted whenever any of the following four conditions exist. Report condition to the Message Branch immediately; do not use the STU-III for secure communications until the condition has been cleared.

(1) If there are questions as to the validity of the authentication information on the display, even though voice recognition may be possible. Authentication information must be representative of the organization in which the distant terminal is located.

(2) When the display indicates that the distant terminal's key has expired.

(3) The display indicates that the distant terminal contains a compromised key.

20 SEP 2006

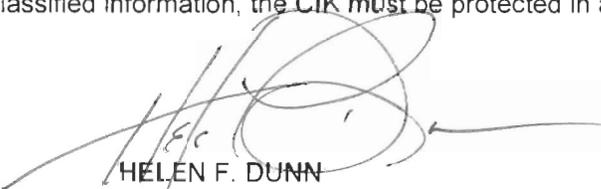
(4) If the display fails.

8. Authorization and Installation

a. Authorization to hold STU-III will be granted by the Message Branch.

b. Work Spaces. Installation will be accomplished by Message Branch personnel. Basic requirements for installation are the existing telephone connection (some exceptions exist) and the availability of 115-volt AC power from a standard three-prong wall outlet.

c. Personal Residences. If the requirements for secure voice in residences should arise, the head of the division concerned should submit a request through the Message Branch to be approved by the Deputy Superintendent/Chief of Staff, stating the requirement and justification. Any costs involved for installation must be borne by the requestor. No new telephone service should be required in the residence as the STU-III will work on any telephone line. A STU-III installed on the Naval Academy grounds in a residence, should be used only by the person for whom it was installed. All of the security requirements must be observed for preventing unauthorized access to the keyed terminal and to classified and sensitive information. The CIK must be removed from the terminal following each use and kept in the personal possession of the user or properly stored. If the CIK is stored in the residence and the associated terminal is used to protect classified information, the CIK must be protected in an approved security container.



HELEN F. DUNN

Deputy Superintendent/Chief of Staff

Distribution:

All Non-Mids (electronically)

STU III LOCAL CUSTODY DOCUMENT

Issue Date _____

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE

Any misuse or unauthorized disclosure can result in both civil and criminal penalties

Privacy Act Statement

Authority: 0 USN 5031, Executive Order 9397.
Purpose: To collect relevant information to issue COMSEC material.
Uses: Documentation will be held in a secure space for equipment accountability.
Disclosure: Not voluntary - Non disclosure may prevent processing of this document and result in denial of request. Social Security Number: Not voluntary. In the event an individual may need to be identified by SSN.

From: USNA STU III Account Manager
To: _____

Code _____

Short Title	QTY	AL	Serial Number
_____	_____	_____	_____

And nothing follows.

(Signature) Date of Receipt

I. Security Manager validates the Background Investigation and Clearance Information.

CLNC Level	Investigation Date/Type	Security Manager Name	Signature	Date
_____	_____	_____	_____	_____

I. STU III Custody Statement

II. _____ certify that I have in my possession and hold myself
Printed Name, Rank/Rate

responsible for the STU III identified above, commencing on _____ I understand the requirements
for safeguarding the same as described below:

1. When the key is inserted into the unit the STU III is classified secret.
2. The key must not be left in the unit while unattended.
3. If the key or unit is unaccounted for, notify the custodian immediately, 410-293-1575.

III. Crypto Ignition Key (CIK) Custody Statement

1. I certify that I have in my possession and hold myself responsible for the CIK identified below
commencing on _____. I understand the requirements for safeguarding this equipment.

CIK Number	Signature	Print Name	SSN	Date
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____