



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
WASHINGTON, DC 20362-5101

IN REPLY REFER TO

NAVSEAINST 2280.2A
OPR 09T
21 Aug 91

NAVSEA INSTRUCTION 2280.2A

From: Commander, Naval Sea Systems Command

Subj: SECURE TELEPHONE UNIT THIRD GENERATION (STU-III)

Ref: (a) DCMS Manual CMS-6 of 19 Oct 90, Communications Material Management Manual

Encl: (1) Acronyms and Coined Words
(2) Sample STU-III Registration Letter

1. Purpose. To reissue policies, procedures, and responsibilities for the allocation, use and control of Secure Telephone Unit Third Generation (STU-III) terminals within the Naval Sea Systems Command. This is a major revision of this instruction to incorporate policy issued by reference (a).

2. Cancellation. NAVSEAINST 2280.2 of 17 December 1988.

3. Background

a. National Security Decision Directive 145 (NSDD 145) dated 17 September 1984 issued "National Policy on Telecommunications and Automated Information Systems Security." NSDD 145 directed the Federal Government to improve the overall level of secure communications and directed the Department of Defense (DoD) to "button up" the DoD telephone communications system by 1991.

b. The Director, National Security Agency (DIRNSA) implemented the Future Secure Voice System (FSVS) program as described in a Key Management Plan dated 1 February 1988. The FSVS program was initiated to provide large quantities of inexpensive secure telephone terminals for DoD and other government agencies.

c. The STU-III was developed to meet this requirement and has become widely used throughout DoD as the primary secure communications voice equipment for non-tactical communications as defined in the FSVS Key Management Plan.

4. Definitions. Enclosure (1) provides a reference list of abbreviations used in this instruction.

a. STU-III Telephone. A telephone that provides secure voice and data service to any level of classification based on the keying material being used. It operates as both a standard telephone and as a secure device. It is a cryptographically controlled item (CCI), accountable by serial number, and is unclassified unless the Crypto Ignition Key is inserted.

21 Aug 91

b. Communications Security (COMSEC) Material Control System. COMSEC material provides cryptographic security for national security-related information. This is the logistic system through which accountable COMSEC material is distributed, controlled and safeguarded. It consists of all COMSEC Central Offices of Record (COR), crypto logistic depots, and COMSEC and Sub-accounts.

c. STU-III COMSEC Account (SCA). An administrative entity, identified by an account number, in which custody and control of STU-III terminals and associated keying material is maintained.

d. SCA Custodians and Alternates. The individuals designated by proper authority to manage the STU-III material issued to the SCA.

e. Command Authority (CA) and Alternates (ACA). Manages all aspects of the STU-III Key program within Command Headquarters and shore activities.

f. Immediate Superior in Command for COMSEC and STU-III. Manages all aspects of the COMSEC and STU-III terminals within Command Headquarters and shore activities.

g. STU-III Users. Individuals authorized to use a STU-III in a secure (classified) mode.

h. Crypto Ignition Key Holders. Individuals who sign a receipt for a Crypto Ignition Key.

i. User Representatives (UR). Individuals authorized by the CA to order keying material for STU-III users.

j. STU-III Directorate Representatives (SDR). Individuals within each Directorate who prepare STU-III requirements which are coordinated with the SCA Custodian and the Staff Responsibility Officer for STU-III.

k. Staff Responsibility Officer for STU-III (SROS). The individual who has oversight responsibility for the STU-III program as required by reference (a). At Command Headquarters, the CA has been assigned the additional responsibility of SROS.

l. Keying Encryption Keys (KEK). Also known as a fill device, this material is used to initially load the STU-III telephone so it can be used in the secure mode. After the KEK is loaded into a terminal it becomes a Crypto Ignition key. Initial loading must be performed by the SCA Custodian for each STU-III telephone.

m. Crypto Ignition Key (CIK). The CIK is a locally accountable device which enables and disables secure operation of the STU-III. It is similar in appearance and size to a standard door key and commonly called THE KEY. Duplicate CIKs can be made from the manufacturer's blank keys provided with the STU-IIIs.

