BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-209

1 FEBRUARY 1998

Communications and Information

OPERATIONAL INSTRUCTION FOR THE SECURE TELEPHONE UNIT (STU-III) TYPE 1

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCI (J.J. Plummer)
Supersedes AFI 33-209, 1 October 1996

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 45
Distribution: F

This Air Force instruction (AFI) implements National Telecommunications and Information Systems Security Instruction (NTISSI) 3013, *Operational Security Doctrine for the Secure Telephone Unit III (STU III),* 8 February 1990. It prescribes operational security doctrine for the Secure Telephone Unit (STU-III), Type 1 terminal, and its operational and seed key encryption keys (KEK). It establishes the minimum standard for all Air Force STU-III operations. This instruction applies to all Air Force units, Air Force contractors, United States Air Force Reserve (USAFR), and Air National Guard (ANG) who handle, distribute, account for, store, or use the STU-III Type 1 terminal and associated communications security (COMSEC) material. It takes precedence over other publications for COMSEC matters relating to the STU-III Type 1 terminal and associated keying material. Do not give extracts to the public without the specific approval of the Headquarters Air Force Communications Agency (HQ AFCA) and the National Manager, National Telecommunications and Information Systems Security Committee (NTISSC). **Violations of the prohibitions of paragraph 3.3 by military members constitute a violation of Article 92, Uniform Code of Military Justice (UCMJ), and may result in punishment under the UCMJ. Violations of paragraph 3.3 by civilian personnel may result in administrative or other disciplinary action under applicable civilian regulations or instructions.** The term "major command" (MAJCOM) used in this instruction includes field operating agencies (FOA). The inclusion of names of any specific commercial product, commodity, or service is for informational purposes only and does not imply endorsement by the United States Air Force. Direct questions or comments regarding the technical content of this instruction through appropriate MAJCOM channels to HQ AFCA/GCIS, 203 West Losey Street, Room 2040, Scott AFB IL 62225-5234. Refer recommended changes and conflicts between this and other publications to HQ AFCA/XPXP, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5233, on AF Form 847, **Recommendation for Change of Publication.** See **Attachment 1** for a list of references, abbreviations, acronyms, and terms.

SUMMARY OF REVISIONS

This revision updates the appointment of STU-III responsible officers (SROs), provides specific instructions for use of STU-III in residences and quarters, provides a description of AT&T 1900/1910 devices, and facsimile requirements when ordering a facsimile machine. The revision bar (|) preceding any part of this publication indicates a major revision from the previous edition.

Chapter 1

GENERAL

1.1. Purpose. This instruction and its attachments contain minimum standards for handling and controlling the STU-III Type 1 terminal and its operational and seed KEKs. It provides COMSEC doctrine essential for the security of the STU-III terminal and keying material.

1.2. System Description. The STU-III Type 1 terminal is a dual-purpose telephone capable of providing secure and nonsecure voice and data capabilities. Use the Type 1 terminal as an ordinary telephone. The Type 1 terminal is interoperable with the public telephone network. Use it as a secure telephone, connectable through the public telephone network to other STU-III Type 1 and Type 2 terminals (see **Attachment 10** to establish a closed community.) In the secure mode, each STU-III terminal (Type 1 and Type 2) displays authentication information of the distant STU-III terminal. The STU-III terminal has a device called a crypto-ignition key (CIK) that locks and unlocks its secure mode. If the CIK is removed, protect the terminal as an unclassified controlled cryptographic item (CCI). In addition, the following statements apply:

1.2.1. Use the Type 1 terminal to provide secure voice and data capabilities throughout the United States (US) Government and US Government contractor communities where there is a requirement for transmission of classified and sensitive unclassified information. Use the Type 1 terminal to replace or augment, where appropriate, all current secure and nonsecure telephones (see **Attachment 7** for STU-III use with North Atlantic Treaty Organization (NATO) countries and **Attachment 8** for using the data port.)

1.2.2. The Electronic Key Management System (EKMS) Central Facility (CF) provides key production, key management, and compromise recovery services for Type 1 terminals. The CF provides user representatives (UR) a variety of physical and electronic options. The Key Management Plan discusses these options in detail. The CF sends the Key Management Plan to URs upon completion of UR registration. Use appropriately keyed, approved Type 1 terminals to transmit all classifications and categories of voice and data. STU-III users should protect even unclassified conversations with the terminal's secure mode when connected to another STU-III terminal.

1.3. Exceptions, Waivers, and Assistance. Submit requests for exceptions or waivers to the minimum standards of this security instruction to HQ AFCA/GCIS. Do not inhibit or prohibit general use of the equipment by the application of controls more stringent than those called for by this instruction. Submit requests for assistance, including advice on the selection of appropriate Type 1 terminals in high-risk environments through COMSEC channels to HQ AFCA/GCIS.

Chapter 2

RESPONSIBILITIES

2.1. Roles and Responsibilities. Section 4 of the STU-III Key Management Plan (EKMS-702.01) explains the interactions among the various members of the STU-III community, including their roles and responsibilities. The EKMS CF distributes the plan to all registered URs. In addition to these roles and responsibilities, the following also apply:

2.1.1. The Air Force STU-III focal point is HQ AFCA/GCIS. HQ AFCA/GCIS will:

2.1.1.1. Coordinate with National Security Agency (NSA)/Y18, using MAJCOMs and other organizations' focal points, to complete the UR registration process.

2.1.1.2. Ensure MAJCOM key material (KM) points of contact (POC) and all assigned URs receive all applicable STU-III key management documents and training materials.

2.1.1.3. Maintain training materials, documents, and publications to ensure URs are familiar with STU-III key management procedures.

2.1.1.4. Approve Department/Agency/Organization (DAO) code descriptions.

2.1.1.5. Ensure the accuracy of entries on all required forms, fill in the required CA blocks, and send to the EKMS CF.

2.1.2. MAJCOMs will:

2.1.2.1. Appoint a STU-III KM POC; publicize the POC to user organizations; and provide name, office, and phone number to HQ AFCA/GCIS.

2.1.2.2. Provide information required to register URs to HQ AFCA/GCIS.

2.1.3. URs will:

2.1.3.1. Initiate UR registration.

2.1.3.2. Complete UR registration and privilege forms and send them to HQ AFCA/GCIS.

2.1.3.3. Identify STU-III key requirements and establish generic free form field identification information.

2.1.3.4. Ensure the classification of the requested key is consistent with the security clearances of the STU-III users.

2.1.3.5. Provide COMSEC responsible officers (CRO)/STU-III responsible officers (SRO) applicable STU-III KM documents and training material for initial and recurring training programs.

2.1.3.6. Provide CROs/SROs applicable STU-III initial training and annual recurring training and document this training.

2.1.3.7. Establish and publicize procedures for annual inventories of CIKs.

2.1.4. Using Organizations. Commanders of using organizations will appoint CROs/SROs according to AFI 33-211, *Communications Security (COMSEC) User Requirements*. Do not appoint COMSEC managers, alternate COMSEC mangers, or COMSEC accountants as SROs.

2.1.4.1. Appoint SROs for units receiving STU-III key only. Do not appoint a SRO where there is a CRO.

2.1.4.2. CROs/SROs are the unit focal point on all STU-III KM matters.

2.1.4.3. Provide STU-III key requirements to the UR.

2.1.4.4. Work with the UR to establish generic free form field identification information.

2.1.4.5. Establish a STU-III user training program on the proper use and security of their STU-III terminals and Key Storage Device (KSD)-64As. Conduct and document this training initially and once each year.

2.1.4.6. Maintain a copy of this instruction and all applicable vendor STU-III operators' manuals.

2.1.4.7. Conduct annual inventories of CIKs according to guidance provided by the UR. During the inventory, make sure the physical protection of the CIKs meets the requirements outlined in this AFI.

2.2. Appointment Letter for STU-III Officers and Alternates. See **Attachment 12** for a sample appointment letter.

Chapter 3

PHYSICAL SECURITY

3.1. Classification Guidance. The Type 1 terminal is a CCI and is unclassified when unkeyed.

3.2. Releasability. The STU-III Type 1 terminal is releasable to the Canadian Government. Handle individual transfers according to existing COMSEC release policies.

3.3. Physical Security. Air Force Systems Security Instruction (AFSSI) 4001, *Air Force COMSEC Publication Controlled Cryptographic Items (CCIs)*, contains general procedures for controlling unkeyed Type 1 terminals and other unkeyed CCIs. Controls are used to guard against preventable losses to an actual or potential enemy. Failure to handle CCIs according to AFSSI 4001 by military personnel violate Article 92 of the UCMJ and may result in punitive action under the UCMJ. Unauthorized disclosure by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions. The following guidance outlines procedures for the physical security of the Type 1 terminal (see **Attachment 9** for outside normal office environment):

3.3.1. Unkeyed Terminal. Protect an unkeyed Type 1 terminal in a manner sufficient to prevent any reasonable chance of theft, sabotage, or tampering. Persons who meet the access requirements of AFSSI 4001 may use an unkeyed terminal for unclassified and nonsensitive calls.

3.3.2. Keyed Terminal. AFKAG 1, *Communications Security (COMSEC) Operations*, requires you to provide a keyed terminal (CIK inserted) with protection commensurate with the classification of the key it contains. You must keep a keyed terminal (CIK inserted) under the operational control and within view of at least one appropriately cleared authorized person, when persons not cleared to the level of the keyed terminal are in the area.

3.3.3. Foreign Access. (see **Attachment 4**).

3.3.3.1. Escorted Access. You may permit foreign nationals access to the terminal area and use of the Type 1 terminal if the terminal is under direct and continuous US control and the use is in support of US operations. Foreign nationals may place nonsecure calls over unkeyed terminals. US personnel must place and supervise all calls using the terminal's secure mode. US personnel must first identify the foreign national to the distant end, indicating his/her clearance (when known and required for the call).

3.3.3.2. Unescorted Access. The commander may permit foreign nationals to have unescorted access to the installed Type 1 terminals, regardless of the terminal's release status, under all of the following conditions (**Attachment 4** provides a list of questions for these conditions):

3.3.3.2.1. The unit commander must determine if the risk of tampering with the Type 1 terminal, that could result in compromise of classified or sensitive unclassified information, is acceptable. Do not allow a foreign national unescorted access to the terminal when the commander determines the risk is unacceptable. Also, evaluate the acceptability of the risk in light of:

3.3.3.2.1.1. Local threat to individual locations.

3.3.3.2.1.2. Vulnerability of individual locations.

3.3.3.2.1.3. Sensitivity of the information protected (i.e., classification level, special security controls, and period of time during which the information is of value).

3.3.3.2.2. Personnel previously unescorted in the area prior to installation of the Type 1 terminal may still require access in conjunction with building maintenance, custodial duties, or other operational responsibilities. The following rules apply:

3.3.3.2.2.1. A foreign national employed by the US Government or a US Government contractor, or integrated into and directly supporting operations of the US Government or a US Government contractor, is authorized to use a keyed terminal in association with his/her responsibilities. Install the terminal in a US-controlled facility or a US-controlled space only. The foreign national must possess a clearance accepted by the US Government or US Government contractor, equal to the level of the key in the terminal. You must inform other STU-III users communicating with this terminal that the STU-III user is not a US citizen, by using a key that designates foreign access (see **Attachment 2**). Such access does not require a continuous US presence.

