

DEPARTMENT OF THE ARMY
 HEADQUARTERS
 FIFTH U.S. ARMY AND FORT SAM HOUSTON
 Fort Sam Houston, Texas 78234-5000

FSH Pamphlet
 No 25-3

1 February 1990

Information Mission Area
 STU-III DESKTOP SECURITY GUIDE

INDEX

	Paragraph	Page
Purpose.....	1	1
Applicability.....	2	1
References.....	3	1
Abbreviations/Acronyms and Explanation of Terms.....	4	1
General.....	5	1
Responsibilities.....	6	1
Installation.....	7	2
Physical Security.....	8	2
Acoustical Security.....	9	2
U.S. Controlled Space.....	10	3
Using the STU-III Terminal.....	11	3
Troubleshooting Problems.....	12	3
Computer Interface.....	13	4
Vehicles.....	14	5
STU-III Keying Material Requirements.....	15	5
Protecting and Managing Crypto Ignition Keys (CIKs).....	16	6
Transportation.....	17	7
Insecurities.....	18	7
Use by Other Persons.....	19	8
Appendix A: References.....		A-1
Glossary.....		Glossary-0

1. PURPOSE. This guide is an aid to those using the Secure Telephone Unit-third generation (STU-III) at Fort Sam Houston.
2. APPLICABILITY. This guide is intended to provide assistance to Commanders, Security Managers, COMSEC Custodians, and STU-III users.
3. REFERENCES. See appendix A.
4. ABBREVIATIONS/ACRONYMS AND EXPLANATION OF TERMS. Abbreviations/acronyms and definitions of special terms are listed in the glossary.
5. GENERAL. The purpose of the STU-III terminal is to provide a readily available, easy to use, secure telephone capability for all personnel who have a need to discuss and/or transmit classified or sensitive information. The STU-III is designed to counter the greatest security threat to telephone communications--the vulnerability to hostile intercept and exploitation during transmission over the telephone network. Users should be aware that incorrect use of the STU-III terminal and its components may introduce other security concerns which may affect not only their own communications, but the integrity of communications for other STU-III system users as well. The STU-III is a move toward achieving the national COMSEC objective of securing all Government telecommunications processing of classified and sensitive unclassified national defense information. To assist in this objective, all users are encouraged to use the STU-III in the secure mode whenever possible, even during unclassified discussions. This pamphlet is provided to assist in developing and implementing local security measures.
6. RESPONSIBILITIES
 - a. Commanders. Commanders are ultimately responsible for the protection of classified information and property within their command.
 - b. COMSEC Custodian. The USAISC-Fort Sam Houston COMSEC Custodian is the person responsible for the distribution and control of COMSEC keys for STU-III Type I terminals. They must verify that the persons to whom they issue keys hold the proper security clearance.
 - c. Security Manager. A designated individual who provides advice, guidance, and information concerning all security matters.
 - d. Terminal User. STU-III terminal users are responsible for proper use and control of their terminals. Users should be aware of their responsibilities and of the required actions. Terminal users have the following responsibilities:
 - (1) Adhere to the security classification displayed on the terminal for each call.

- (2) Limit terminal access to those with a proper security clearance
- (3) Control Crypto Ignition Keys (CIKs) in accordance with instructions from the USAISC-Fort Sam Houston COMSEC Custodian.
- (4) Users will not perform electronic rekeying annually as this service will be provided by DPTMSEC Security Division.
- (5) Report insecurities to the COMSEC Custodian and Unit Security Manager.

7. INSTALLATION. The following considerations are appropriate prior to STU-III installation:

- a. Confirm that the telephone service jack is a standard six-position modular telephone jack (RJ11, 12, or 13). This jack must be located within 10 feet (3 meters) of the desired STU-III location. The user must submit a Local Service Request (DA Form 3938) to USAISC-Fort Sam Houston for installation of the telephone jack and associated line.
- b. The STU-III user must ensure that power (115/230VAC) is available within 10 feet (3 meters) of the desired STU-III location.
- c. STU-III terminals should be installed by appropriately trained U.S. citizens, or by appropriately trained foreign nationals under continuous supervision by authorized U.S. citizens. The terminals may be installed in U.S. controlled facilities and in residences following specific guidance in FSVS-120, 1 Feb 88, Key Management Plan.