21 Aug 91

5. Policy

a. Allocation of STU-IIIs. STU-III telephones are allocated to Command Headquarters and shore activities according to the need for secure or sensitive communications.

b. Accounting. All STU-III terminals and keying material located at Command Headquarters and shore activities is subject to STU-III accounting and inventory procedures, established by reference (a), as follows:

(1) STU-III Telephones. Annual accounting to the Director, Communications Security Material System (DCMS) is required.

(2) CIKs. Annual accounting is required locally.

(3) STU-III Keying Material. Semiannual accounting to DIRNSA is required.

c. Physical Security of STU-III Terminal.

(1) Unkeyed. An unkeyed terminal must be protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering. An unkeyed terminal may be used as a standard telephone. Unkeyed refers to a terminal that; (1) has not been loaded with keying material, or (2) is loaded with keying material but which is being used without the Crypto Ignition Key.

(2) Keyed. When the terminal is keyed and the associated Crypto Ignition Key inserted into it, it must be afforded protection commensurate with the classification level of the key it contains.

d. Physical Security of Crypto Ignition Keys. Crypto Ignition Keys must be protected against unauthorized access because the keys permit the STU-III terminal to be used in the secure mode.

(1) User CIKs. During normal working hours the CIK must be removed from the terminal when authorized persons are not present. When the CIK is stored in the same room as the terminal, the CIK must be afforded protection commensurate with the classification level of the key it contains (e.g., in an approved security container). If the CIK is stored in an area apart from the terminal it should be stored under the best conditions available (e.g., a locked cabinet or desk). CIKs may not be removed from the building. Procedures should be incorporated into the daily security checklist to ensure that the CIKs have been removed from the terminals and properly stored.

(2) Master CIKs. All Master CIKs will be held by the SCA Custodians or by individuals designated by the CA/SROS as a Master CIK User. Master CIKs will be protected to the classification level of the keyed terminal.

21 Aug 91

e. Acoustic Security. Acoustic security for the STU-III is based on a "common sense approach" using the following basic policies and procedures:

(1) Standard Handset Mode. When using the STU-III to discuss classified or sensitive unclassified information, it is the responsibility of STU-III users to ensure that conversations are not overheard by those who do not have the proper clearance and need-to-know.

(2) Secure Speaker Phone Mode. To ensure that only properly cleared individuals with a need-to-know hear a STU-III broadcasting in the Secure Speaker Phone mode this feature may only be used in private offices or conference rooms. The authorized user of the STU-III must ensure that the Secure Speaker Phone may not be monitored from connecting offices or from a common hallway.

f. Security For STU-III Data Port Applications. While fielded primarily for secure voice the STU-III has the added ability to transmit data through a built-in data port. When using the STU-III for the transmission of classified or sensitive data using a transfer device (e.g., computer or facsimile), the following security policies and procedures shall be adhered to:

(1) Approval must be obtained in writing from the Command Authority for each data application prior to its purchase and use.

(2) Contact your Directorate AISSM at Command Headquarters or the AIS Security Officer at shore activities for AIS guidance.

(3) When connecting any data instrument to a STU-III terminal, the incoming telephone line must be connected to the STU-III. The data instrument will be connected to the STU-III with the appropriate cable.

(4) Establish secure voice contact first and verify that the security level displayed on the STU-III terminal is equal to or greater than the maximum security level of the data to be transmitted via the computer/facsimile.

(5) During data transmissions, authorized persons must be present to monitor the terminal. Use of the STU-III's auto-answer capability is prohibited. The data must be sent only after the sending and receiving parties have observed the STU-III terminal display and have assured themselves that the information on that display is correct. Existing Command regulations governing document control apply to all incoming/outgoing facsimile transmissions.