3.3.3.2.2.2. Except as permitted above, a foreign national may not have unescorted access to a keyed Type 1 terminal. Authorize unescorted access to an unkeyed terminal with no US presence only after removal and protection of the associated CIK (**Attachment 2** provides guidance on protecting CIKs).

3.3.3.3. The Type 1 terminal must remain US property. A US citizen (appropriately cleared if the key is classified) employed by the US Government or a US Government contractor remains responsible for its keying and control. This person must verify the presence of the terminal on a monthly basis. **NOTE:** Normally, do not move Type 1 terminals from an environment where the tampering risk presented by foreign national access is acceptable to a more sensitive environment where risk is not acceptable. If such action is an operational necessity, it must receive the prior approval of the unit commander, and qualified COMSEC maintenance personnel must examine it for signs of tampering. Report any evidence of tampering as a COMSEC incident and remove the terminal from operational use pending notification from the Director, NSA (DIRNSA).

3.3.4. Accountability. As a CCI, each Type 1 terminal is accountable to HQ Cryptologic Support Group (HQ CPSG/ZCK) by its serial number. **NOTE:** If a STU-III is moved or replaced, notify the local equipment custodian and CRO/SRO.

3.3.5. Storage. Store Type 1 terminals to provide protection sufficient to preclude any reasonable chance of theft, sabotage, or tampering. Foreign nationals employed by the US Government in a foreign country where there is a significant US military presence (two or more military bases where US military personnel are present) may handle Type 1 terminals in connection with warehouse functions, provided they are under constant supervision by an individual who meets the access requirements of AFSSI 4001.

3.3.6. After Duty Hours Protection. Remove the CIK from the terminal and properly protect it (see **Attachment 2**) when authorized persons leave for the day. Establish area controls sufficient to ensure access and accounting integrity of the terminal. Leave the terminal keyed (CIK inserted) only if it is in an approved area for open storage of classified material at the level authorized for the terminal's COMSEC key.

3.3.7. Transportation. AFSSI 4001 provides guidance on acceptable means of transportation for CCIs. In addition:

3.3.7.1. Zeroize or remove the associated CIK for all Type 1 terminals during shipment. Do not place seed or operational KEKs in the same carrying case, container, or shipment as Type 1 terminals.

3.3.7.2. Authorized users may also transport Type 1 terminals, KEKs, and/or associated CIKs. However, appropriately package and protect KEKs and/or CIKs separately from the terminal (e.g., in a separate container or on his/her person).

3.3.8. Installation:

3.3.8.1. Install Type 1 terminals only in:

3.3.8.1.1. US-controlled facilities.

3.3.8.1.2. US-controlled spaces worldwide.

3.3.8.1.3. Residences and vehicles of US Government and US Government contractor officials. **NOTE:** When foreign access is required follow the criteria in paragraph 3.3.3. (see Attachment 4.)

3.3.8.2. To install Type 1 terminals in foreign facilities located in countries hostile or unfriendly to the US, get approval through COMSEC channels from DIRNSA/S1 prior to installation. Submit request for either a list of countries or approval through COMSEC channels to HQ AFCA/GCIS.

3.3.8.3. Installation of Type 1 terminals is authorized in foreign facilities located in countries friendly (see **Attachment 5** for questions on this type of installation) to the US under the following conditions:

3.3.8.3.1. The purpose of the installation is to support US Government or US Government contractor communications.

3.3.8.3.2. At least one US citizen or US resident alien employee of the US Government or a US Government contractor is assigned, on a permanent basis, to the facility (and reports for work at the facility on a regular basis).

3.3.8.3.3. The terminal is installed in a US-controlled space.

3.3.8.3.4. When the terminal is installed in a non US-controlled space, it must be collocated with a US citizen or resident alien employee of the US Government or a US Government contractor. The commander must make a determination of the risk of tampering (see paragraph 3.3.3.2.1). If the risk of tampering is not acceptable, remove the terminal and place in secure storage or remove from the facility when there is no US presence. If the risk is acceptable, remove the CIK from the terminal and properly protect it when there is no US presence (**Attachment 2** provides guidance on storing CIKs). When there is no US presence for longer than 96 hours, place the terminal in secure storage or move it to a US-controlled facility or space.

3.3.8.4. Type 1 terminals meet the security requirements of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 1-92 (C), *Compromising Emanations Laboratory Test Requirements, Electromagnetics* (U). Therefore, for general use, additional emission security (EMSEC) countermeasures are not required when the

Type 1 terminal is used as a stand-alone device (i.e., secure voice only). If the Type 1 terminal transmits classified data, ensure the data port connection is made with a shielded cable.

3.3.8.5. Only appropriately trained US citizens or foreign nationals, under continuous supervision by authorized persons, may install Type 1 terminals.

3.3.8.6. Install the CCI component of the cellular STU-III Type 1 terminal in the trunk of a vehicle. Under most circumstances, locking the vehicle, removing and retaining the CIK and keys to the terminal mounting mechanism provide adequate security for the terminal when the vehicle is unattended. However, if the vehicle is unattended for an extended period of time, or turned over to maintenance personnel for repair, you cannot maintain access control and must remove the terminal (CCI portion). **Attachment 6** provides information on cellular application.

3.3.9. Maintenance:

3.3.9.1. National policy, as stated in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4000, *Communications Security Equipment Maintenance and Maintenance Training*, requires that persons who maintain COMSEC equipment used for operational purposes (including the STU-III Type 1 terminal) are formally trained US citizens. Such persons do not need clearances unless they require access to classified COMSEC material information to perform terminal maintenance.

3.3.9.2. Ordinarily, maintenance personnel may not have access to a terminal keyed for normal operations. Zeroize any terminal removed or disassembled for repair, if possible, or ensure an authorized person removes and protects the CIKs. If the zeroization function fails and the CIK is not removable, the following procedures apply:

3.3.9.2.1. For an American Telephone and Telegraph (AT&T) or a Radio Corporation of America (RCA) terminal, remove all power (alternating current and battery) that causes the terminal to zeroize.

3.3.9.2.2. Some early model Motorola terminals do not contain a battery and will not zeroize upon removal of power. Treat these terminals as classified at the same level of the key it contains. Prearrange with Motorola the return of any terminal containing key classified up to SECRET, non-sensitive compartmented information (SCI) level. DIRNSA (ATTN: V2) provides shipping instructions for terminals containing TOP SECRET or SCI key. For Motorola models that have a zeroize feature and contain a battery, follow instructions contained in the user's guide.

Chapter 4

STU-III KEY INFORMATION

4.1. Type 1 Terminal Keys. Accomplish initial keying for all Type 1 terminals (either seed or operational KEKs) with a KSD used as a fill device. Normally accomplish subsequent rekeying by remote electronic rekeying from the EKMS CF (see **Attachment 3**.) Once the initial keying has taken place, never rekey the terminal by a KSD unless the terminal was zeroized, you need to change the authentication information, maintenance was performed, or an additional keyset was added.

4.1.1. Use of Seed KEKs for Electronic Rekeying.

4.1.1.1. Electronic rekeying provides a high level of security for operational KEKs and is the standard STU-III keying method. Accomplish electronic rekeying by loading a seed KEK into the terminal with a KSD, followed immediately by the creation of at least one CIK and a call to the EKMS CF. (The seed KEK permits calls only to the EKMS CF.) During the call, the EKMS CF electronically provides an operational KEK to replace the seed KEK in the terminal. The term for this process is "conversion." Once conversion is complete, use the terminal in the secure mode to call other keyed STU-III terminals.

4.1.1.2. With electronic rekeying, users need to order only seed KEKs.

4.1.1.3. For each COMSEC account served, the EKMS CF will periodically publish a key conversion notice which is a listing of all seed KEKs charged to that account and converted through a call to the EKMS CF. The COMSEC manager must use this information to ensure all seed KEKs listed as converted were actually converted. If the manager finds a seed KEK listed on the notice still in their possession, they must promptly report this discrepancy to NSA (EKMS CF and V51A) through COMSEC channels.

4.2. Use of Operational Key Encryption Keys Loaded by Key Storage Device.

4.2.1. Under circumstances where requirements dictate (e.g., special operations requiring anonymity, or in areas where you cannot call the EKMS CF) users may load their operational KEK with the KSDs.

4.2.2. When you load an operational KEK into the terminal and at least one CIK was created, the terminal is fully operational and you can place secure calls.

4.2.3. The only terminals that can fully participate in the STU-III compromise recovery mechanism are those electronically rekeyed during a call to the EKMS CF. When possible, users must call the EKMS CF immediately following the initial loading of an operational KEK with the KSD, or as soon as possible afterward.

4.3. Classification and Accountability. Seed and operational KEKs are centrally accountable to the EKMS CF and protected according to AFKAG 1. In addition, handle and store TOP SECRET operational KEKs according to two-person integrity (TPI) procedures.

4.3.1. Normal System Operation.

4.3.1.1. Assign Accounting Legend Code (ALC) 1 to seed and operational KEKs ordered for use during normal operations. Both seed and operational KEKs are CRYPTO. Depending on the

maximum classification level approved for the terminal, operational seed KEKs are available at four levels:

4.3.1.1.1. UNCLASSIFIED.

4.3.1.1.2. CONFIDENTIAL.

4.3.1.1.3. SECRET.

4.3.1.1.4. TOP SECRET.

NOTE:

URs must query the EKMS CF for the status of all seed and operational KEKs not received within 60 days of ordering. Seed KEKs are unclassified.

4.3.1.2. Regardless of the level of a conversion, a witness is not required for keying terminals with seed KEKs. Operational KEKs, up to the SECRET level, also do not require a witness. You need a witness when you key terminals with TOP SECRET operational KEKs. You need a witness because of the requirement to handle this level of key under TPI.

4.3.1.3. Consider seed and operational KEKs destroyed for accountability purposes once you successfully key the terminal and you create a CIK. The KEK is automatically zeroized from the fill device during the key loading process. The COMSEC manager must submit a destruction report to the EKMS CF for operational KEKs. You do not require a destruction report for used seed KEKs. They are automatically dropped from accountability to the EKMS CF after you key the terminal through a call to the EKMS CF.

4.3.2. System Testing. Use test operational KEKs for unclassified on and off-line testing, and terminal maintenance. Terminals keyed with test keys are not interoperable with terminals keyed with non-test key. Test operational KEKs are unclassified, marked CRYPTO, and assigned ALC-4 (i.e., after receipt at the user COMSEC account, test KEKs are locally accountable). Do not transmit classified information when you use test operational KEKs. Test operational KEKs are not automatically zeroized during terminal loading, which allows them to be reused. ***NOTE:*** You must maintain local records until a test operational KEK is finally zeroized from the KSD.

4.4. Expiration Dates/Cryptoperiods.

4.4.1. Seed KEKs have no specified cryptoperiod since they are designed for one-time use; however, they have an expiration date that reflects the period you may use the seed KEK (e.g., up to five years).

