

3 JULY 1997



Communications

**SECURE TELEPHONE UNIT (STU-III)
PROCEDURES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO/PP WWW site at:
<http://afpubs.hq.af.mil>

OPR: 60 CS/SCBS (SrA Kenneth W. Lackey, Jr)
Supersedes TAFBI 33-104, 15 February 1997

Certified by: 60 CS/CC (Lt Col R. K. Norvell)
Pages: 7
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*. It establishes STU-III procedures for Travis Air Force Base and sets the minimum requirements for safeguarding and controlling the STU-III and its associated crypto ignition keys. It applies to all 60th Air Mobility Wing, 349th Air Mobility Wing, and tenant unit personnel assigned or attached to Travis Air Force Base.

SUMMARY OF REVISIONS

Paragraph **5**. has been modified to further define training procedures. Paragraphs **6**. through **11**. have been added. Paragraph **6**. establishes the STU-III functional review program. Paragraph **7**. clarifies STU-III shipping procedures. Paragraph **8**. discusses communications security incidents. Paragraph **9**. explains STU-III keying responsibilities. Paragraph **10**. defines local STU-III outage procedures. Paragraph **11**. explains the content requirements for local operating instructions.

1. General Information:

1.1. STU-III System Description. The STU-III is a dual-purpose telephone capable of providing secure and nonsecure voice and data transmission capabilities. It may be used for unclassified calls and is interoperable with the public telephone network. It is intended to provide secure voice and data capabilities throughout the U.S. Government and U.S. Government contractor communities where a requirement for transmission of classified and sensitive unclassified information exists.

1.2. STU-III User Agency Program. The base COMSEC Account is responsible for managing the STU-III user agency program. COMSEC Account personnel administer policy and doctrine as directed by the Air Force STU-III Command Authority, Headquarters, Air Force Communications Agency (HQ AFCA).

1.3. Definitions. The following is a glossary of related STU-III terms.

1.3.1. Authentication Information. Unclassified information identifying an individual STU-III. Authentication information is automatically displayed on the distant end STU-III during a secure call. Authentication information includes the following:

1.3.1.1. The highest classification level authorized for an individual STU-III. During a secure call, the clearance level that appears in the display is the highest level common to both STU-IIIs, and is the authorized level for the call. A STU-III keyed to SECRET can access a STU-III keyed to TOP SECRET; however, SECRET will appear in both displays and is the authorized level for the call.

1.3.1.2. Identification of the using organization (e.g., USAF) followed by the using unit (e.g., 60 AMW).

1.3.1.3. Expiration date of the STU-III's crypto ignition key.

1.3.1.4. Foreign access to the STU-III, where appropriate (e.g., US/NATO).

1.3.2. Authorized User. An individual who is a US citizen whose duties require access, and has a security clearance commensurate with the level of the crypto ignition key.

1.3.3. Crypto Ignition Key (CIK). A key-shaped device containing a portion of the STU-III algorithm in encrypted form, encoded for use only with its associated STU-III. Insertion of the CIK into the STU-III allows the user to access the secure mode, while its absence disables the secure mode.

1.3.3.1. Master CIK. A CIK which may be used to create additional CIKs for a STU-III as they are required, up to the maximum allowed by the STU-III (usually eight). It is general policy not to create master CIKs.

1.3.3.2. User CIK. This allows the user to access the secure mode only. It does not provide a duplication function like the master CIK.

1.3.4. Keyed STU-III. A STU-III in which the CIK has been inserted.

1.3.5. Secure Telephone Unit (STU-III). A telephonic device designed to cryptographically protect sensitive unclassified and classified information. The STU-III may also be used for unclassified telephone calls.

1.3.6. STU-III Responsible Officer (SRO). An individual appointed by their commander who is responsible for controlling, protecting, and accounting for all STU-IIIs and CIKs within their unit or section. They are also responsible for training all authorized users within their unit or section. SRO duties and responsibilities are explained in greater detail in the Travis AFB STU-III User Agency Training Guide, which is available from the COMSEC Account.

1.3.7. STU-III User Representative. A member of the COMSEC Account who manages the STU-III user agency program. They are also responsible for training SROs.