8. PHYSICAL SECURITY.

- a. Office Environment. When the STU-III is installed in an office environment which is not occupied during nonduty hours, the terminal(s) should be secured as a high dollar item; i.e., double barrier protection IAW AR 190-51, and the CIK should be removed.
- b. Residences. The procedure in paragraph 7 above should apply. STU-III terminals installed in a residence can only be used by the person for whom it is installed. All security requirements must be observed for preventing unauthorized access to a keyed terminal and to classified and sensitive information. The CIK must be removed from the terminal following each classified conversation requiring its use and kept in the personal possession of the user or properly stored. If the CIK(s) is stored in the residence and the associated terminal is used to protect classified information, the CIK(s) must be stored in an approved security container.

9 ACOUSTIC SECURITY

- a. The STU-III should only be keyed to the classification authorized for the area which it will be used (i.e., key to Secret in areas approved for Secret discussions, etc.). The introduction of the STU-III terminal into an area should not change requirements for those areas which already process classified or sensitive information.

b. Areas designated for Top Secret (TS) discussion require successful completion of a Technical Surveillance Countermeasures (TSCM) inspection and application of necessary acoustic security measures.

10. U.S. CONTROLLED SPACES. Ideally, all persons assigned to an area where classified work is performed would have the appropriate clearance. Where this is not possible or practical, local procedures must be developed in writing to prevent uncleared persons assigned to, or temporarily in the area, from overhearing classified telephone conversations. Use "Common Sense" if normal conversation can be heard next door--lower your voice and/or install sound proofing. Remember the main threat may no longer be electronic interception, but unauthorized disclosure in the office area(s) containing the STU-III.

11. USING THE STU-III TERMINAL.

a. Users must pay close attention to the authentication information displayed on their terminal during each secure call. The validity of the display is intrinsic to the security of the STU-III system. When two terminals communicate in the secure mode, each terminal automatically displays authentication information of the distant terminal. The information displayed indicates the approved security level for the terminals, but does not authenticate the clearance of the person using the STU-III terminal. Therefore, users should apply judgment in determining need-to-know when communicating classified information.

b. Classified information must not be transmitted when the following conditions exist:

- (1) If there is a question as to the validity of the authentication information on the display, even though voice recognition may be possible. Authentication information should be representative of the organization in which the distant terminal is located.
- (2) When the display indicates that the distant terminal key has expired and the period exceeds 60 days.
- (3) When the display indicates that the distant terminal contains a compromised key. This should be reported as an insecurity to your Security Manager and USAISC-Fort Sam Houston COMSEC Custodian.
- (4) When the display fails to function properly.

c. Users must adhere to the classification level indicated on the terminal display. Because of interaction among terminals of different classification levels, the display may indicate a level less than the actual classification of one terminal's key(s) (e.g., when Secret terminal calls a Confidential terminal, "Confidential" is displayed on both terminals as the authorized level for the call). Therefore, users must observe the display with each call and limit the level of information accordingly.

12. TROUBLESHOOTING PROBLEMS.

a. If the STU-III is unable to complete any call, the user should check the following:

- (1) Is there power to the terminal?
- (2) Is there power to the outlet?
- (3) Is the terminal connected to the telephone system?

(4) Is a dial tone present? If dial tone is not present, notify the USAISC-Fort Sam Houston Telephone Trouble Desk (telephone number 16) and advise of a possible telephone line problem.

b. If the STU-III is unable to make a secure call, check the following:

1) Is the terminal keyed?

(2) Refer to the appropriate STU-III operating guide provided with each STU-III Type I terminal.

c. If following above procedures fails to correct the problem, notify the USAISC-Fort Sam Houston Telephone Trouble Desk (telephone number 16). USAISC-Fort Sam Houston personnel will determine if the problem is being caused by a telephone line failure or instrument failure. Line problems will be corrected; however, if the instrument has failed, the STU-III user is responsible for obtaining repair as follows:

(1) Instrument is still under warranty: The user notifies the appropriate property book officer for return of the instrument to the vendor for repair in accordance with the vendor's instructions.

