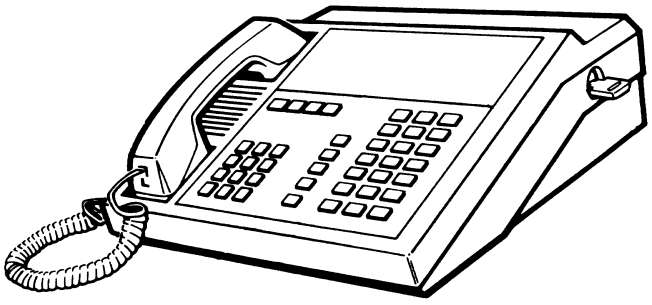
Department of Defense Security Institute

STU-III

HANDBOOK

FOR

INDUSTRY



February 1997

ACKNOWLEDGMENTS

The Department of Defense Security Institute thanks the National Security Agency and the Defense Investigative Service for their assistance in the development of this handbook and gratefully acknowledges the contributions of these individuals:

Mr. Bruce Blake	Mr. David Kendrick
Mr. Bud Bowers	Ms. Otelia Rice
Mr. James Jones	Mr. Mike Williams
Mr. Melvin Kearney	Ms. Pat Wyatt

ABBREVIATIONS

AIS	Automated Information System
CAO	Central Accounting Office
CAGE	Commercial and Government Entity
CAP	Contractor Acquired Property
CCI	Controlled Cryptographic Item
CIK	Crypto Ignition Key
CIM	Compromise Information Message
CKL	Compromised Key List
COMSEC	Communications Security
COP	Contractor Owned Property
COR	Central Office of Record
DAO	Department/Agency/Organization
DCS	Defense Courier Service
DIS	Defense Investigative Service
DoD	Department of Defense
DoDSI	Department of Defense Security Institute
EKMS	Electronic Key Management System, Central Facility
FAR	Federal Acquisition Regulation
FSO	Facility Security Officer
FSVS	Future Secure Voice System
GFE	Government Furnished Equipment
GFP	Government Furnished Property
HR	Hand Receipt
IS	Industrial Security
ISM	Industrial Security Manual, DoD 5220.22-M
KCN	Key Conversion Notice
KMID	Key Material Identification Number
KSD	Key Storage Device
NACSI	National Communication Security Instruction
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
POTS	Plain Old Telephone System
SOCA	STU-III Only COMSEC Account
SPP	Standard Practice Procedures
STU-III	Secure Telephone Unit, Third Generation, Type 1

CONTENTS

INTRODUCTION

Secure transmissions – whether telephone conversations, facsimile (fax) copies, or automated information systems (AIS) communications – have long been possible through encryption, but for many years the equipment was bulky, complex, and expensive. In the 1960s the KY-3, one of the first practical voice encryption devices, came on the market. In 1970, the Secure Telephone Unit, First Generation (STU-I) was launched, followed in 1975 by the STU-II, which mustered some 10,000 users.

In 1984, the **National Security Agency** (**NSA**) initiated the **Future Secure Voice System** (**FSVS**), an aggressive, accelerated program to button up US voice communications by the end of the 1980s. In fact, the **Secure Telephone Unit, Third Generation** (**STU-III**) was developed and produced by 1987. To ensure widespread use, the STU-III was designed to be about the size of a conventional telephone desk set, user-friendly, and relatively low-cost (the goal was $2000).

In 1986, **National Communication Security Instruction** (**NACSI**) **6002**, "Protection of Government Contractor Telecommunications," was issued requiring defense contractors to transmit classified information and sensitive unclassified information solely over encryption equipment approved by the NSA. In 1987, the NSA-approved STU-III placed secure telephone service within the reach of nearly every defense contractor.

AT&T, GE (formerly RCA), and Motorola are the vendors for the STU-III. The **Type 1 terminal** is used to secure classified information and unclassified but sensitive information. All STU-IIIs are compatible, so if you obtain a STU-III from, say, GE it can "go secure" with a STU-III made by Motorola or AT&T. The **Type 2 terminal** is used to secure unclassified communications only.