4.4.2. All operational KEKs (regardless of how you load them into the terminal) have a one year cryptoperiod. You may display the expiration date on the terminal when it is one year from the production date of the operational KEK. At the end of the cryptoperiod, place a call to the EKMS for a new operational KEK. You should call once a quarter to ensure an up-to-date compromise key list is resident in the STU-III. Once the call is complete, users must verify the date has changed (the new date will reflect the current month and the next year). If it is not possible to call the EKMS CF, you must manually load a new operational KEK.

4.5. Access. You must have an appropriate clearance for access to classified operational KEKs. Handle seed KEKs as UNCLASSIFIED CRYPTO. However, clear COMSEC managers/URs and users to the level of classification of the operational KEK that will replace the seed KEK during electronic rekeying.

4.6. Transportation Guidelines for Seed and Operational Key Encryption Keys.

4.6.1. Within the US, its territories, and possessions, a cleared designated courier or the DCS routinely transports classified operational KEKs. However, in an emergency, if distribution is to a location not reasonably served by these means, or the urgency for delivery precludes their use, you may transport operational KEKs classified up through SECRET by US registered mail. Transport seed KEKs and unclassified operational KEKs by any means prescribed for transporting classified COMSEC material or by US registered mail.

4.6.2. Outside of the US, transport all seed and operational KEKs by cleared designated courier, US Diplomatic Courier Service, or the Defense Courier Service.

4.6.3. Normally, you may ship up to 50 operational and/or seed KEKs in a single package. However, when shipping classified operational KEKs by US registered mail for emergency reasons (paragraph 4.6.1), do not include more than 25 operational KEKs in a single package.

4.7. Reserve Key. There is no prohibition against a COMSEC manager holding some level of seed or operational KEKs in reserve for emergency use (e.g., if a terminal fails). You must keep the level to a minimum, consistent with operational requirements, to limit exposure of the keys in long-term storage.

4.8. Disposition of Seed and Operational Key Encryption Keys.

4.8.1. COMSEC managers must notify the EKMS CF by the most expeditious means of damaged, broken, or otherwise unusable fill devices and return them to the EKMS CF for disposition. Return the devices at their original classification by appropriate means as specified in paragraph 8.6. Managers must also notify the EKMS CF if they discover any evidence of tampering with the KSD package, or any discrepancy between the information on the card that accompanies the fill device and that displayed on the terminal during the loading process.

4.8.2. Once an unused KEK has passed its expiration date, do not use that KEK to key a terminal. The COMSEC manager must destroy the KEK locally. The COMSEC manager will zeroize the fill device in a Type 1 terminal (carefully follow vendor's instructions to avoid zeroization of current key loaded in the terminal during this procedure). Once destroyed (e.g., zeroized), use the blank fill device as a CIK or return it to the EKMS CF. You must witness its destruction and submit a destruction report.

4.9. Training. See **Attachment 11** for a sample training list.

Chapter 5

DESTRUCTION/EMERGENCY PROTECTION/COMSEC INCIDENTS

5.1. Destruction and Emergency Protection. Follow the provisions of AFKAG 1 in the disposal and emergency protection of Type 1 terminals and KSDs used as fill devices and CIKs.

5.2. Reportable COMSEC Incidents. The following COMSEC incidents specifically apply to the Type 1 terminal and its keys, and are reportable to DIRNSA (ATTN: V51A/Y181) according to AFI 33-212, *Reporting COMSEC Incidents*:

5.2.1. Failure of the COMSEC manager to notify the EKMS CF that a seed KEK listed on the conversion notice still exists in his or her COMSEC account.

5.2.2. Any instance where the authentication information displayed during a secure call is not representative of the distant terminal.

5.2.3. Failure to adequately protect or to erase a CIK associated with a lost terminal.

5.2.4. Any instance where the display indicates the distant terminal contains a compromised key.

5.2.5. Any lost or missing STU-III terminals.

5.2.6. Failure to adequately protect an unattended, keyed STU-III.

5.2.7. CIK left in unattended terminal for more than five minutes.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 100-235, *The Computer Security Act of 1987*

Title 5 United States Code, Section 552a, *The Privacy Act of 1974*

Uniform Code of Military Justice (UCMJ)

NTISSI 3013, *Operational Security Doctrine for the Secure Telephone Unit III (STU III)*.

NSTISSAM TEMPEST 1-92 (C), *Compromising Emanations Laboratory Test Standards, Electromagnetics* (U)

NSTISSI 4000, *Communications Security Equipment Maintenance and Maintenance Training*

AFSSI 4001, *Air Force COMSEC Publication Controlled Cryptographic Items (CCIs)*

AFKAG 1, *Communications Security (COMSEC) Operations*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFMAN 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*

Abbreviations and Acronyms

ACL—Access Control List

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFSSI—Air Force Systems Security Instruction

AIS—Automated Information System

ALC—Accounting Legend Code

ANG—Air National Guard

AT&T—American Telephone and Telegraph

CCI—Controlled Cryptographic Item

CF—Central Facility

CIK—Crypto-Ignition Key

COMPUSEC—Computer Security

COMSEC—Communications Security

CONUS—Continental United States

CPSG—Cryptologic Support Group

CRO—COMSEC Responsible Officer

CSSO—Computer Systems Security Officer

DAO—Department/Agency/Organization

DIRNSA—Director, National Security Agency

DRU—Direct Reporting Unit

DTE—Data Terminal Equipment

ECCM—Electronic Counter Countermeasure

EKMS—Electronic Key Management System

FOA—Field Operating Agency

GSA—General Services Administration

IVSN—Initial Voice Switched Network

KDC—Key Distribution Center

KEK—Key Encryption Key

KM—Key Material

KMID—Key Material Identification Number

KSD—Key Storage Device

LCT—Low Cost Terminal

MAJCOM—Major Command

MAXSL—Maximum Security Level

MINSL—Minimum Security Level

MLS—Multi-Level Secure

NATO—North Atlantic Treaty Organization

NSA—National Security Agency

NSTISSAM—National Security Telecommunications and Information Systems Security Advisory Memorandum

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

NTISSI—National Telecommunications and Information Systems Security Instruction

NTISSC—National Telecommunications and Information Systems Security Committee

POC—Point of Contact

PTT—Public Telephone and Telegraph

RCA—Radio Corporation of America

SACS—STU-III Access Control System

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SCT—Secure Cellular Terminal

SECAN—Military Committee for Communications and Information Systems Security Evaluation Agency

SHAPE—Supreme Headquarters, Allied Powers Europe

SRO—STU-III Responsible Officer

STU—Secure Telephone Unit

TELCO—Telephone Company

TPI—Two-Person Integrity

UCMJ—Uniform Code of Military Justice

UR—User Representative

US—United States

USAFR—United States Air Force Reserve

(Vn)—Special STU-II unique network key

(Vu)—Special STU-II unique user key

Terms

AFKAG—Air Force cryptographic operational general publication.

Authentication Information—Unclassified information that identifies a STU-III terminal. Each STU-III key ordered has authentication information included as a part of the key. Authentication information, displayed on the distant terminal during a secure call, includes:(1) the highest classification level authorized by the key for an individual STU-III terminal. 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 SCI. Display compartments only when they are common to both terminals; (3) identification of the using organization (e.g., 27 FW, 54 CS, 445 MDS and some times the office symbol); (4) foreign access to a keyed terminal where approved (e.g., CANADA identifies terminals supporting US/Canadian operations, and US/UK, US/AUS, or US/FORN [for terminals supporting US operations, where both US and foreign national personnel place/receive secure calls][paragraph A7.3]); and (5) expiration date of the key.

Authorized Persons—A person who meets the access requirements of AFSSI 4001, possesses a security clearance commensurate with the level of information involved, and has a need to know.

COMSEC Responsible Officer (CRO)—Unit level individual acting as the focal point for unit COMSEC activities.

Crypto-Ignition Key (CIK)—A KSD that contains information used to electronically lock and unlock a terminal's secure mode. Unlock the secure mode by inserting and turning the CIK and lock it by removing the CIK.

Department/Agency/Organization (DAO) Code—A 6-digit identification number assigned by the EKMS CF to organizational descriptions. The UR uses it when placing an order for STU-III keying

material.

Interoperable Crypto-Ignition Key—A CIK created to work in more than one terminal.

Key—Information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for encrypting or decrypting electronic signals; for determining electronic counter countermeasures (ECCM) patterns (e.g., for frequency hopping or spread spectrum); or for producing other keys. **NOTE:** "key" replaces the terms "variable," "key(ing) variable," and "cryptovariable."

Keyed Terminal—A terminal that is key loaded and in which any of its associated CIKs is inserted.

Key Encryption Key (KEK)—A key used in the encryption and/or decryption of other keys for transmission or storage.

Key Material Identification Number (KMID)—A unique number automatically assigned to each piece of STU-III keying material by the EKMS CF. The EKMS CF uses this number for key accountability purposes.

Key Storage Device (KSD)—The name given to the physical device used as a fill device and also as a CIK for all Type 1 terminals. It is a small device shaped like a physical key and contains passive memory. When used to carry key to Type 1 terminals, it is a "fill device." When used to protect key loaded into STU-III Type 1 terminals, it is a "crypto-ignition key."

MAJCOM STU-III Key Management Point of Contact (MAJCOM KM—POC) An individual or office assigned to represent a using MAJCOM at STU-III workshops, seminars, conventions, and draft operational policy.

Master CIK—The first CIK created for a terminal is designated a Master CIK which allows the holder to create additional CIKs when required, up to the terminal's maximum number of CIKs and open special features of the STU-III.

Sensitive Information—The loss, misuse, unauthorized access to, or modification of information that could adversely affect the national interest, the conduct of federal programs, or the individual privacy entitled under Title 5 United States Code, Section 552a, *The Privacy Act of 1974*, but not specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (Public Law 100-235, *The Computer Security Act of 1987*.).

STU-III Access Control System (SACS)—An option permitting STU-III users to establish special, closed communities of interest, based on a programmable access control list (ACL). Each SACS terminal can be programmed with an ACL containing selected DAO codes and/or specific KMIDs of all STU-IIIs participating in a given net.

STU-III Compromise Recovery Mechanism—The method by which the EKMS CF promulgates lists of compromised keys to all terminals.

STU-III Responsible Officer (SRO)—Unit-level individual acting as the focal point for unit STU-III activities when there is no CRO.

TEMPEST—Control of compromising emanations from message-processing hardware.

Two-Person Integrity (TPI)—A system of storage and handling designed to prohibit access to certain COMSEC keying material, by requiring the participation of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task performed. The TPI

procedures differ from no-lone zone procedures. Under TPI controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction).

Type 1 Terminal—A STU-III terminal endorsed by NSA for securing classified or sensitive information when appropriately keyed.

Type 2 Terminal—A STU-III terminal endorsed by NSA for protecting sensitive information.

US-Controlled Facility—A base or building, with access physically controlled by US citizens or resident aliens who are US Government or US Government contractor employees.

