



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

USNAINST 2210.1D
6/ITSD
12 Jun 2017

USNA INSTRUCTION 2210.1D

From: Superintendent, U.S. Naval Academy

Subj: SECURE TELEPHONE EQUIPMENT TERMINAL

Ref: (a) EKMS-1 (Series)

1. Purpose. To publish policy, guidance, and instructions concerning the use and security of Secure Telephone Equipment (STE) as required by reference (a).
2. Cancellation. USNAINST 2210.1C and USNA 2280/1 STE Local Custody Document.
3. Background. STE is a "state-of-the-art" phone that is used to protect sensitive and classified U.S. Government voice and data transmissions. Due to the unique capabilities of STE phones, specific handling instructions are required. This instruction establishes policy for the use and control of STEs and their associated Communications Security (COMSEC) keying material (keymat).
4. Action. All USNA and contingent staff personnel who are authorized STE users will familiarize themselves and comply with the contents of this instruction.
5. Definitions
 - a. Command Authority. The individual or entity responsible for the appointment of user representatives for a department, agency, or organization and key ordering privileges. The Senior Message Center Person, Information Technology Services Division (ITSD), serves as USNA's command authority. This position must be filled by a First Class Petty Officer or above and shall be designated in writing by the Superintendent.
 - b. Crypto Ignition Key (CIK). A storage device that contains information used to electronically lock and unlock a STEs secure mode. The secure mode is usable when the CIK (KSV-21 card) is inserted and disabled when it is removed. The CIK is unclassified when not inserted in a STE.
 - c. Authentication Information (Key ID). The information which identifies a STE telephone. Authentication information is specified for each STE 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 STE. 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. At USNA, the highest classification level authorized for an individual STE is SECRET.

(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.

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 the 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 operational 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 must be locked in an appropriate security container per reference (a) or kept in the possession of the authorized user(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 Center (x31575). Master CIKs are only created by the Message Center. The Message Center will retain and store the Master CIK to preclude unauthorized creation of CIKs.

d. **Terminal/CIK Chain of Custody.** Upon issue/receipt of STE or CIK, a COMSEC Responsibility Acknowledgement Form and an SF 153 COMSEC Material Report are required to be completed. The custody documents will be retained by the Message Center. All secure voice equipment is subject to semi-annual inventory. When the user is transferred or relieved,

the user will notify the Message Center and a new custody documents will be updated to reflect the custody change before the member departs.

7. User Responsibilities

a. Users are responsible for the proper security, control, and accountability of all STE and COMSEC keymat that they are authorized to use. All personnel having access to secure voice material shall have a security clearance equal to, or greater than, the classification of the material. Users must be U.S. Government employees (military or civilian) who are natural born or naturalized U.S. Citizens.

b. Users must pay close attention to 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 to determine "need-to-know" when communicating classified information.

c. Whenever any of the following four conditions exist, classified information shall not be transmitted. Report conditions to the Message Center immediately; do not use the STE for secure communications until the condition has been cleared.

(1) 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 at the distant terminal.

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

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

(4) The display fails.

d. The crypto period for the STE 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 STE user's manual. In the event of an expired key, (STE will indicate "Invalid User CIK") the KSV-21 card must be rekeyed by Message Center personnel.

8. Authorization and Installation

a. Authorization to hold STEs is only granted by the Message Center.

b. Work Space Installation. Installation will only be accomplished by Message Center personnel. Basic requirements for installation are an 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 requirements for secure voice in residences should arise, the head of the division concerned should submit a request through the Message Center to be approved by the Deputy Superintendent/Chief of Staff, stating the requirement and justification. Any cost involved for installation will be borne by the requesting division. No new telephone service should be required in the residence, as the STE will work on any telephone line. A STE 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 in accordance with reference (a). 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.

9. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

10. Review and Effective Date. ITSD will review this instruction annually on the anniversary of the effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or otherwise canceled prior to the 5-year anniversary date, or an extension has been granted.

11. Forms. SF 153 COMSEC Material Report can be found in the General Service Administration's website at <http://www.gsa.gov/portal/forms/type/SF> and should be completed at the time of COMSEC issue/receipt and retained by ITSD. The COMSEC Responsibility Acknowledgement Form will be generated locally by ITSD using the template provided in reference (a), annex k, and retained by ITSD.


W. E. CARTER, JR.

Distribution:
All Non-Mids (electronically)