We developed this handbook to assist **Facility Security Officers** (**FSOs**) of cleared defense contractors who require the STU-III, Type 1 unit. It covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations. It summarizes and synthesizes directive guidance for the STU-III to supplement, not replace, such guidance. *This guidance does not apply to the Type 2 terminal.*

ASSESSING YOUR NEEDS

First, determine which contracts will require STU-III, Type 1 access. As a rule of thumb, you should count all of your classified contracts in the total. Secure telecommunication via STU-III will improve your facility's performance on virtually any classified contract.

Work with your facility's top management to ensure that the contracting officer for each classified contract inserts a statement of the requirement for protecting the telecommunication of classified information (and unclassified national security-related information).

You will also need to know the highest classification level involved for each contract, so that telecommunications can be safeguarded at that level. Then determine how many STU-III terminal users there will be for each contract.

TERMINALS

Now is not too early to consider where you will put the STU-III equipment. In choosing locations, remember that in a cleared facility STU-III terminals must be installed only in private offices or work areas where access to the STU-III may be controlled in keeping with the requirements to protect **Controlled Cryptographic Item (CCI)** equipment. A CCI, such as the STU-III, must be safeguarded as a *high-value item*, that is, as though it were a computer.

Will STU-III equipment be used in applications besides in-facility telephone terminals? You may need to use a STU-III for secure facsimile (fax) or AIS transmission. Perhaps there is a need for a cellular unit installed in a vehicle. Someone may need to use a STU-III at a residence. Take all of these uses into account from the outset.

Once you have drawn up a list of the STU-III applications at your facility, you can decide how many STU-IIIs you will require by type (e.g., single-line or five-line desk unit; cellular unit; mobile/ portable/ transportable unit).

KSD-64As, KEY, and CIKs

Next you need to decide how many KSD-64As you will need. Each STU-III comes with one blank KSD-64A.

KSD-64A stands for Key Storage Device with storage of 64,000 bits of information. The device is a key-shaped piece of plastic that contains a computer chip called an EEPROM. The EEPROM chip has Electronically Erasable Programmable Read Only Memory. The device is inserted like a key into a slot in the STU-III and turned to engage its computer chip with the electronic components of the STU-III. Since the KSD-64A is an EEPROM, NSA can use its special equipment to program it, erase the information it contains, and reprogram it with other information.

Key Storage Device, KSD-64A

It is incidental, even confusing perhaps, that the KSD-64A is key-shaped. It is in fact named for the cryptographic information, called "key" by security professionals, that it often stores. "**Key**" is a unique sequence of random bits used to set up and change the encoding and decoding function of a security device so that it can encode, decode, and authenticate information. It is this meaning of "key" that is used in the following terms:

SEED KEY - Key that is loaded into a STU-III terminal, enabling it to electronically obtain its operational key during a rekey phone call.

OPERATIONAL KEY - Key that is loaded into a STU-III terminal, enabling it to make direct secure calls to other STU-IIIs.

The KSD-64A may also function as a CIK:

CIK - A KSD-64A that stores an electronic "password." The CIK is inserted and turned in the STU-III terminal that shares this "password" to unlock the terminal's secure transmission features. The secure mode is locked when the CIK is removed. CIK stands for Crypto Ignition Key.

A particular KSD-64A is commonly referred to by the type of electronic information it is storing at the time. A KSD-64A that is used to transport and transfer seed key to a STU-III unit is called a "seed key." A KSD-64A that is used to transport and transfer operational key to a STU-III unit is called an "operational key." A KSD-64A that contains an electronic "password" is called a "CIK."

Note also that when a KSD-64A is used to transport and transfer either seed key or operational key, it is referred to as a **fill device**. It will "fill" the unkeyed STU-III with key; when, in addition, a CIK has been created and is inserted in the unit, the STU-III is said to be **keyed**.