US-Controlled Space—A space (e.g., room or floor) within a facility, other than a US-controlled facility, with access physically controlled by US citizens or resident aliens who are US Government or US Government contractor employees. Keys or combinations to locks controlling entrance to the US-controlled space remain under the exclusive control of US citizens or resident aliens who are US Government or US Government contractor employees.

Unkeyed Terminal—A terminal that contains no key or one keyed with the CIK removed.

User Representative (UR)—A US citizen formally designated to order keys for STU-III terminals and perform other STU-III related duties. Assign UR responsibilities to base COMSEC managers.

Attachment 2

SYSTEM SECURITY GUIDANCE

A2.1. Purpose. The fundamental purpose of the Type 1 terminal is to provide a readily available, easy to use, secure telephone capability for all personnel who have a need to discuss and transmit classified or sensitive US information. The greatest security threat to telephone communications is where they are most vulnerable to hostile interception and exploitation (during transmission over the telephone network). Users must know that incorrect use of the terminal and its components, and failure to follow applicable communications policy may introduce security breaches that could affect not only their own communications but the integrity of communications of other STU-III system users as well. The following guidance covers those areas where there is no prescribed doctrine but where you must implement local security measures. Other directives require many of these recommended security measures.

A2.2. Using the Terminal.

A2.2.1. Observing the Display. Users must pay close attention to the authentication information displayed in the terminal window during each secure call. When two terminals communicate in the secure mode, each terminal automatically displays authentication information of the distant terminal. This does not authenticate the person using the terminal; therefore, users must use judgment in determining need-to-know when communicating classified information.

A2.2.2. Do not transmit classified information when:

A2.2.2.1. There is a question as to the validity of the authentication information in the display, even though voice recognition is possible.

A2.2.2.2. There is doubt of the validity of the organization where the distant terminal is located. (This is a reportable COMSEC incident.)

A2.2.2.3. The display indicates the distant terminal's key has expired and the period exceeds a reasonable period of time (e.g., two months).

A2.2.2.4. The display indicates the distant terminal contains compromised key. (This is a reportable COMSEC incident.)

A2.2.2.5. The display fails.

A2.2.3. Users must not exceed the classification level indicated on the terminal display. Because of interoperability among terminals of different classification levels, the display may indicate a level less than the actual classification of one terminal's keys (e.g., when a SECRET terminal calls a CONFIDENTIAL terminal, "CONFIDENTIAL" is displayed on both terminals as the authorized level for the call). Therefore, users will observe the display with each call and limit the level of information accordingly.

A2.2.4. Users will not transmit classified information designated "NOT RELEASABLE TO FOREIGN NATIONALS" when the display indicates a foreign national has access to the distant terminal (paragraph 3.3.3.2.2).

A2.3. Installation.

A2.3.1. Acoustic Security. Unit commanders must implement a common-sense approach to acoustic security concerns since introduction of the Type 1 terminal into an area must not change those requirements normally implemented in areas conducting classified or sensitive operations. Ideally, all persons assigned to an area where classified work is carried out should have the same clearance. Where this is not possible or practical, implement local procedures to prevent uncleared persons assigned to or temporarily in the area from overhearing classified face-to-face or telephonic conversations.

A2.3.2. Residences/Quarters. The unit commander or equivalent must sign a letter authorizing installation of the STU-III in the residence or quarters of US Government or US Government contractor officials. This authorization also complies with fiscal law guidance concerning the extent of government supported telephone service that may be placed in private residences. In addition, only the designated person uses the instrument, and then only for official purposes. Remove the CIK from the terminal following each use. When not in use, secure the CIK in a General Services Administration (GSA)-approved container. If there is no GSA-approved container, keep the CIK in the personal possession of the user at all times. When the user is sleeping keep the CIK in the same location of credit cards and cash. When you use terminals in the data mode, remove classified information on the screen as soon as possible and do not print out unless there is appropriate classified storage capability. For voice use only, you may key the STU-III to TOP SECRET. For data use, the unit commander must approve in writing the use of CONFIDENTIAL, SECRET or TOP SECRET key. A STU-III located in a residence must not contain a SCI key. The DAO Code for residences/quarters must read:

LINE ONE: USAF 375CG

LINE TWO: SCOTT AFB IL

and have the privilege Class 6 Code 15 “RESDENCE” (NOTE: RESDENCE is an eight digit code, not a word). When taking your STU-III TDY, the DAO Code must read:

LINE ONE: USAF 375CG

LINE TWO: DEPLOYED

NOTE:

These security requirements apply to on and off base quarters and residences, and transient and TDY quarters both on and off base (whether military or civilian).

A2.3.3. Use By Other Personnel. When operationally required, authorized persons may permit others (not normally authorized) to use the keyed terminal (e.g., persons not assigned to the organization identified in the display, persons whose clearance does not meet the level indicated on the display, and foreign nationals) (except as permitted in paragraph **3.3.**) under the following conditions:

A2.3.3.1. An authorized person must place the call and must continuously observe foreign national use.

A2.3.3.2. After reaching the called party, the caller must identify the party on whose behalf the call was made, indicating their level of clearance.

A2.3.4. Use of STU-III Terminals for Data and Facsimile Transmission:

A2.3.4.1. If you connect the terminal to a computer or a facsimile machine, the user organization must contact the base command, control, communications, and computer (C4) systems security

office to discuss computer security (COMPUSEC) and EMSEC issues before doing the connection.

A2.3.4.2. When using the STU-III to secure data and facsimile messages, authorized and appropriately cleared personnel must monitor each end of the circuit to ensure circuit continuity, the STU-III is in the secure mode, and the STU-III preempt feature remains enabled throughout the transmission. Send data only after the sending and receiving parties have observed the terminal display and have assured themselves of the appropriateness of the information transfer (e.g., the sending and receiving organizations are correct and the classification of the data does not exceed the level in the terminal display). Also observe instructions governing document or information control. You may operate the STU-III terminals in an unmanned mode if you use a SACS (see Attachment 8) and you satisfy local security and EMSEC requirements.

A2.3.4.3. Protect a keyed STU-III in an unattended operation at least as well as the data the STU-III protects. A STU-III terminal filled with classified key and CIK inserted must be in an area approved for open storage of classified material at the level of the key.

A2.4. Protecting and Managing CIKs. Terminal procedure requires the creation of at least one CIK immediately following the loading of a KEK into a terminal. If the first CIK created is a master CIK, you may create two additional CIKs. The unit commander must authorize, in writing to the CRO/SRO, if more than two CIKs are required. You can use the master CIK to make additional CIKs in case you lose one, zeroize one, or to make secure calls. You must remove CIKs from terminals when no authorized users are present. Authorized users may keep the CIKs in their personal possession. Additionally, use the following guidelines for protecting and managing CIKs:

A2.4.1. Access. During normal duty hours, you may leave the CIKs in the terminal when authorized personnel are present. This procedure ensures a quick switch to secure mode during a conversation. If authorized personnel are not present, keep the CIKs in the personal possession of an authorized person or store in an approved security container.

A2.4.2. Accountability. The CRO/SRO must locally account for CIKs to minimize unsecure practices associated with their use. Local accounting involves maintaining a record of all CIKs created along with the names and organizations of the persons that have them. The unit or section CROs/SROs will verify annually, as directed by the Base COMSEC manager, that all unit STU-III users still hold their CIKs. Retain this verification until the next verification is accomplished.

A2.4.3. Transportation. Transport CIKs on the person of an authorized user, or if shipped, through US-controlled mail systems, preferably by US registered mail. Always ship CIKs separately from their associated terminals.

A2.4.4. Storage in Office Environments. When stored in the same room as the terminal, store the CIK in a GSA-approved security container. Only authorized STU-III users will have access to the container. You may also store the CIK in another room in a GSA-approved security container (if available). If a security container is not available, store the CIK in a locked cabinet, desk, etc. Include the CIK on the end-of-the-day security check. Determine the adequacy of storage alternatives for the CIK on a case-by-case basis with the unit security manager within each using organization. You may place the CIK on a personal key ring.

A2.4.5. Losses. Promptly report loss of a CIK to the unit's CRO/SRO, who must immediately ensure deletion of that CIK from all associated terminals. In the event of a loss of an unkeyed terminal,

zeroize any associated CIKs where possible. If absence of a terminal prevents erasure of the CIK, protect the CIK at the classification level of the key in the terminal until you:

A2.4.5.1. Find and zeroize the terminal.

A2.4.5.2. Zeroize the CIK by using another terminal.

A2.4.6. Disposition. Once you disassociate a CIK from a terminal (through its erasure or deletion from the terminal, or zeroization of the associated operational KEK in the terminal), you do not need to control the CIK and you may retain it for further use in the same or in other terminals. Ship all excess blank KSDs via US registered mail to EKMS CF, P.0. Box 718, Finksburg MD 21048-0718.

A2.4.7. Master CIK: (1) Each terminal does not require a master CIK. (2) Create master CIKs only when the user has a requirement to do so. A master CIK is required to operate the SACS, when utilizing the "clear data" feature of a STU-III, when updating software in some models of STU-IIIs and when making other CIKs. (3) Store master CIKs in a GSA-approved security container. When master CIKs are in use, the CRO/SRO or user must control them. When you use master CIKs to create additional CIKs, the CRO/SRO must report the new CIKs to the UR.

A2.4.8. Interoperable CIK. Authentication information associated with the interoperable CIK (e.g., organization and clearance level) must represent every person with access to this CIK. If the clearance level varies between terminals, you must clear any person with access to the interoperable CIK to the highest level of the associated key. While use of an interoperable CIK provides users operational flexibility, maintain appropriate accounting and act on losses promptly. Users and CROs/SROs must stay aware of the status of an interoperable CIK, and the location of the terminals, since each terminal may also have other CIKs associated with it. For these reasons, an interoperable CIK should remain at all times in the personal possession of a single individual assigned responsibility for its use.

A2.5. Insecure Practices. The following occurrences are insecure practices (also known as "practices dangerous to security") that you do not need to report to NSA unless there is an indication of espionage or sabotage. Monitor such occurrences and evaluate within each using organization for possible follow-up action:

A2.5.1. If a CIK that had operated properly fails, the CIK or the terminal may have malfunctioned. It could also indicate a copied CIK was used in the terminal. To preclude the possibility of further use in the event of a copied CIK, promptly delete the failed CIK from the terminal (deleting the CIK does not affect the usability of other CIKs created for that terminal).

A2.5.2. Failure to rekey a terminal within a reasonable period of time following the end of the cryptoperiod (e.g., two months).

A2.5.3. Loss of any CIK.

A2.5.4. Transmission of classified information using a terminal whose display has failed.

A2.6. Records Retention. In addition to the normal records you retain for accounting purposes, you must keep certain information to facilitate the automated STU-III compromise recovery mechanism. Maintain the following information for each KEK until you destroy the KEK (e.g., finally zeroized from the terminal or overwritten by a new KEK):

A2.6.1. The identification of the terminal into which each KEK was loaded.

A2.6.2. The identification of all CIKs associated with each KEK, by terminal.

