

**30 September 1996**

**Communications**

**PROTECTION/USE OF STU-III**



**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the HQ AFRC WWW site at: <http://www.afrc.af.mil> and the AFRCEPL (CD-ROM) published monthly.

---

OPR: 914 CF/SCS (Henry P. Mailloux)  
Supersedes 914 AGR 56-2, 17 August 1992

Certified by: 914 CF/SC (Paul M. Kendzierski)  
Pages: 2  
Distribution: F

---

This instruction provides guidance regarding the use and protection of the STU-III. It implements AFPD 33-2, *Information Protection*, AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type I*, and AFCA, Air Force Command Authority Policy. It applies to all 914 AW personnel.

**SUMMARY OF REVISIONS**

This revision changes implementing publications from Policy Messages to AFPD 33-2 and AFI 33-209. It references a change in reporting problems experienced to the STU III office in paragraph 2.9.

**1. Responsibilities .** Each STU-III user will ensure that the procedures outlined in this instruction are adhered to at all times.

**2. Procedures:**

- 2.1. Use the STU-III in the unkeyed mode to place unsecured, unclassified calls. Remove the Crypto Ignition Key (CIK) to unkey the terminal.
- 2.2. When the terminal is in the keyed mode (CIK in the phone), it must be afforded protection commensurate with the level of the key it contains and may only be used by authorized personnel. When unauthorized personnel are in the area, the keyed STU-III must be under the operational control and within the view of at least one known, appropriately cleared, and authorized person.
- 2.3. STU-IIIs not operational 24 hours a day will have the CIK removed at the close of business. The CIK must be an item on the end of day security checklist. The CIK will be stored in a GSA approved security container, if kept in the same room as the STU-III. Only authorized STU-III users will have access to the container. When the CIK is stored in another room, it will be kept in a GSA approved security container. If a security container is not available, store the CIK in a locked cabinet, desk, etc.

The adequacy of storage alternatives is determined on a case-by-case basis, by the unit security manager within each using organization.

2.4. Strict attention must be paid to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance classification displayed. Recommend users scroll the distant end to ensure the distant end key is current and not expired.

2.5. Before discussing classified information on the STU-III, the person making the classified call must ensure all personnel in the area are cleared and those remaining have a need to know.

2.6. Users should pay close attention to the authentication information displayed in the terminal during each secure call. When two terminals communicate in the secure mode, each terminal automatically displays the authentication information of the distant terminal. The information displayed indicates the organization reached, the approved level of the call, and when there is foreign access of the terminal, but does not authenticate the person using the terminal. Therefore, users must use judgment in determining need-to-know when communicating classified information.

2.7. Report a lost CIK to the base COMSEC manager, immediately. You will be instructed by the COMSEC manager on what actions to take.

2.8. Ensure the equipment custodian has all STU-III's assigned to the section listed on the CA/CRL.

2.9. If any problems are experienced with the STU-III, call the STU-III support office (SCS).

**3. Emergency Action Procedures.** In the event of fire, natural disaster, or covert threat, the CIK will be removed from the STU-III telephone and locked up, or kept in the personal possession of an authorized individual.

GERALD A. BLACK, Col, USAFR  
Commander