(6) Use of STU-III terminals within Sensitive Compartmented Information Facilities (SCIFs) will be coordinated with the CA and SEA 00G.

g. Loss of STU-III and Related Items. Loss of any STU-III or related item will be immediately reported to the SCA Custodian who will report the loss to the Command Authority as follows:

(1) Loss of a STU-III telephone will be reported to the Command COMSEC Custodian who will take action per reference (a). At the same time, the appropriate SCA Custodian will erase those CIKs associated with the lost STU-III.

(2) Loss of a CIK will require the SCA Custodian to erase the CIK from its associated STU-III by rekeying the terminal.

(3) Loss of both a STU-III and its associated CIK is a COMSEC security violation which must be reported to Director, Communications Security Material System and National Security Agency per reference (a).

h. Training. No formal training for the STU-III user(s) is available nor required. Self-training for STU-III users will consist of reviewing the manufacturer's manual, this Command Instruction and completing the STU-III registration letter, enclosure (2). Additional guidance or assistance can be obtained from the SCA Custodian or Alternate, if required.

6. Responsibility.

a. Immediate Superior in Command (ISIC) for STU-III (SEA-09T2).

(1) Performs oversight responsibility for the STU-III program within the Naval Sea Systems Command.

(2) Consolidate Command Headquarters and shore activity STU-III telephone requirements for the Chief of Naval Operations (OPNAV 941J) annual configuration report.

(3) Review requests from Command shore activities for the establishment of STU-III COMSEC Accounts.

(4) Conduct inspection of Command shore activity SCAs to ensure they are in compliance with all Department of the Navy and higher authorities pertaining to the STU-III.

b. Command Authority. Approve User Representatives for Command headquarters and shore activities.

c. Staff Responsibility Officer for STU-III (SROS).

(1) Performs oversight responsibility for the STU-III program at Command Headquarters.

(2) Appoints in writing SCA custodian and alternates for the Command headquarters SCA.

(3) Approve STU-III computer and facsimile applications located at Command Headquarters.

21 Aug 91

(4) Establish user guidance for the local use and security of the STU-III telephones, keying material and CIKs.

d. User Representatives.

(1) Order keying material as approved by the Command Authority per reference (a), and provide a copy of each keying material order to the Command Authority and to the SCA Custodian.

(2) Act as principal advisor to STU-III users on matters related to STU-III keying material.

(3) Use Department, Agency, and Organization (DAO) codes as assigned by the Command Authority and keymat identification for users according to the format required by reference (a).

e. SCA Custodians and Alternates.

(1) Act as advisor to STU-III users on matters relating to the STU-III program.

(2) Verify clearances of CIK holders prior to distributing CIKs.

(3) Receive and distribute STU-III telephones according to the distribution plan specified by the SROS and SDRs for STU-III.

(4) Brief CIK holders on the security and operation of the STU-III.

(5) Perform initial key loading of STU-III telephones and create CIKs for CIK holders.

(6) Maintain a list of serial numbers, holders, and locations for the STU-III telephones, keying material and CIKs.

(7) Perform semiannual inventory for the keying material and annual inventory for the STU-III telephones and CIKs.

(8) Destroy expired keying material and fill devices by "zeroizing" the keys on an unloaded terminal and return damaged keying material to DIRNSA.

(9) Report STU-III problems listed in paragraph 4f to the command STU-III SCA Custodian, Command Authority and/or COMSEC Custodian.

f. Directorate Representatives.

(1) Determine allocations of STU-III telephones and priority of installations within their organization.

21 Aug 91

(2) Coordinate with the Facilities Design Branch (SEA 09P) concerning the installation of any additional telephone line connections, data interfaces, and electrical power requirements.

g. CIK Holders.

(1) Obtain a briefing from the SCA Custodian on the operation and security of the STU-III.

(2) Ensure the STU-III is properly used and protected and access is restricted to authorized personnel having an appropriate clearance.

(3) Store the CIK in a secure container when not in use and control access to it.