A2.6.3. The identification of all terminals associated with each CIK, by CIK. Maintain this information in any form desired (e.g., recorded on the card accompanying each fill device, or computerized).

Attachment 3

STU-III TYPE 1 KEYING SUMMARY

A3.1. STU-III Keying. STU-IIIs incorporate modern keying techniques that allow the terminals to generate a new traffic key for each secure call. A STU-III user simply places a normal phone call, and if the called party is also using a keyed STU-III, either communicant can convert the call from clear to secure by pressing one button and waiting about 16 seconds. Built-in displays on all STU-IIIs indicate when the terminals are in the secure mode.

A3.2. Initial Keying. Initial STU-III keying consists of inserting a plastic key-shaped storage device, called a KSD-64A, into the terminal (see vendors user guides for complete instructions). The KSD-64A can contain either an operational or seed key. Operational key allows the user to call other keyed STU-IIIs directly, while seed key requires a call to the EKMS CF to obtain operational key electronically via the telephone line. In both cases, the operational key remains valid for up to one year.

A3.3. The CIK. Once the key is loaded into the STU-III, the KSD-64A is converted to a CIK. The CIK serves as a mechanism to enable/disable the security function of a STU-III and is required to be in place before a secure call can occur. Normally, two CIKs are created. You may create up to seven additional CIKs per terminal; however, a unit commander must authorize, in writing, more than two. Normally, STU-III rekeying is performed annually; however, quarterly rekeying is recommended. Accomplish STU-III rekeying by dialing a toll-free or commercial number to the EKMS CF. The CF electronically provides the terminal with new key via the telephone line. Electronic rekey is transparent to the user, and physical replacement of CIKs is not required.

A3.4. The KSD-64A. KSD-64A functions, classification, control accountability, and description of keying material are:

KSD-64A FUNCTIONCLASSIFICATIONCONTROL

Blank KSD-64AUnclassifiedNone

KSD-64A containing seed keyUnclassified CRYPTOALC-1

KSD-64A containing operational keyCRYPTO and classified up toALC-1
TOP SECRET

Crypto-Ignition Key (CIK)UnclassifiedLocally Accountable

A3.4.1. KSD-64A descriptions:

A3.4.1.1. You can convert all KSD-64As to CIKs.

A3.4.1.2. Blank KSD-64A. A KSD not storing key or CIK information.

A3.4.1.3. KSD-64A containing seed key. A KSD used to initialize a STU-III terminal to accept operational key electronically from the EKMS CF.

A3.4.1.4. KSD-64A used as a CIK. Used to lock/unlock a STU-III terminal's secure mode.

A3.4.1.5. KSD-64A containing operational key. A KSD used to load a STU-III terminal with a crypto key (a call to the EKMS CF is not required). Refer paragraph **4.2.3.** for compromise recover instructions.

Attachment 4

QUESTIONS FOR UNESCORTED FOREIGN NATIONAL ACCESS TO STU-III TYPE TERMINALS

A4.1. Doctrinal Requirements for Unescorted Foreign National Access to Type 1 Terminals. This checklist summarizes the doctrinal requirements that apply when determining the appropriateness of unescorted foreign national access to installed Type 1 terminals. Within each category, deny unescorted foreign national access if the answer to any of the questions is "NO." **NOTE:** Refer to paragraph **3.3.3.** for a comprehensive listing of the requirements. The specific paragraph is referenced below with each requirement.

A4.2. Category 1 - Unescorted Access to an Unkeyed Type 1 Terminal.

A4.2.1. Is the risk to US information acceptable? (*Paragraph* **3.3.3.2.1.**)

A4.2.2. Is access required in conjunction with responsibilities normally performed without a US escort? (*Paragraph* **3.3.3.2.2.**).

A4.2.3. Is the CIK protected when US personnel are not present? (*Paragraph* **3.3.3.2.2.**)

A4.3. Category 2 - Unescorted Access to a Keyed Type 1 Terminal.

A4.3.1. Is the risk to US information acceptable? (*Paragraph* **3.3.3.2.1.**)

A4.3.2. Is access required in conjunction with responsibilities normally performed without a US escort? (*Paragraph* **3.3.3.2.2.**)

A4.3.3. Is the foreign national employed by the US Government/US Government contractor or is he/she integrated into and does she/he directly support US operations? (*Paragraph* **3.3.3.2.2.**)

A4.3.4. Is the terminal installed in a US-controlled facility/space (a foreign facility in a country friendly to the US may provide the US with controlled space)? (*Paragraph***3.3.8.**)

A4.3.5. Does the foreign national possess a clearance accepted by the US Government/US Government contractor, equal to the level of the key in the terminal? (*Paragraph* **3.3.3.2.2.**)

A4.3.6. Does the terminal's key identify foreign national access (e.g., US/Foreign)? (*Paragraph* **3.3.3.2.2.**)

A4.3.7. Will the terminal remain US property and is a US citizen responsible for it? (*Paragraph* **3.3.3.3.**)

Attachment 5

QUESTIONS FOR INSTALLING STU-III TYPE 1 TERMINALS IN FOREIGN FACILITIES

A5.1. Installing Type 1 Terminals in Foreign Facilities. This checklist summarizes the doctrinal requirements when installing Type 1 terminals in foreign facilities. Do not install a Type 1 terminal in a foreign facility when the answer to any of the questions is "NO" (except for question number 4). **NOTE:** Refer to paragraph **3.3.8.** for a comprehensive listing of the requirements. Each requirement references the specific paragraph:

A5.1.1. Is the foreign facility in a country that is friendly to the US? (*Paragraph* **3.3.8.3.**)

A5.1.2. Is the purpose of the installation to support US communications? (*Paragraph* **3.3.8.1.**)

A5.1.3. Does at least one US citizen/US resident alien who is permanently assigned to the facility report for work on a regular basis? (*Paragraph **3.3.8.3.2.)***

A5.1.4. Is the terminal installed in US-controlled space? (The answer must be "Yes," if unescorted foreign national access to a keyed terminal is required.) *(Paragraph* **3.3.8.3.3.**)

A5.1.5. If the terminal is not installed in a US-controlled space, is the terminal collocated with the US citizen/US resident alien assigned to the facility? (*Paragraph* **3.3.8.3.4.**)

A5.1.6. If the terminal is not installed in a US-controlled space, is the risk to US information acceptable? *(Paragraph* **3.3.3.2.1.**)

A5.1.7. If the terminal is not installed in a US-controlled space, is the terminal and CIK placed in secure storage or removed from the facility when US personnel are absent longer than 96 hours? *(Paragraph **3.3.8.3.4.)***

Attachment 6

SYSTEM SECURITY GUIDANCE FOR THE MOTOROLA VEHICULAR-MOUNTED STU-III SECURE CELLULAR TELEPHONE (TYPE 1)

A6.1. Systems Description. The STU-III/cellular telephone is a member of the STU-III family and is interoperable with all other versions of the STU-III. This telephone, currently offered by Motorola Inc., combines cellular mobile radio-telephone technology with advanced secure voice/data communications. The unit includes a message center integrated with the standard cellular handset. You can conveniently mount the message center inside a vehicle and provide all STU-III functions including authentication and classification display. The unit also includes a secure cellular terminal (SCT) and a transceiver mounted in the trunk of a vehicle. The STU-III secure cellular telephone operates over cellular phone systems that conform to the advanced mobile phone system specification, that includes the US and a limited number of foreign counties.

A6.1.1. The trunk-mounted SCT provides the security for transmitted information and is the only component of the STU-III secure cellular telephone designated a CCI.

A6.1.2. As a CCI, it is accountable by its serial number according to AFSSI 4001.

A6.2. Systems Security Guidance. The following guidance covers those areas where doctrine is not prescribed but where you need to implement local security measures. Many of the recommended security measures required by other publications are consolidated here as a reminder. These procedures provide guidance for protecting the SCT and the removable components of the STU-III secure cellular telephone in a mobile environment. They do not address countermeasures to protect the vehicle against technical penetration (e.g., "bugging"). Users must understand that, given the current state of technology, any vehicle left in an uncontrolled environment is vulnerable to technical penetration.

A6.2.1. Protection While Unattended. Under most circumstances, locking the vehicle and removing and retaining the CIK and physical keys to the SCT mounting mechanism provide adequate security when the vehicle is unattended. However, if the vehicle is unattended for an extended period (hours or days), depending on the degree of threat of theft or tampering, (e.g., in some overseas areas, or if the vehicle is turned over for commercial repair), first remove the SCT, message center, and handset. Remove the above components from high-targeted vehicles (e.g., vehicles of heads of state or senior government officials), when parking the vehicles in areas where you cannot continuously monitor them.

A6.2.2. Protection While Loading Key. During the loading of STU-III keying material, the operator needs simultaneous access to the SCT and to the message center. To prevent unauthorized access during this process, accomplish key loading only in areas where you can maintain proper control. Immediately following key loading and creation of CIKs, remove the CIK in the trunk-mounted SCT.

A6.2.3. Use of CIKs. The STU-IIIs secure mode is operable when the CIK is inserted in the CIK receptacle either in the trunk-mounted SCT or in the hang-up cup in the interior of the vehicle. For day-to-day operations, users must use the CIK receptacle in the hang-up cup only. Do not use the CIK receptacle in the trunk-mounted SCT for day-to-day operations. Before leaving the vehicle, users must check both the hang-up cup and the trunk to make sure they have removed all CIKs.

A6.2.4. Observation of the Display. STU-III users will give full attention to the display during terminal authentication. Therefore, whenever the driver is placing a secure STU-III call, he/she must not move the vehicle until terminal authentication is complete.

A6.2.5. Protection of User Information. STU-III users must take all necessary precautions to protect classified and sensitive unclassified information, regardless of the environment. Such conversations must not take place unless the user is reasonably certain that the area is secure. Because secure storage is not available in this environment, do not print classified or sensitive unclassified material from peripheral data devices. If users are permitted by their organizations to receive data for viewing only, protect such information and erase from the screen as soon as possible.

A6.2.6. Protection During Emergencies. Using organizations will develop emergency procedures to ensure adequate protection of STU-III secure cellular telephones when used in environments where there is a high probability of overrun (e.g., sudden hostile takeover). During emergencies where time does not allow removal of the STU-III SCT, CIK, message center, and handset, or secure storage is inadequate or impractical, take the following actions, listed in order of priority.

A6.2.6.1. Step 1. Zeroize the STU-III. The STU-III SCT does not have an emergency zeroization capability. Therefore, you must zeroize the SCT by accessing the STU-IIIs program mode when the STU-III is under power. Do not use STU-IIIs without emergency zeroization capability in environments where there is the possibility of sudden hostile takeover because you may lose power to the STU-III or have inadequate time to zeroize the equipment. As a minimum, break the CIK shaft in half.

A6.2.6.2. Step 2. Disconnect the STU-III SCT by unlocking the mounting mechanism in the trunk and unscrewing all connected cables.

A6.2.6.3. Step 3. Disable the STU-III SCT by smashing or hacking it with a heavy instrument such as a hammer or ax.