The **Electronic Key Management System, Central Facility** (**EKMS**) generates and distributes all key used by STU-IIIs. The EKMS prepares customized key by combining user-specified ID information and NSA-generated cryptographic information. After the EKMS has generated the customized key, it assigns to it a unique **Key Material Identification Number** (**KMID**). The customized key, referred to as the terminal's key, is then loaded into a fill device. A card label attached to the fill device identifies the key contained in the device. The fill device is then shipped to a **COMSEC account** (COMSEC = Communications Security), where it is officially received and provided to an individual authorized to key the STU-III terminal (i.e., to load the key into the terminal).

A fill device may be used just once to transfer key; after the transfer the fill device is empty or blank. A KSD-64A or a STU-III that does not contain key is said to be **zeroized**; a button at the rear of the unit (Motorola and RCA/GE) or on the bottom of the unit (AT&T) is used to zeroize the STU-III. A fill device is required to key the STU-III only during initial setup and later on to rekey the STU-III after it has been zeroized (for instance, to change its ID information).

A STU-III into which operational key has been transferred (loaded) is ready to operate in the secure mode. However, a STU-III unit into which seed key only has been loaded must have its seed key converted to operational key before it can go secure. The STU-III user initiates this conversion by placing a call to the EKMS. ***During this call, the EKMS electronically converts the seed key in the STU-III to operational key.***

During this call, the EKMS also downloads the latest **Compromise Information Message/Compromised Key List** (**CIM/CKL**) into the STU-III. When NSA determines that a possible compromise has occurred, it places the number of the compromised key (its KMID) onto the CKL. Updates to this list are provided in a CIM, which is exchanged automatically between the STU-III terminals during the setup, or **handshake**, for a secure call. If the KMID of a STU-III terminal is on the CKL, no other STU-III terminal can establish secure communications with it.

Since operational key enables a user to make a secure call without having to be converted, it is more vulnerable to compromise than seed key. For this reason, NSA prefers *not* to transmit to STU-III users fill devices containing operational key. We will include operational key in what follows, but *unless there are special circumstances at your facility, only "seed keys" should be ordered.*

KEYSETS

Determine how many keysets of each STU-III unit will be needed. A **keyset** consists of a combination of "key" and user ID data. The number of keysets that are available within a STU-III differs by vendor, as shown:

VENDOR	KEYSETS PER STU-III
AT&T	4
GE/RCA	3
Motorola	2

Only one keyset is needed per STU-III, unless some users have a different clearance level and/or need-to-know than other users of that STU-III. If more than one keyset is needed, a separate seed key (or operational key) with its own identifying information must be obtained for each keyset you establish within the STU-III. For each keyset, the STU-III terminal can create a **master CIK**, which will permit you to enable and disable some security functions of the STU-III and to create additional CIKs in the future as needed. With all of the STU-III models, up to 7 CIKs can be created per keyset if a master CIK is also made; otherwise, up to 8 CIKs per keyset can be created. *The CIKs that enable a given keyset (designated for secure use at a particular classification level and with a particular need-to-know) within the STU-III will not enable any other keyset.*

Once you know the number of keysets you will be using, you also know the minimum number of seed keys [and/or operational keys] that will be required. Bear in mind, however, that you may wish to order duplicate fill devices from the EKMS, so that they will be on hand to refill the STU-III if you have to zeroize it (or if an employee zeroizes it by accident).

You will also need to decide whether to create one or more master CIKs. That is, for each keyset to be established, you must determine whether:

1. No master CIK need be created,

2. A master CIK will be created only to enable/disable some security functions of the STU-III, then zeroized, or

3. A master CIK will be created and retained to create additional CIKs in the future as needed. *In this case, the facility must have storage capability at the level of the seed key's conversion classification level or a higher level.*

Next, determine how many regular CIKs will be needed. Will you issue a CIK to each STU-III user? Or will you have only one or a few CIKs for each keyset, available for common use?