(2) Instrument is not under warranty: The unit property book officer is notified so drop accountability can be issued and the instrument is returned to Lexington Blue Grass Army Depot.

d. STU-III users are reminded that the STU-III instruments are TDA items and no maintenance floats/spares are authorized. If a high priority instrument fails and has to be shipped out for repair, then the user's unit must replace the instrument with a lower priority instrument. Coordination with the USAISC-Fort Sam Houston COMSEC Custodian must be made prior to relocating STU-III instruments. If there has been a power fluctuation/outage, disconnect the instrument from the power source for approximately one minute, then reconnect to the power source.

e. Insure STU-III is set for "pulse" dialing

13. COMPUTER INTERFACE.

a. Data Mode. When the STU-III terminal is utilized in the Data Mode, each terminal should be manned by authorized users. The data can be sent only after the sending and receiving parties have observed the terminal display and have assured themselves that the information transfer is appropriate (i.e., the sending/receiving party's organization is correct and the classification of the data does not exceed the security level in the terminal display). When a terminal is used in the Data Mode, classified information received must be controlled and protected as required by AR 380-5, as supplemented.

b. Accreditation. If the STU-III terminal is attached to a computer (personal computer, mainframe, etc.), it should be addressed to the appropriate accreditation authority IAW AR 380-380, as supplemented.

c. Facility (TEMPEST) Assessment/Risk Analysis (FTA/RA). Commanders are required to review AR 530-4 for possible TEMPEST countermeasures for their specific operations. Facilities or systems electronically processing classified information that qualify as an exception must process an FTA/RA to determine the appropriate TEMPEST countermeasures. If necessary, this FTA/RA should be forwarded through command channels to Commander, TEMPEST DET MI BN (CI) (T), 902d MI Group, ATTN: IAGPA-A-TD, Vint Hill Farms Station, Warrenton, VA 22186-5126.

14. VEHICLES

a. Cellular STU-III terminals may be installed in vehicles of U.S. Government Officials IAW paragraph 8 above. The Controlled Cryptographic Item (CCI) component of the cellular STU-III terminal is installed in the trunk of the vehicle.

b. Under most circumstances, locking the vehicle and personal retention of the CIK and key(s) 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 (three days or longer), or if vehicle is turned in for repair, it would not be possible to maintain access control. In this instance, the terminal (CCI portion) will be removed from the vehicle.

15. STU-III KEYING MATERIAL REQUIREMENTS.

a. STU-III Key. Keying material should be ordered through your local STU-III User Representative. The key is available at different levels, unclassified through Top Secret (TS), depending upon user needs, clearance, and operating environment. Unclassified through Secret keys require no special justification from the user. Top Secret key is addressed in subparagraph b below.

b. TS Key. Very few of us have a recurring requirement to discuss TS information in our day-to-day operations. Many times STU-III devices are installed within uncontrolled office environments where the discussion of TS information is not acceptable. You should also consider the additional security clearance and other administrative requirements for offices with a TS key.

(1) Any requests for TS key should be fully justified

(2) A required method to control the TS key is to route requests to the Commander/Director through the Security Manager prior to allowing such a key to be ordered.

c. Any TS key currently ordered or on hand without prior written approval should be reordered through the User Representative at a lower classification or justified to their unit's Commander/Director.

d. The following requirements should be considered when determining key requirements:

(1) Top Secret material is not routinely held in office areas. The discussion of Top Secret information in an uncontrolled office environment is an

unacceptable risk. All individuals who would have access to a TS-keyed STU-III and the associated CIK would require a TS clearance. Consider the lowest possible classification level when deciding on a STU-III key. It is strongly encouraged that Confidential be the highest classification level considered for the common office environment.

(2) Keep in mind the Department of the Army (DA) requirement for Two-Person Integrity (TPI) of TS material when considering a key at that level. In all cases, consult your Security Manager concerning the discussion of classified information within the office.

(3) Areas keyed for TS discussion require successful completion of a TSCM and must have acoustic physical security safeguards.

16. PROTECTING AND MANAGING CRYPTO IGNITION KEYS (CIKs).

a. Terminal procedures require the creation of at least one CIK immediately following the loading of a KEK (Key Encryption Key) into the STU-III. Additional CIKs, up to the terminal's maximum (Model Type), can be created at this time; or, if the first CIK is designated as a master CIK, additional CIKs may be created as they are required. Since CIKs permit terminal use in the secure mode, those created for use during normal operations should be protected against unauthorized access and use (i.e., they must be removed from the terminals when authorized persons are not present).

b. Additional control issues include:

(1) Access. Crypto Ignition Keys should be retained by only authorized persons, who should protect them as valuable personal property. Any person who is permitted unrestricted access to the STU-III terminal should retain the CIK on their person or secure it.

(2) Accountability.

(a) Crypto Ignition Keys are accounted for locally and a record of issue must be maintained. All CIKs will be brought under the control of the key custodian and issued to the terminal user. You must ensure that the key custodian is appropriately cleared to have access to the CIK. If necessary, appoint a separate, properly cleared key custodian responsible only for STU-III keys. Master CIKs should not be issued, but stored in a manner similar to security container combinations. Key control custodians should use DA Form 5513-R (Key Control Register) to identify and control all CIKs. Crypto Ignition Keys, like all personally retained keys, must be quarterly inventoried on a "SHOW" basis.