A6.2.7. Overseas Use. When using STU-III cellular telephones overseas in vehicles that will operate across national borders, accomplish prior coordination with the Department of State or the local US embassy to prevent seizure by foreign customs officials.

A6.2.8. Reportable COMSEC Incidents. Failure to follow the guidelines in paragraph A6.2 is locally reportable within each using organization. The following incidents are reportable according to AFI 33-212:

A6.2.8.1. Physical overrun of a facility/vehicle containing COMSEC material.

A6.2.8.2. Failure to protect the SCT whether it is keyed (CIK inserted) or unkeyed (CIK removed).

A6.2.8.3. Failure to protect STU-III key.

A6.2.8.4. Any loss or suspected compromise of STU-III key.

A6.2.8.5. Any loss of equipment.

Attachment 7

SUPPLEMENTAL OPERATIONAL SECURITY DOCTRINE FOR THE STU-III/A TERMINAL (TYPE 1)

A7.1. General. Operational security doctrine applicable to safeguarding, control, and use of all STU-III family members, including the STU-III/A, STU-III KEK, and associated CIKs, is contained in the basic AFI and**Attachment 2**, which contains additional doctrinal provisions specific to the STU-III/A.

A7.2. Equipment Description:

A7.2.1. The STU-III/A is the STU-III compatible version of the STU-III family. It is a specialized version of the STU-III low cost terminal (LCT) that retains all of the basic STU-III functions and capabilities. Added features include the STU-II BELLFIELD key distribution center (KDC), STU-II net, and STU-III multi-point modes of operation. The STU-III/A has been designed to operate over two-wire and four-wire switched telephone systems in the continental United States (CONUS) and overseas. The STU-III/A provides the means for the US to communicate securely with the North Atlantic Treaty Organization (NATO) and other countries equipped with STU-IIs as well as providing STU-III interoperability with other US forces.

A7.2.2. The STU-III/A is a CCI and is accountable by serial number to a central point (CPSG/ZCK).

A7.3. Keying. There are three ways to key a STU-III/A:

A7.3.1. The first, for STU-III interoperability, uses the normal STU-III keying concept where initial key is produced in a KSD-64A. Accomplish follow-on (rekeying) electronically by a call to the EKMS CF once a year. No per-call access to a KDC is required as is the case with the STU-II. Whenever the STU-III is zeroized, order a new STU-III key.

A7.3.2. The second and third ways for STU-II interoperability use the BELLFIELD KDC concept with per-call access or commonly held net key.

A7.3.2.1. KDC concept. STU-III/A users who have Supreme Headquarters, Allied Powers Europe (SHAPE)/NICS-COA approval to directly connect into NATO's Initial Voice Switched Network (IVSN) must order STU-II unique key (Vu) from the Military Committee for Communications and Information Systems Security Evaluation Agency (SECAN). STU-III/A users who access the IVSN by way of a gateway from national telephone (i.e., public telephone and telegraph [PTT]) services or the US European Telephone System must order STU-II unique key (Vu) from DIRNSA/Y13. Indicate specific connectivity in all STU-Il unique key (Vu) orders.

A7.3.2.2. Net key. Order STU-Il net key (Vn) through the appropriate office.

A7.3.3. The STU-II key is produced in punched tape form (SECRET/NATO SECRET, CRYPTO, and TOP SECRET, CRYPTO). The STU-II key for STU-III/A terminals will be sent only to COMSEC accounts approved to store SECRET or TOP SECRET (as appropriate) keying material. The STU-II key is loaded directly into the STU-III/A using a KOI-18, or using a KYK-13 whose key was loaded from a KOI-18. Once loaded into the STU-III/A, the STU-II net key (Vn) is manually updated on a daily basis; the KDC key (Vu) is <u>not</u> updated.

A7.3.4. When both types of keys (STU-II and STU-III) are loaded into a STU-III/A, the STU-III KEK is loaded first. Create at least one CIK at this time.

A7.3.5. The STU-III/A uses the same type CIK as other members of the STU-III family. A single CIK locks and unlocks the STU-III/A, STU-II, and STU-III secure modes, protecting both types of keys (STU-II and STU-III). The STU-III/A does not use a KYK-71 like the KY-71.

Attachment 8

STU-III DATA PORT GUIDANCE

A8.1. General:

A8.1.1. This attachment provides system security guidance that is essential in determining appropriate security measures to implement when using the STU-IIIs data port. Although this attachment specifically addresses the STU-III data port, the concerns expressed generally apply to the use of the data port on any COMSEC equipment that provides only link encryption (e.g., those without built-in or embedded security protection). When attaching data terminal equipment (DTE) (e.g., computer or facsimile machine to the STU-IIIs data port), the total system must provide protection commensurate with the highest classification level authorized or the clearance level of the facility. The area of procedural security also deserves special attention as the most likely and potentially costly risks are those of human error. Clear, easy to read procedures help to enhance security.

A8.1.2. The basic AFI contains the requirements for protecting a keyed or unkeyed STU-III, after duty hour protection, and EMSEC requirements associated with connecting DTE to the STU-IIIs data port. **Attachment 2** describes how to use the STU-III to maximize COMSEC benefits. It also indicates a need to address COMPUSEC and other system security issues when STU-IIIs are attached to DTEs.

A8.1.2.1. The AT&T 1900 and 1910, Secure Data Devices are voiceless STU-IIIs designed to pass data traffic only and fall under all requirements of a STU-III with full capabilities.

A8.2. Assessing the Application. Information security needs vary significantly among and within organizations. Some installations may require minimal security, while at others maximum security is a primary concern. Due to varying levels of information systems security, using organizations are responsible for implementing security measures relevant to specific applications. The significant diversity of requirements and the wide range of information classification/sensitivity does not make a general solution practical. It is important for users to develop a data port security plan that meets specific organizational needs and also provides a requisite level of security. In developing an appropriate data port security plan, consider the following issues specific to the STU-III.

A8.2.1. Interoperability Concerns:

A8.2.1.1. All STU-IIIs (Type 1 and 2) are interoperable in the secure mode. For applications that need to limit interoperability (e.g., closed-net and system-high operations), you must take additional measures attended operation and/or use of a STU-III with access control features (see **Attachment 7** and **Table A8.1.**, **Table A8.2.**, and **Table A8.3.**).

A8.2.1.2. Since use of the STU-III data port provides a very flexible capability to allow two automated information systems (AIS) to share information, use of the data port makes the user responsible for addressing those security concerns associated with connecting two or more AISs. You must remember the STU-III is designed to prevent disclosure of information in transit only and the end system is still responsible for determining and properly reacting to the accreditation range of the distant end system, the identity of the user of the distant end system, and the STU-III negotiated classification level of the connection. This is particularly important when either end system is not operating in the system-high mode at the same level, or when there is no automated means

for the end system to reliably communicate the above mentioned type of information with the STU-III.

A8.2.2. Terminal Versus User Authentication. Although the STU-III identifies the distant terminal, it does not authenticate the person using the terminal. Therefore, where information sensitivity warrants, using organizations will implement a means to authenticate the terminal user. A STU-III with access control features can help in this process.

A8.2.3. Availability Increases the Need for Training. The US Government and government contractors have purchased unprecedented numbers of STU-IIIs, more than any other equipment in the US inventory. Because of the STU-IIIs wide availability, using organizations must institute or expand existing data security training programs to meet current and future requirements.

A8.2.4. Installation Flexibility Could Increase the Need for Classified Storage. Because of wide deployment possibilities in using STU-IIIs, users must assure appropriate secure storage is available for classified hard copy and/or magnetic/optical media devices on which transmitted information is stored.

A8.3. Countermeasures and Enhancements. The STU-III has a dial-up communications modem which can transmit and receive relatively large amounts of data in a short time. The STU-III provides cryptographic security for the data during transmission. Hardware/software/firmware residing in data devices attached to the STU-IIIs data port must provide data controls where required by STU-III access control features, and also procedural controls. The following countermeasures and enhancements address security concerns. You must consider them along with specific STU-III issues in paragraph 2, this attachment, during development of a data port security plan:

A8.3.1. Ongoing training and education of STU-III/DTE/facsimile users.

A8.3.2. Regular review of STU-III/DTE/facsimile operational procedures, administrative regulations, policies, and day-to-day activities supporting security and safeguards.

A8.3.3. AT&T's STU-IIIs have the capability to program minimum far-end security so you can restrict secure connections to a minimum security level (MINSL).

A8.3.4. Use of dedicated STU-IIIs and dedicated DTEs allows implementation of a more definitive set of security controls.

A8.3.5. Use of system-high DTE operation avoids the risk of mixing security classification levels and transmitting/receiving data between persons/locations that do not have appropriate security clearances. This applies only to STU-IIIs that enforce minimum and maximum security levels (MAXSL), and when the minimum is set equal to the maximum.

A8.3.6. Use of storage media that contains only files intended for transfer can prevent unintentional transmission of information.

A8.3.7. Use of facsimile equipment without store-and-forward capability can help prevent misrouting information. Limiting data and facsimile transfers to a single transaction per session will help prevent misrouting information and avoid inadvertent mixing of security classification levels. When using a STU-III with a facsimile that is usable in either the secure or clear mode, you must invoke security features (i.e., hardware lockout strap or master CIK lockout) to prevent the transmission of classified data in the clear. To ensure the facsimile machine you buy is compatible with the STU-III, make sure the facsimile meets MIL-Standard 188-161C.

A8.3.8. Establishing secure voice contact prior to transmitting data or facsimile provides an additional means of authenticating the person at the distant end. Even when a SACS limit is employed to limit STU-III connectivity, persons having access to the authorized terminals do not necessarily "need to know" the information passed.

A8.3.9. Invoke call-back procedures to enhance the authentication process and counteract the vulnerabilities of operating over a dial-up access telephone line.

A8.3.10. Well-defined procedures and record keeping, coupled with data/facsimile operations conducted only at approved control points, will establish a method for auditing information transfers.

A8.3.11. Install STU-IIIs with lock-down security brackets, hard wired to the telephone company (TELCO) line, or equipped with a tamper resistant TELCO line connector device to limit relocation of a terminal without proper authorization.

A8.4. System Considerations:

A8.4.1. When a STU-III is connected to any computer system, the user must consider all aspects of information security. While a STU-III secured link will protect the data transmission path, you must use COMPUSEC safeguards to prevent improper file transfers, unauthorized access to data bases, etc.

A8.4.2. Protection of the interface between a STU-III and a computer, whether that interface takes the form of human supervision or automated control, is critical to secure operation. Interface concerns include positive control of STU-III functions (e.g., secure versus clear data, unattended answer, access control, etc.) end-system/end-user identification and consistency between data classification levels and STU-III security classification levels.