Once you know your needs — keysets per terminal, CIKs per keyset, fill devices (seed key/operational key) per keyset, and the number of terminals by type — you are ready to obtain your STU-III equipment.

METHODS OF OBTAINING TERMINALS

Next, you need to settle on the method of obtaining the STU-III, Type 1 equipment. The contractor (your company) and the contracting officer negotiate agreements that govern how the costs of the STU-III capability will be treated under existing or new contracts that require the securing of telecommunication of classified information or unclassified but sensitive Government information.

There are three main methods of obtaining a STU-III terminal, as follows:

GFE A US department or agency, normally the User Agency for the contract, purchases the STU-III equipment and provides it to the contractor as **Government Furnished Equipment** (**GFE**). The government provides disposition of the equipment at the conclusion of the contract. The STU-III equipment may also be obtained as GFE under the **NSA/DIS Loan Program**, under which the Defense Investigative Service has loaned out approximately 5,700 STU-IIIs to NSA-approved contractors. Under this program, a contractor may retain the STU-III as long as a classified contract is maintained. Then the government handles disposition.

CAP Upon authorization of the contracting officer, the contractor may purchase the equipment from a vendor and charge it to the contract as **Contractor Acquired Property** (**CAP**). CAP is owned by the government, which handles disposition at the end of the contract.

COP Subject to an administrative determination by NSA that the contractor is eligible from a security viewpoint to own the equipment, the contractor may obtain it from a vendor as plant equipment as defined in the *Federal Acquisition Regulation*, 48.101(a). The equipment becomes **Contractor Owned Property** (**COP**). The contractor may recover the cost as for other plant equipment overhead. Only companies organized and existing under the laws of the US and Puerto Rico may acquire the STU-III as COP. *(See COMSEC Supplement to ISM, Section V, para. 32b.)*

Once a STU-III has been obtained as GFE, CAP, or COP, it may be redistributed to a subordinate entity, such as a division or subsidiary:

HR The STU-III is provided on a **hand receipt** (**HR**) by a home office, parent company, or some other entity which will execute the STU-III COMSEC requirements.

If the contractor is to acquire the STU-III equipment directly, i.e., under CAP or COP, send a letter to the **NSA Central Office of Record** (**NSA COR**) at this address:

National Security Agency
Operations Building Nr. 3
ATTN: Y131
9800 Savage Road
Fort George G. Meade, MD 20755-6000

If CAP, provide in the letter:

A request for eligibility to directly procure the STU-III equipment.

- The contract to which the STU-III equipment will be charged.
- The type of STU-III unit (e.g., single-line or five-line desk unit; cellular unit; mobile/portable/transportable unit) to be acquired.
- The location(s) where the equipment will be installed.
- The Contracting Officer's Authorization to Purchase form.
- If a COMSEC account is in place at the facility, or if an existing COMSEC account is available to support the requirement, so state. If not, state that the facility will initiate a request for the establishment of a COMSEC account with NSA.

If COP, provide in the letter:

- A request for eligibility to procure the STU-III equipment as plant equipment.
- A statement that the facility desiring to own the STU-III equipment is performing or will be performing under a US Government contract at the time of the STU-III equipment delivery.
- The requesting facility's CAGE code.
- The full name, address, and CAGE code of its corporate headquarters or parent company, if any.
- If a COMSEC account is in place at the facility, or if an existing COMSEC account is available to support the requirement, so state. If not, state that the facility will initiate a request for the establishment of a COMSEC account with NSA.

NSA will determine the contractor's eligibility to procure the STU-III equipment and will notify the contractor in writing. The contractor will be required to execute a **CCI Control Agreement** with NSA.

How you obtain your STU-III determines whether your facility will need to execute a CCI Control Agreement and have a COMSEC account, as the chart shows.

DO YOU NEED A CCI CONTROL AGREEMENT/COMSEC ACCOUNT?