(b) Normal key control procedures, as outlined in AR 190-51, appendix C, as supplemented, generally will suffice; however, common sense must be used.

(3) Multiple Terminal Users. There are a number of methods for permitting multiple users for a terminal. The organization must determine how many people are allowed use of a terminal, which method(s) of multiple use will be allowed, and how many CIKs are required. The methods for supporting multiple users of a terminal are as follows:

(a) Shared CIKs. A CIK can be shared among a number of users; in this way, a CIK can be left in the terminal when it is located in a secure area where no unauthorized person(s) could gain access. For Type I terminals (U.S. Government and Government contractors use only), the CIK could also be locked in a safe to which only properly cleared personnel have access. For Type II terminals (used by any U.S. corporation or individual to protect unclassified information) the CIK may be locked in a desk or file cabinet to which only authorized persons have access.

(b) Multiple CIKs. A STU-III terminal will support up to eight CIKs per key. The identification information will be the same for each of the eight CIKs and any of them can be used to operate the terminal.

(c) Multiple Key Sets. Certain STU-III models offer, as an option, terminals which can be filled with more than one KEK at a time. Each operational key is entered independently and will have its own associated information. As before, there can be up to eight CIKs per KEK stored in the terminal. This method provides a capability to limit a person to a certain classification level and still allows use of the STU-III terminal with keys of other levels of display information.

(d) Multiple Terminals Per CIK. Some STU-III models offer as an option a feature which will allow a single CIK to be associated with more than one STU-III terminal. This feature would require a CIK to be programmed by each terminal with which it is used.

(e) Master CIKs. All STU-III terminals allow programming of up to eight CIKs during the key loading process; some models offer an option to program a Master CIK which can be used to create additional CIKs at a later date. In any case, the total number of CIKs per terminal may never exceed eight per KEK. Master CIKs should be controlled in a manner similar to the combinations to security containers. Loss of the Master CIK is a reportable insecurity.

(f) Disposition. Once a CIK has been disassociated from a terminal (through its zeroization, deletion from the terminal, or zeroization of the associated KEK in the terminal), the CIK is no longer required to be controlled and may be retained for future use in the same or other terminals.

17. TRANSPORTATION. The STU-III must be unkeyed during shipment. In no instance may a seed key or a KEK be included in the same container. The STU-III is a Controlled Cryptographic Item (CCI) and should only be transported as indicated below:

Officially designated courier or unit designated courier service. Such couriers must be U.S. citizens, permanently admitted resident aliens who are U.S. Government civilian employees, or active duty or reserve members of the U.S. Armed Forces. Non-U.S. citizens employed by or in support of the U.S. Government, including employees of U.S. Commercial Carriers, may engage in transportation of STU-III equipments and components; however, specific requirements must be adhered to. You should refer to the specific guidance contained in TB 380-40-22.

18. INSECURITIES. The terminal user should immediately report the following, as indicated.

- a. Loss of a CIK. Report to the activity security manager, who in turn reports such loss to the Security Division, DPTMSEC.
- b. Loss of a STU-III terminal. Report to activity security manager, who in turn reports loss to Security Division, DPTMSEC, and Chief, CIPB.
- c. Leaving a CIK in the terminal when access to the terminal is uncontrolled. Report to activity security manager, who in turn reports insecurity to the Security Division, DPTMSEC.
- d. Any instance where the authentication information displayed during a secure call is not representative of the distant terminal. Notify the activity security manager, who in turn notifies the Security Division, DPTMSEC.
- e. Any instance where the display indicates that the distant terminal contains compromised key. Notify the activity security manager, who in turn notifies the Security Division, DPTMSEC.
- f. Other occurrences defined by the Commander, security manager, or COMSEC custodian will be reported IAW instructions received.

19. USE BY OTHER PERSONS

a. Other Persons. When operationally required, authorized persons may permit personnel not normally authorized to use the keyed STU-III terminal use of the keyed terminal (e.g., persons not normally assigned to the organization identified in the display, persons whose clearance does not meet the level indicated on the display, or foreign nationals), under the following conditions:

(1) The call must be placed by an authorized person. (Use by a foreign national will require continuous presence of an authorized person.)