1.3.8. Unkeyed STU-III. A STU-III from which the CIK has been removed.

2. Operating Procedures:

2.1. Unclassified Calls. When the STU-III is unkeyed, it will be used to place nonsecure, unclassified calls only. Dial the distant party as usual.

2.2. Classified/Sensitive Unclassified Calls:

2.2.1. When the STU-III is keyed, it must be afforded protection commensurate with the classification level of the CIK it contains and may only be used by an authorized user. 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 authorized user.

2.2.2. STU-IIIs not operational 24 hours a day will have the CIK removed and secured at the close of business. The removal of the CIK must be an item on the Standard Form 701, **Activity Security Checklist**. The CIK will be stored in a GSA-approved security container if kept in the same room as the STU-III, and only authorized users will have access to the container. The CIK may be stored in another room in a GSA-approved security container or in a locked cabinet, desk, etc. The adequacy of storage alternatives for the CIK should be determined on a case-by-case basis by the unit security manager within each using organization.

2.2.3. Before discussing classified information on the STU-III, the caller must ensure all personnel in the area are cleared and have a need to know.

2.2.4. Users should pay close attention to the authentication information displayed on the STU-III during each secure call. The information displayed indicates the organization reached, the approved level of the call, and when there is foreign access to the STU-III, but does not authenticate the person using the STU-III. Therefore, users must exercise judgment in determining need-to-know when communicating classified information. Strict attention must be paid to the classification level of the conversation to ensure it does not exceed the highest classification displayed. It is recommended users scroll through the distant end authentication information to ensure the distant end CIK is current and not expired.

2.3. Losses. A lost STU-III or CIK must be immediately reported to the COMSEC Account. COMSEC Account personnel will give instructions on what actions to take.

2.4. Accountability. The equipment custodian must ensure all STU-IIIs assigned to the unit/section are listed on the Custodian Authorization/Custody Receipt Listing (CA/CRL).

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

4. Requirements To Install A STU-III In A Residence (On/Off Base): The unit commander must sign a letter to authorize the installation of a STU-III in a private residence. This ensures the commander knows where unit assets are and authorizes use of government equipment in a private residence. All personnel with a STU-III in their residence must contact their SRO to receive instructions for use and protection of the STU-III and its associated CIKs.

5. Training: All SRO/alternate SRO training will be documented on 60 AMW Form 10, **STU-III Responsible Officer and User Training Checklist**, to ensure training is standardized for all Travis AFB personnel.

5.1. SROs. SROs and alternate SROs will be trained and certified annually by the STU-III User Representative per the STU-III Command Authority. This training will include a block on the use of the STU-III.

5.2. Authorized Users. Authorized users will be trained by their SRO prior to being granted access to a keyed STU-III, and on an annual basis thereafter. This ensures they understand the security requirements pertaining to the STU-III and its associated CIKs.

6. Functional Reviews: All STU-III user agencies will be reviewed annually by COMSEC Account personnel. The functional review checklist covers administrative functions, physical security measures, accountability, and training procedures. A copy of the checklist can be obtained by contacting the COMSEC Account or downloading from the COMSEC Account Internet site at <http://w3.travis.af.mil/com-sec>.

6.1. Procedures. COMSEC Account personnel will contact the SRO to schedule a functional review. During the functional review, COMSEC Account personnel will review the STU-III user agency binder, and visually inspect the STU-III, its associated CIK(s) and the security container where it is stored, and any other applicable documentation. At the conclusion of the functional review, the user agency will be rated as satisfactory or unsatisfactory. If rated unsatisfactory, another functional review will be scheduled after 90 days.

6.2. Reports. All noted discrepancies will be documented in a report sent to the SRO and their unit commander. The SRO will have ten working days to respond to the noted discrepancies. This response will document all actions taken to correct the noted discrepancies. If all discrepancies cannot be corrected within 30 days, the SRO must send amplifying reports every 30 days until all discrepancies are corrected.

7. Shipping Instructions: To ensure strict accountability of the STU-III as a cryptographic controlled item (CCI), all STU-IIIs requiring vendor repair or shipment to another unit must be shipped through the Standard Base Supply System. Contact the Supply Squadron, Equipment Management Section, for more information on shipment of CCIs.