YOUR STU-III OBTAINED BY:	CCI CONTROL AGREEMENT?	COMSEC ACCOUNT?
GFE	NO	YES
CAP	YES	YES
COP	YES	YES
HR	NO	❷

Under the NSA/DIS Loan Program, a Memorandum of Loan Agreement is required.

❷ Required only when the facility has to obtain its own key.

If your organization is obtaining the STU-III equipment under CAP or COP, it must execute a CCI Control Agreement with NSA. If you do not have a blank CCI Control Agreement, obtain one from:

- Your DIS Field Office
- NSA COR
- *COMSEC Supplement to ISM*, Appendix 3

If your organization is obtaining the STU-III equipment as GFE under the NSA/DIS Loan Program, it must execute a **Memorandum of Loan Agreement**. If a COMSEC account is in place at your facility, or if an existing COMSEC account is available to support the requirement, well and good. If not, you will need to initiate a request for the establishment of a COMSEC account with NSA.

COMSEC ACCOUNT

A COMSEC account is "an administrative entity identified by an account number, responsible for maintaining custody and control of COMSEC material." Simply put, NSA or some other governmental agency will establish an accountability system for your COMSEC equipment (STU-III) and other necessary material (key) and will assign a 6-digit number to the account.

As the chart above shows, a COMSEC account is required unless your facility is receiving both the STU-III and the key under a hand receipt issued by another entity, such as a home office. In this case your facility is using the COMSEC account of the other entity, which is assuming the accounting responsibilities. If, however, the STU-III comes to your facility on a hand receipt ***and if*** you are instructed to obtain the key on your own, then you must establish a COMSEC account with NSA.

If your contract or the instructions you have received indicate that the STU-III and key are the only COMSEC material needed, you will be applying for a **STU-III Only COMSEC Account (SOCA)** . If you have been told that you will need additional COMSEC equipment, such as a KG-84 or KG-94, then you must obtain a *regular COMSEC account.*

In applying for the COMSEC account, you need to nominate to NSA the persons who will serve as **COMSEC Custodian** and **Alternate COMSEC Custodian.** If the key is at, or will convert to, the SECRET level or below, they must have final SECRET clearances. If the key is at, or will convert to, the TOP SECRET level, they must have final TOP SECRET clearances. When applying for a *regular COMSEC account*, the investigative basis for each clearance (investigation or periodic reinvestigation) must fall within the past 5 years.

To apply for the COMSEC account send a letter to the NSA COR at the following address:

National Security Agency
Operations Building Nr. 3
ATTN: Y131
9800 Savage Road
Fort George G. Meade, MD 20755-6000

Include in the letter:

- The facility name, address, facility clearance level, and cage code.
- The purpose of the COMSEC account.
- The number of a current contract that the STU-III will support (attach a copy of the "DoD Contract Security Classification Specification," DD Form 254).
- A statement that the facility will require a STU-III and a seed key that will be converted to the (CONFIDENTIAL/SECRET/TOP SECRET) classification level.
- The physical address where the account will be located.
- The CCI shipment address, if different from that provided above.
- A statement that the unit will or will not be installed in a Sensitive Compartmented Information Facility (SCIF).
- Identifying data for the individuals nominated for the positions of COMSEC Custodian and Alternate COMSEC Custodian. The information on each must include: name, social security number, date of birth, place of birth, date and level of security clearance, date of investigative basis for clearance (for regular COMSEC account), and office telephone number.
- The name, social security number, and business telephone number of the FSO.
- A statement that a current "Certificate Pertaining to Foreign Interests," DD Form 441s, has been completed and is on file with DIS.

Send a copy of the letter to your **DIS Field Office**.

If your method of obtaining the STU-III equipment is CAP or COP, attach a copy of the CCI Control Agreement executed by your organization to the letter sent to the NSA COR.

When the NSA COR has reviewed your documentation, they will respond to you by letter, with a copy to the DIS Field Office. The letter will confirm the establishment of the COMSEC Account, the assignment of the 6-digit account number, and the appointment of the COMSEC Custodian and Alternate. The letter will include a copy of the CCI Control Agreement you forwarded, now also executed by NSA.