(2) After reaching the called party, the authorized user must identify the party on whose behalf the call is being made, and the level of clearance of that person.

b. Use by Foreign Nationals. Foreign nationals working within Fort Sam Houston normally should not perform duties that will require the use of a STU-III terminal. This should be a decision made by the Security Manager/Commander/Director.

APPENDIX A

REFERENCES

1. COMMUNICATIONS SECURITY.

a. Confidential AR 380-40, 1 Jun 82, Policy for Safeguarding and Controlling COMSEC Information (U), as supplemented.

b. TB 380-40-22, 16 Dec 85, Security Standards for Controlled Cryptographic Items (CCI).

c. AR 530-2, 15 Jun 84, Communications Security, as supplemented.

2. PHYSICAL SECURITY. AR 190-51, 31 Mar 86, Security of Army Property at Unit and Installation Level, as supplemented.

3. AUTOMATION SECURITY. AR 380-380, 13 Mar 87, Automation Security, as supplemented.

4. MISCELLANEOUS

a. AR 380-5, 25 Feb 88, Department of the Army Information Security Program, as supplemented.

b. Confidential AR 530-4, 1 Apr 84, Control of Compromising Emanations (U), as supplemented.

c. Confidential Interim Change No. IO2, 23 Nov 87, Control of Compromising Emanations (U) to Confidential AR 530-4.

d. Secret AR 381-14, 3 Oct 86, Technical Surveillance Countermeasures (TSCM) (U), as supplemented.

e. FSVS-120, 1 Feb 88, Key Management Plan. Cited document can be obtained from the area User Representative or the Command COMSEC Officer.

f. Message, SAIS-ADS/DAMI-CI, 111242Z Oct 88, subject: Security Procedures for Secure Telephone Unit III. Cited message can be obtained from supporting area User Representative or the Command COMSEC Officer.

GLOSSARYSection I.

CAO - Central Accounting Office. Provides to the COMSEC community complete and centralized accounting and control reports, records, and service for STU-III key.

CCI - Controlled Cryptographic Item.

CIK - Crypto Ignition Key. The device that splits the key in the STU-III terminal so that the STU-III may be left unattended without being zeroized when the CIK is removed. The device CIK is physically a KSD-64A Key Storage Device.

CKL - Compromised Key List. A list of STU-III keys that have been compromised. The CKL is stored in each STU-III terminal to be used during the Compromise Recovery process. Management of CKL is the responsibility of the STU-III KMS (Key Management System).

FSVS - Future Secure Voice System. The STU-III family of secure voice terminals and the supporting key management structure.

FTA/RA - Facility TEMPEST Assessment/Risk Analysis.

HQ - Headquarters

KEK - Key Encryption Key. Key used to encrypt another key when being securely distributed.

PCO - Publications Control Officer

TPI - Two Person Integrity

TS - Top Secret

TSCM - Technical Surveillance Countermeasures.

UR - User Representative. An individual designated by the command authority to order STU-III key for an organization.

USAG - United States Army Garrison

GLOSSARY

Section II.

COMSEC - Communications Security; protective measures taken to deny unauthorized persons information derived from the telecommunications of the U.S. Government or its contractors.

KSD-54A - Key Storage Device. A black plastic key with a programmable read-only memory (PROM). KSD-54A can be maintained in three ways: (1) Fill Device (can be loaded with operational or seed key); (2) Crypto Ignition Key (CIK); (3) Blank.

SEED - Seed Key. Key that can be electronically rekeyed.

STU-III - Secure Telephone Unit-third generation. A family of low-cost, user-friendly secure telephones that operate over the public switch network. The STU-III, in most cases, can replace a standard business telephone since STU-IIIs provide a secure voice capability, in addition to standard telephone features.

TEMPEST - An unclassified short name referring to investigations and studies of compromising emanations. The term "TEMPEST," as commonly used in the Army, is synonymous with emission security and control of compromising emanations.

TYPE I - STU-III Type I terminal or key used by the U.S. Government and Government contractors to protect classified or unclassified national security related information (unclassified-TS).

TYPE II - STU-III Type II terminal or key used by any U.S. Corporation or individual to protect unclassified national security related or privacy information.

The proponent of this memorandum is the Directorate of Information Management. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, U.S. Army Garrison, ATTN: AFZG-IM, Fort Sam Houston, Texas 78234-5000.

FOR THE COMMANDER:



GEORGE A. FINLEY
Director of Information Management

GEORGE A. FINLEY
Director of Information Management

DISTRIBUTION:
A
25 - AFZG-IM-LSBP