A8.4.3. Address interface concerns in different ways, depending on the class and type of computer system used. Computer systems are generally divided into two classes, with each class having two modes. These classes are multi-user (e.g., mainframes, workstations) and single user (e.g., personal computer, smart fax). The two modes contained in these two classes are single level (system high) and multi-level (e.g., a system that uses security labels and contains data of varying security classification levels). A description of interface concerns associated with each class and type is provided in the following paragraphs:

A8.4.3.1. Multi-user/single-level. When a STU-III is operated in the remote mode, the host computer's trusted computing base must control the STU-III. Host and user authentication must verify that the proper computer is connected to the STU-III, and the proper user is at the host or computer. Label consistency is necessary between the end system and its STU-III (e.g., the end system must properly understand the session label negotiated by the STU-III). Label consistency is required between end systems in cases where both systems are not operating at the same single level. For example, in cases where the distant system is multi-level, the distant system must know the label of the single-level system and the single-level system know the range of the multi-level system.

A8.4.3.2. Multi-user/multi-level. The host must have control over the STU-III and must have host-to-host and user authentication as stated above. Compare the level of the data and the level of the STU-III link to determine consistency with the data port security policy. Furthermore, the communicating end systems must employ some sort of label negotiation between end systems.

A8.4.3.3. Single-user/single-level. The operator/user is responsible for controlling the STU-III and for verifying the remote user or system by voice recognition or other means. Both end users are responsible for ensuring the classification of the transferred data does not exceed the classification level indicated in the STU-III display.

A8.4.3.4. Single-user/multi-level. The host must know the classification level of the STU-III-to STU-III link, and users will authenticate the distant user/system by voice recognition or other means. Label consistency and negotiation are stated in paragraph A8.4.3.1.

A8.5. Methods/Procedures for Planning STU-III Data Port Use. As an organization develops a data port security plan tailored to its particular application of the STU-III data port, there are certain approaches to assist in establishing an effective plan. These guidelines are outlined below. **Table A8.1.** through **Table A8.3.** are included to facilitate selection of controls for representative security classification applications. Although not all-inclusive, this guidance will help users employ the STU-III data port in a secure manner.

A8.5.1. Develop requirements and justification for choosing the STU-III as a data/facsimile transfer device:

A8.5.1.1. Description of use.

A8.5.1.2. STU-III vendor.

A8.5.1.3. Location of STU-III and DTE/facsimile.

A8.5.1.4. Telephone number/serial number of STU-III.

A8.5.1.5. Type of DTE facsimile to attach.

A8.5.1.6. Classification level for operation (classification level of STU-IIIs contacted).

A8.5.1.7. Diagram of installation.

A8.5.1.8. Networks/systems to access.

A8.5.1.9. Executive level approval of request.

A8.5.1.10. Reasons why the STU-III more effectively meets the requirements than existing data/facsimile transfer devices.

A8.5.2. Develop a written security plan, including operating procedures for connection of a device to the data port.

A8.5.3. Establish an audit mechanism for real-time facsimile transmissions. Suggested elements include:

A8.5.3.1. Security classification level of STU-III connection.

A8.5.3.2. Date/time.

A8.5.3.3. Originator/addressees.

A8.5.3.4. Document classification.

A8.5.3.5. Control number.

A8.5.3.6. Incoming/outgoing category.

A8.5.3.7. Subject.

A8.5.3.8. Operator names/organizations/telephone numbers for both the sending and receiving ends of connection.

A8.5.3.9. Number of pages.

A8.5.3.10. Approval signature.

A8.5.3.11. Receipt verification.

A8.6. Establish formal agreement (e.g., memorandum of agreement) for data communications with external organizations.

A8.7. In the event of a security violation, assess the system and procedures before continuing operation. Notify the computer systems security officer (CSSO) of connected AISs so the CSSO can assess the potential for damage to the connected system.

A8.8. Ensure appropriate controls (e.g., accountability, distribution, storage, and handling) for classification/sensitivity levels send/received are established.

A8.9. Develop appropriate COMPUSEC controls (to include classification and protection of memory devices that have processed classified information) for all information systems and office automation systems connected to the STU-III data port (see AFI 33-212). Establish audit capabilities as described in paragraph A8.5.3 for transmissions via such systems.

A8.10. Summary of Applicable Controls. Table A8.1., **Table A8.2.**, and **Table A8.3.** provide user guidance for typical STU-III data applications. Table A8.1 pertains to the protection of unclassified, sensitive information; Table A8.2 pertains to classified non-SCI applications below TOP SECRET; and Table A8.3 pertains to TOP SECRET and/or SCI applications. These tables feature a matrix that lists applications (e.g., facsimile, system-high and multi-level computers), along with a series of recommendations for mandatory, recommended, and optional controls associated with each application. The various controls listed in these tables are described below:

A8.10.1. STU-III Voice Authentication. A means of orally identifying the distant end user during a STU-III call before a data transfer. Voice recognition is possible based on prior contact and observance of the display. Voice authentication verifies the end user is properly cleared, has a need to access certain information, and verifies the existence of proper controls on the system at the distant end. Voice authentication includes voice recognition when the end user is personally known.

A8.10.2. SCIF. Any physical location (i.e., room, building, or complex) that is authorized for the discussion, processing, and storage of SCI.

A8.10.3. SCI Key. Special STU-III key with additional authentication properties that identifies a STU-III residing in a SCIF.

A8.10.4. Dedicated STU-III. A STU-III connected to a specific data device and not employed for any other purpose than to protect the transmission path between that DTE and a distant terminal.

A8.10.5. AIS Authentication. Assuring that end DTEs are legitimate, usually through the use of system passwords.

A8.10.6. Trusted AIS. An information system that employs sufficient hardware and software integrity measures to allow its use for processing a range of sensitive or classified information simultaneously.

A8.10.7. SACS-MINSL. A special feature of STU-IIIs that incorporate the SACS feature. MINSL allows an authorized user to establish a MINSL that precludes secure mode operation with any distant STU-III not keyed at the selected level or higher.

A8.10.8. SACS-MAXSL. Allows an authorized user of a SACS-equipped STU-III to establish a MAXSL that precludes secure mode operation with any distant STU-III keyed above the selected classification level.

A8.10.9. CSSO. The computer systems security officer is responsible to a designated approval authority, and makes sure security is implemented through the systems design, development, operational, maintenance, and secure disposal stages.

Table A8.1. STU-III Data Port Applications – Sensitive Unclassified.

	FACSIMILE		PC/AIS SMART FAX, ETC.; SYSTEM HIGH		AIS MULTI-LEV-EL		OFF-SI TE HOME/ HOTEL
	Attended	**Unattended**	**Attend-ed**	**Unat-tended**	**At-tended**	**Unat-tended**	
STU-III Voice Authentication	R	N/A	R	N/A	N/A	N/A	R (O if SACS)
SCIF	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SCI Key	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Dedicated STU-IIIs	O	R	O	R	N/A	N/A	O
AIS Authen-ti-cated (Pass-word)	N/A	N/A	O	R	N/A	N/A	O
Trusted AIS	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SACS-MINSL	O	O	O	O	N/A	N/A	O
SACS-MAXSL	O	R	O	R	N/A	N/A	O
SACS-Access Control List	O	O	O	R	N/A	N/A	O
Computer Sys-tems Security Officer	O	O	O	R	N/A	N/A	O

Legend:

M = Mandatory R = Recommended O = Optional N/A = Not Applicable

Table A8.2. STU-III Data Port Applications – Classified (up to and including SECRET).

	FACSIMILE		PC/AIS SMART FAX, ETC.; SYS-TEM-HIGH		AIS MULTI-LEVEL	
	Attended	Unat-tend-ed	Attended	Unat-tend-ed	Attended	Unattend-ed
STU-III Voice Au-thentication	M	N/A	M	N/A	M	N/A
SCIF	N/A	N/A	N/A	N/A	N/A	N/A
SCI Key	N/A	N/A	N/A	N/A	N/A	N/A
Dedicated STU-IIIs	O	M	O	M	O	M
AIS Authenticated (Password)	N/A	N/A	R	M	M	M
Trusted AIS	N/A	N/A	R	M	M	M

SACS-MINSL	O	M	O	M	M	M
SACS-MAXSL	O	M	O	M	M	M
SACS-Access Control List	O	M	O	M	M	M
Computer Systems Security Officer	O	R	O	M	R	R

Legend:

M = Mandatory R = Recommended O = Optional N/A = Not Applicable

Table A8.3. STU-III Data Port Applications – TOP SECRET and/or SCI.

	FACSIMILE		PC/AIS SMART FAX, ETC.; SYSTEM-HIGH		AIS MULTI-LEVEL	
	Attended	Unattended	Attended	Unattended	Attended	Unattend-ed
STU-III Voice Authentication	M	N/A	M	N/A	M	N/A
SCIF	M	M	M	M	M	M
SCI Key	M	M	M	M	M	M
Dedicated STU-IIIs	O	M	O	M	O	M
AIS Authenticated (Password)	N/A	N/A	R	M	M	M
Trusted AIS	N/A	N/A	R	M	M	M
SACS-MINSL	O	M	O	M	M	M
SACS-MAXSL	O	M	O	M	M	M
SACS-Access Control List	O	M	O	M	M	M
Computer Systems Security Officer	O	M	O	M	M	M

Legend:

M = Mandatory R = Recommended O = Optional N/A = Not Applicable

Attachment 9

SYSTEMS SECURITY GUIDANCE FOR A STU-III (TYPE 1) OUTSIDE NORMAL OFFICE ENVIRONMENT

A9.1. Systems Description. Any Type 1 STU-III (portable cellular, Motorola 1500, etc.) used outside the Air Force normal office environment.

A9.2. Systems Security Guidance. The following guidance is provided to cover those areas where doctrine is not prescribed, but where you need to implement local security measures. These procedures provide guidance for protecting the STU-III while in a TDY status or in residence.

A9.2.1. Protection While Unattended. Under most circumstances, locking the door to the room (hotel, motel, dormitory, etc.) or house (residence) containing the STU-III, and removing and retaining the CIK provide adequate security when the STU-III is unattended. You must protect the STU-III as any high value item; therefore, you must use personal judgment on leaving the STU-III unattended, or taking it with you.

A9.2.2. Protection While Loading Key. To prevent unauthorized access during this process, key loading is accomplished only when you can maintain proper physical control.

A9.2.3. Protection of User Information. STU-III users must take all necessary precautions to protect classified and sensitive unclassified information, regardless of the environment. Such conversations must not take place unless the user is reasonably certain the area is secure. Because secure storage is not normally available in this environment, do not print classified or sensitive unclassified material from peripheral data devices. If users are permitted by their organizations to receive data for viewing only, protect such information and erase from the screen as soon as possible.

A9.2.4. Overseas Use. Before taking a STU-III overseas, check with the unit you are visiting to make sure you need to bring it. Some overseas bases have STU-IIIs designated for TDY personnel. If you take a STU-III to an overseas area you must contact the overseas base STU-III support office to make sure you follow all the security rules in place for that area.

A9.2.5. Required STU-III Key. If you take a STU-III on TDY it must contain a deployed key. If you have a STU-III in-residence, the key must identify the location as a residence. Check with your base COMSEC manager to ensure you have the correct key.

A9.2.6. Reportable COMSEC Incidents: See paragraph **5.2.** Report all incidents to the local base COMSEC manager. If in an area with no COMSEC manager present, notify your base COMSEC manager as soon as possible by a secure mode.