COMSEC CUSTODIANS

The COMSEC Custodians are responsible for the accounting, handling, and disposition of all key for your STU-III terminals. They must verify that the persons to whom they issue key have an appropriate security clearance and need-to-know and that STU-III users follow your Standard Practice Procedures. Requirements and procedures for COMSEC Custodians are detailed in Section III, para. 18, of the *COMSEC Supplement to the ISM* and in Section 8 of the *STU-III Key Management Plan*.

If you (the FSO), the COMSEC Custodian, and the Alternate COMSEC Custodian have not received a COMSEC briefing by a government representative, arrange for your DIS IS Representative to give the briefing. Also, if the COMSEC account will receive COMSEC material besides STU-III material, you must arrange for the COMSEC Custodian and the Alternate to attend the **NSA CS-140 COMSEC Custodian Course**. However, even if your account is a SOCA, we recommend that the COMSEC custodians take this course.

Once your COMSEC account is in place, the NSA COR will send a copy of **National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3013**, "Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal" and its annexes. However, if other INFOSEC policy documents are needed for contract performance, the contractor must request the User Agency contracting officer to provide the documents as Government Furnished Property (GFP).

For further guidance, have the COMSEC Custodian obtain the following:

From DIS:

- *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M.
- *COMSEC Supplement to ISM, DoD 5220.22-S*.

From NSA:

- *INFOSEC Bulletins*.

From EKMS:

- *STU-III Key Management Plan*, EKMS-702.01.
- *STU-III Keynotes / EKMS Keynotes*.

COMMAND AUTHORITY

Next, nominate to the EKMS a person to serve as the **Command Authority**. The three responsibilities of the Command Authority are:

1. To establish **Department/ Agency/ Organization (DAO) descriptions**, which will become part of the customized key issued by the EKMS and part of the identification displayed in the message window of the distant STU-III during a secure call.

2. To select and register the **User Representative**, indicating appropriate "privileges," which include:

   - The DAO descriptions for which the User Representative can order key.
   - The types of key that the User Representative can order.
   - The security classification of the key.

3. To monitor and maintain the accuracy of the User Representative information on file at the EKMS.

Send the Command Authority appointment letter to:

EKMS Central Facility
P.O. Box 718
Finksburg, MD 21048-0718

The appointment letter must:

- Be on corporate letterhead stationery.
- State the person's name and title (if any).
- State the person's business address and phone number.
- Be signed at the corporate level.
- Be embossed/stamped with the corporate seal.

After the EKMS has processed your letter, it will send letters confirming the appointment of the Command Authority to both the contractor and the Command Authority, as a double check to detect any data entry errors or attempts to make unauthorized appointments.

USER REPRESENTATIVE

Besides the confirmation letter, the EKMS will send the Command Authority a package of information that includes the "User Representative Registration Form." The Command Authority can then appoint and register the User Representative. (See Section 6 of the *STU-III Key Management Plan*.) Note that in a small organization one person may serve as COMSEC Custodian, Command Authority, and User Representative. The User Representative's responsibilities are:

1. To determine requirements for key within the organization,

2. To interact with the Command Authority for DAO administration and User Representative privilege changes,

3. To prepare and submit key orders to the EKMS, and

4. To monitor the status of key orders.

Responsibilities and procedures for the User Representative are detailed in Section 7 of the *STU-III Key Management Plan*.

After the EKMS has processed the registration form, they assign the User Representative a 6-digit identification number to use when ordering key. As with the double-check confirmation of the Command Authority appointment, the EKMS will send letters confirming the registration of the User Representative to both the Command Authority and the User Representative to detect any data entry errors or attempts to make an unauthorized registration.

When the registration of the User Representative is confirmed, ensure that an approved contractor employee –– such as you (the FSO), the COMSEC Custodian, or the Alternate –– gives a COMSEC briefing to the User Representative.