(4) Perform electronic rekeying of the STU-III terminal annually at the key expiration date, or when notified or prompted by the Key Management System (KMS). Rekeying is accomplished electronically via a telephone call to the KMS computer (1-800-635-6301). A recorded message provides the tutorial instruction necessary to accomplish rekeying function and the display on the STU-III telephone will indicate completion.

(5) Report suspected security violations to the SCA Custodian.

(6) Obtain approval of the Command Authority for a change of location of any STU-III terminal.

(7) Notify the SCA Custodian of any personnel moves, transfers, or terminations so that accountability for the STU-III and CIK can be maintained.

h. STU-III Users.

(1) Ensure that the STU-III is properly used and protected and access to the keyed telephone is restricted to authorized personnel having the appropriate clearance. If an individual with a clearance lower than the key STU-III needs to use the terminal, the STU-III user must place the telephone call, notify the second party of the lower clearance level, and remain present for the duration of the telephone call.

(2) Monitor the identification information the STU-III display and verify the identity of called parties, and report to the SCA Custodian if errors are observed on the display.

(3) Ensure classified conversations are not overheard or classified data observed by persons not having a proper security clearance.

NAVSEAINST 2280.2A

21 Aug 91

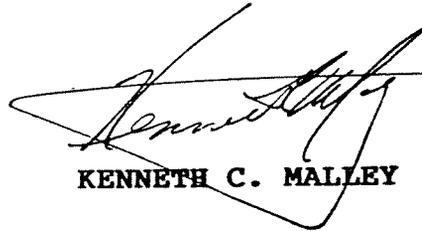
(4) Supervise the use of STU-IIIs by foreign nationals.

(5) Report suspected security violations to the SCA Custodian.

(6) View the terminal display to identify the distant end party and the authorized security classification level of the call.

7. Action. All Command personnel, as well as Program Executive Officers and Direct Reporting Program Managers, shall comply with this instruction.

8. Exclusion. This instruction does not apply to the Nuclear Propulsion Directorate (SEA 08).



KENNETH C. MALLEY

Distribution:

NAVSEA Special List Y4
PEO-SSAS
PEO-SCWS
DRPM (PMS350)
DRPM (PMS400)

Copy to:

SNDL A3 CNO (OP 941J)
C84B COMNAVSEASYS COM Detachments
FKP COMNAVSEASYS COM Shore Activities (less FKP6B)

Stocked: COMNAVSEASYS COM (SEA 09P22) (100 copies)

21 Aug 91

ACRONYMS AND COINED WORDS

ACA Alternate Command Authority
AIS Automated Information System
AISSM Automated Information System Security Manager
CA Command Authority
CCI Cryptographically Controlled Item
CIK Crypto Ignition key
COMSEC Communications Security
COR Central Offices of Record
DAO Department, Agency, and Organization
DCMS Director
Communications Security Material System
DIRNSA National Security Agency
DoD Department of Defense
FSVS Future Secure Voice System
ISIC Immediate Superior in Command
KEK Keying Encryption Keys
KMS Key Management System
SCA STU-III COMSEC Account
SDR STU-III Directorate Representatives
SROS Staff Responsibility Officer for STU-III
STU-III Secure Telephone Unit Third Generation
TEMPEST Control of Compromising Emanations
UR User Representatives

21 Aug 91

2280
Ser 09T2/STU

MEMORANDUM

From: (STU-III User)
To: STU-III Account Custodian (SEA 09T2)
Subj: STU-III USER REGISTRATION STATEMENT
Ref: (a) NAVSEAINST 2280.2A

1. I certify that I am familiar with reference (a).
2. I have assumed the duties of a STU-III User effective this date.
3. For information or general assistance, I will contact SEA 09T2, the Command's primary STU-III Account Custodian, on (703) 602-3210 or 602-3213.

NAME: _____

CODE: _____ BLDG/RM: _____ TELEPHONE: _____

STREET ADDRESS: _____

STU-III MANUFACTURER AND SERIAL NUMBER: _____

Signature