Attachment 10

SYSTEMS SECURITY GUIDANCE FOR THE STU-III ACCESS CONTROL SYSTEM (TYPE 1)

A10.1. Description. The SACS terminal is a member of the STU-III family and is interoperable with all other versions of STU-III. The SACS terminal includes all the features of a standard Type 1 STU-III. In addition, the SACS option permits users to establish special, closed communities of interest based on a programmable ACL. Each SACS terminal can be programmed with an ACL containing selected DAO codes and/or specific key material identification numbers (KMID) of all STU-IIIs participating in a net. SACS terminals use information exchanged during each STU-III call setup to identify distant STU-IIIs, terminates calls to/from units whose KMIDs or DAO codes do not reside on the ACL.

A10.1.1. SACS terminals will also allow users to set the minimum and/or maximum security classification programmable straps at which their terminals will interoperate with other STU-IIIs, e.g., a STU-III with its MINSL set to SECRET will terminate secure calls from distant terminals keyed at the CONFIDENTIAL or UNCLASSIFIED level. Calls are also terminated if the near-end terminal is keyed at less than SECRET since the common security level of each call is compared to the MINSL strap. A (MAXSL setting of SECRET will terminate secure calls from distant terminals keyed at the TOP SECRET level.

A10.1.2. You may make entries to the ACL and MINSL/MAXSL via the STU-III keypad, or via the data port from an external data terminal. You can also copy ACL from a SACS terminal on to a blank KSD-64A and then load it into other SACS terminals. To prevent unauthorized manipulation of either the ACL or MINSL/MAXSL settings, a master ClK is required to enable/disable SACS capabilities, and to perform access control entries, updates, and transfers.

A10.1.3. SACS terminals will allow users to limit their STU-III calling community to specific terminals and/or security classification levels. The SACS terminal feature affects secure calls only (voice and data), and does not preclude nonsecure voice use. The SACS terminal, combined with auto-answer, auto-secure, and remote operation features also provides the capability for setting up unattended, secure data networks subject to policy established at each using organization.

A10.1.4. When a SACS terminal is connected to a host computer, two of its standard features may be used to establish an audit trail.

A10.1.4.1. With the terminal's remote control software strap enabled, all of the display information is output connected data terminal. The host can also request a more detailed ID from the SACS terminal at any time. In the remote control mode, the display information is outputted as the terminal receives it, so even if the call is terminated for not meeting the SACS preset conditions, you can record the call information for an audit trail.

A10.1.4.2. With the terminal's "remote authentication" software strap enabled while in the remote control mode, the SACS terminal will output the display information to the connected data device and wait for the device to acknowledge (ACK) or not acknowledge (NACK) the request before completing the secure call setup. You cannot complete the secure call setup if the request is NACKed or the SACS terminal does not receive air ACK or NACK before the timer expires. The host computer can do additional checks on each call during ACK/NACK and record the data for an audit trail.

A10.2. Systems Security Guidance.

A10.2.1. General:

A10.2.1.1. Because the first version of the SACS terminal has only one ACL operating across all key sets, dedicate each SACS terminal of this version to a single application (e.g., with only one KEK loaded, to screen secure voice or secure data calls). Since the new version locks out the other three key sets, the terminal becomes dedicated when the ACL is enabled.

A10.2.1.2. For SACS terminals protecting interactive and receive-only data bases, the MAXSL strap setting must not exceed the classification level of the KEK loaded in the SACS terminal.

A10.3. Key Material Identification Number. Use of KMIDs is the preferred method of identifying terminals on the ACL since each key set ID specifically identifies a single terminal. If the ACL is used, add KMIDs to the list when the number of terminals identified does not exceed the list's capacity (e.g., 500 entries). Users must remain aware; however, that whenever an identified terminal is physically rekeyed, they must change the KMID on the ACL to reflect the KMID of the newly loaded KEK.

A10.4. Department/Agency/Organization Codes.

A10.4.1. When users cannot use KMIDs, they must carefully select the DAO codes to places on the ACL. DAO codes will represent the most specific and restrictive descriptions possible for the particular application. Use of DAO codes for broad descriptions could permit secure access to a larger number of STU-IIIs than desired. Also, when using DAO codes, users must know that terminals with the same DAO code could have different classification levels. Use the MINSL or MAXSL, as appropriate, in conjunction with DAO codes where classification level is important.

A10.4.2. When a STU-III call is received by a digital conference switch, the SACS terminal receiving the call receives and displays the ID information of the digital conferencer, not the actual caller. Therefore, unless the user controls the switch, assign DAO codes placed on the ACL to a conference switch (currently this would affect voice applications only, but could affect data in the future).

A10.5. Access Control List.

A10.5.1. Protect the ACL at the classification level of the information to which the list applies. This includes when the list is loaded in the SACS terminal, on floppy or hard disks, or in KSD-64As. Protect the access control master CIK, which enables/disables the SACS features, against unauthorized access (i.e., removed from the terminal immediately after each use and store it at the highest classification level of the KEK in the terminal).

A10.5.2. Reload the ACL and verify the SACS straps each time the SACS terminal is restored to service, and after removed from storage or out of the control of personnel cleared to the level of the terminal's KEK.

A10.6. Unattended STU-IIIs. When authorized persons are not present, remove the CIK from the terminal and properly protect (see **Attachment 2** and **Attachment 5** for guidance on safeguarding CIKs). It is also recommended to have authorized personnel present at each STU-III to validate display information before transmitting data. NOTE: After-duty-hours' protection of keyed STU-IIIs is discussed below.

A10.7. Unattended Operations. Protect keyed STU-III used in an unattended operation at least to the level of the data it is used to protect. As a minimum, protect a STU-III SACS terminal left keyed after duty hours within an area approved for open storage of classified material to the classification level of the key in the terminal.

A10.8. Connection of a STU-III Access Control Terminal to Data Transfer Equip ment:

A10.8.1. If a STU-III terminal is attached to a DTE (e.g., a computer or facsimile), responsible information protection personnel at base level must address information protection issues.

A10.8.2. "System High" computer systems require setting the MINSL and MAXSL to the same level as the system. Multi-level secure (MLS) systems will set the MINSL and MAXSL to the level of the port to which the SACS terminal is connected. In MLS systems supporting multi-level ports, set the MAXSL and MINSL to the limits of the port. In addition, the host system will incorporate separate identification and authentication procedures for allowing access to the system.

A10.8.3. The display provides information about a site and is used for auxiliary verification and auditing purposes. Since the display does not identify a user, do not use it as the identification and/or authentication process for system access. The SACS terminal provides security for information during transmission only. It does not provide COMPUSEC protection, although the SACS terminal incorporates a number of security features which enhance the user's ability to implement COMPUSEC. Use SACS terminal's security features in conjunction with COMPUSEC protection provided by the host computer.

A10.8.4. If a data system contains both classified and unclassified data, do not use the SACS terminal connected to it in the clear data mode. This will prevent inadvertent transmission of classified data in the clear.

A10.9. Reporting Requirements:

A10.9.1. Failure to follow the guidelines provided by this attachment (except paragraph A10.7) is locally reportable within each using organization.

A10.9.2. Failure to adequately protect an unattended keyed STU-III is reportable according to AFI 33-212.

Attachment 11

SAMPLE TRAINING LIST

A11.1. When the STU-III is in the unkeyed mode, use only for placing unsecure, unclassified calls. Removing the crypto-ignition key (CIK) makes the terminal unkeyed.

A11.2. When the terminal is in the keyed mode (CIK in the STU-III), afford protection commensurate with the level of the key it contains and ensure use only by authorized personnel. When unauthorized personnel are in the area, keep the keyed STU-III under the operational control and within the view of only appropriately cleared, authorized personnel.

A11.3. Pay strict attention to the authentication display to ensure the classification level of the conversation does not exceed the highest clearance classification displayed.

A11.4. To ensure the distant STU-III does not contain expired key, scroll the distant end STU-III as soon as you go secure. If it does contain an expired key, do not discuss classified information. Call the base COMSEC account and identify the distant end.

A11.5. Before discussing classified information on the STU-III, the person making the classified call must make sure all personnel in the area are cleared and have a need to know.

A11.6. Each STU-III user must call the Electronic Key Management System Central Facility (EKMS CF) (Area Code 800-635-6301) once each year to update the STU-III COMSEC key. Recommend you call once a quarter to receive an updated compromise information message.

A11.7. A STU-III not operational 24 hours a day will have the CIK removed at the close of business. Place this action on the end of the day security checklist. Store the CIK 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. If you store the CIK in another room, keep it in a GSA-approved security container. If a security container is not available, store the CIK in a locked cabinet, desk, etc. You may place the CIK on your personal key ring. The adequacy of storage alternatives for the CIK is determined on a case-by-case basis by the unit security manager within each using organization.

A11.8. If you lose your CIK, notify your COMSEC Responsible Officer/STU-III Responsible Officer (CRO/SRO) immediately.

A11.9. The following are reportable COMSEC incidents that you must report to the base COMSEC manager:

A11.9.1. CIK left in STU-III overnight (except 24-hour workcenter or area approved for open storage of classification of STU-III).

A11.9.2. Lost STU-III.

A11.9.3. Lost seed/operational key.

A11.9.4. Unauthorized user making a secure call on a STU-III.

A11.9.5. Secure call completed using expired key.

A11.9.6. Failure of the COMSEC manager to notify the EKMS CF that a seed KEK listed on the conversion notice still exists in his/her COMSEC account.

A11.9.7. Any instance where the authentication information displayed during a secure call is not representative of the distant terminal.

A11.9.8. Failure to adequately protect or to erase a CIK associated with a lost terminal.

A11.9.9. Any instance where the display indicates the distant terminal contains compromised key.

A11.9.10. Keyed STU-III (CIK inserted) left unattended (i.e., no authorized user present for more than five minutes).

A11.9.11. Any instance where the display is inoperative and a secure call is completed.

A11.10. Emergency Procedures. In the event of fire, natural disaster, or covert threat, remove the CIK from the STU-III and secure it or keep it in the personal possession of an authorized individual.

_____

Printed/Typed Name of UserSignature of User

_____

Printed/Typed Name of TrainerSignature of Trainer

(Modify this training list for your location)

Attachment 12

SAMPLE APPOINTMENT LETTER FOR
STU-III RESPONSIBLE OFFICERS AND ALTERNATES

(Letterhead)

DD MMM YYYY

MEMORANDUM FOR (Base COMSEC Account)

FROM: (Office and Address)

SUBJECT: STU-III Responsible Officer and Alternate(s)

1. (Name), (SSN), is the STU-III Responsible Officer (SRO) for (office symbol/duty phone/E-mail address) and cleared to receipt for material up to and including (clearance).

2. The following person(s) is/are Alternate SRO(s). He/She may receipt for material up to (clearance) from (COMSEC Account Number).

NAME:

RANK:

SSN:CLEARANCE:

PHONE:

E-MAIL ADDRESS:

3. Request you train personnel to perform their duties for handling and safeguarding the classified COMSEC material you have assigned to them.

4. This letter supersedes all previous letters from this office on this subject (or give specific dates).

(Commander's Signature Block)