7.1. Forms. A copy of the completed AF Form 1149, **Requisition and Invoice/Shipping Document**, must be sent to the COMSEC Account prior to shipment of the STU-III. If the STU-III is being sent to the vendor for repairs, an AF Form 9 must also be completed.

7.2. Security Requirements. A STU-III being sent to the vendor for repair must be zeroized prior to shipment, and all associated CIKs returned to the COMSEC Account. Zeroization instructions can be found in the STU-III owner's manual. STU-IIIs sent to deployed locations are exempt from zeroization; however, all associated CIKs must be kept separate from the STU-IIIs, in the possession of the SRO or an authorized user. If the STU-III cannot be zeroized, contact the COMSEC Account for instructions.

8. 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.

8.1. Examples:

8.1.1. A CIK left unattended in or near its terminal, without an authorized user present.

8.1.2. A lost STU-III.

8.1.3. A lost STU-III fill device.

- 8.1.4. An unauthorized user making a secure call on a STU-III.
- 8.1.5. A lost CIK not reported to the user representative within 72 hours.
- 8.1.6. A secure call completed using an expired CIK.
- 8.1.7. Any instance where the authentication information displayed during a secure call is not representative of the distant terminal.
- 8.1.8. Failure to adequately protect or erase a CIK associated with a lost STU-III.
- 8.1.9. Failure to delete a lost CIK from its associated STU-III.
- 8.1.10. Any instance where the display indicates the distant terminal contains a compromised key.
- 8.1.11. Any instance where the display is inoperative and a secure call is completed.
- 8.1.12. Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or the use of a maintenance procedure that deviates from established standards.
- 8.1.13. Tampering with or penetration of a STU-III, discovery of an electronic surveillance or recording device in or near an operational STU-III or unexplained zeroization of a STU-III when other indications of unauthorized access or penetration are present.
- 8.1.14. Violation of two-person integrity (TPI) on Top Secret operational fill devices.
- 8.1.15. Unauthorized access to STU-III materials, including access by persons who were mistakenly believed to have held appropriate clearances.
- 8.1.16. Deliberate falsification of STU-III accounting records.
- 8.1.17. The crash of any aircraft that has STU-III materials aboard.
- 8.1.18. Any missing aircraft, ship, or mobile unit that has STU-III materials aboard.

8.2. Reporting Procedures. Any suspected or known COMSEC incidents must be reported by secure means to the COMSEC Account immediately. The COMSEC Account will send a report to the Controlling Authority, Command Authority, and MAJCOM within four hours of the discovery of the incident. Follow-up reports will be sent in accordance with AFI 33-212, *COMSEC Incident Reporting*.

9. STU-III Keying Responsibility: It is the responsibility of the SRO to ensure all STU-IIIs are keyed as required, to include annual electronic rekeying. Contact the COMSEC Account for keying instructions.

10. Outage Procedures: STU-III outages are separated into key error or STU-III malfunction categories.

10.1. Key Errors. If the user has a problem engaging the secure mode or if the display indicates a key error message, then the SRO will perform an electronic rekey on the terminal. If this is ineffective, the SRO will receipt for a new fill device at the COMSEC Account and rekey the terminal.

10.2. STU-III Malfunctions. If a STU-III is experiencing problems other than a key error, the SRO will call the 60 CS Base Network Control Center Help Desk, to open a work order. Help Desk personnel will coordinate the work order with the 60 CS Secure Communications facility, who will provide limited troubleshooting and maintenance. If the problem is a hardware failure inside the STU-IIIs outer casing, Secure Communications personnel cannot repair the STU-III, and it must be shipped to the vendor for repairs. Contact the individual vendor for information on repair of terminals.

11. Operating Instructions: An operating instruction (OI) is required for offices where STU-IIIs are used. This OI will contain normal operating procedures as well as emergency planning for fire, bomb threats, and natural disasters. When preparing the OI, the SRO must consider the available options for securing or removing the CIK to ensure security. The OI must also contain deployment procedures, if applicable.

12. Prescribed Forms: AF Form 1149, 60 AMW Form 10 and SF Form 701.

MICHAEL J. REAGAN, Lt Col, USAF
Director of Wing Staff

Attachment 1

GLOSSARY OF REFERENCE AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection*.