Next, ensure that the Command Authority and the User Representative check the information (registration data and ordering privileges) entered on the "STU-III User Representative Key Ordering Authorization Form" sent to them by the EKMS. The User Representative keeps this form for use when ordering key.

ORDERING KEY

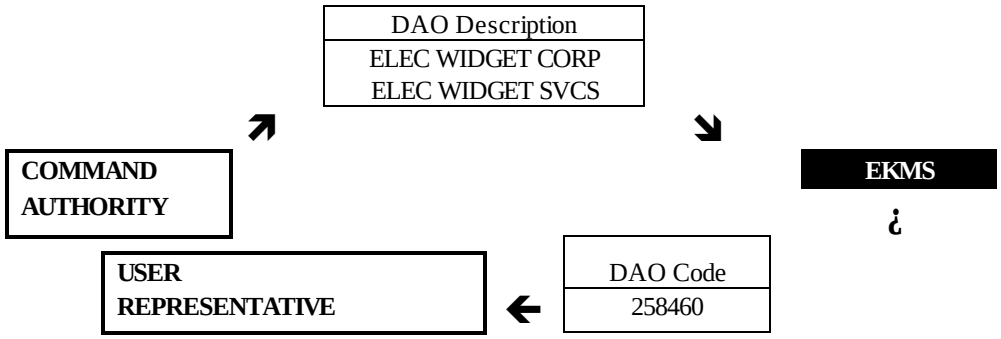
Recall that each STU-III terminal stores certain user-specific identification information and displays this information during a secure call. The display is critical because each party uses it to authenticate the distant party. For this reason, the identification information is also referred to as "authentication data." There are two parts to the identification: the ***DAO description*** and the ***Additional Identification Data*** ("free form" information).

The Command Authority defines the DAO description, which specifies the terminal user's parent *department, agency, or organization*. The DAO description may be one or two lines:

① The first line of a contractor's DAO description is the name of the US Corporation or other legal entity for which the Command Authority is appointed (e.g., Electric Widget Corporation). This line is displayed on the terminal of the distant party throughout a secure call.

A second line can be used to show location, division, or staff element (e.g., Electric Widget Services). It is displayed briefly to the distant user during the secure call setup.

The Command Authority supplies the DAO description as part of registering the User Representative. The EKMS then assigns a unique 6-digit number (the ***DAO code***) to the DAO description. The User Representative uses the DAO code when placing an order for key.



To order the required seed key(s) [and/or operational key(s)], the User Representative must do the following:

- *Define the key order.* (See Section 7.3.1 of the *STU-III Key Management Plan*.) The key order should be submitted ***about four weeks before the user will receive the STU-III terminal*** to ensure that the key is available when the STU-III is installed.
- *Complete the STU-III Key Order Request.* First, enter the DAO code on the order form. (The EKMS provides the assigned DAO code(s) to the User Representative through the "Key Ordering Authorization Form.") The EKMS will translate the DAO code on the order form back to the DAO description in its database and use the description as the first part of the authentication data of the STU-III key.

The User Representative next enters the second part of the user identification: the Additional Identification Data, or "free form" information. The STU-III user determines this information, such as a specific location, section, position (title), or project, even the user's name, and notifies the User Representative. In all, three lines are available for authentication data. If the Command Authority has already specified a two-line DAO description, then there can be only one line of free form information:

ELEC WIDGET CORP	DAO Description
ELEC WIDGET SVCS	DAO Description
LASER WIDGET	Additional Identification Data

If the Command Authority specifies only a one-line DAO description, there can be up to two lines of free form information:

ELEC WIDGET CORP	DAO Description
LASER WIDGET	Additional Identification Data
CHIEF ENGINEER	Additional Identification Data

- *Submit the STU-III Key Order Request.* (See Section 7.2 of the *STU-III Key Management Plan*.)

- *Notify the COMSEC Custodian to expect delivery of key*. The User Representative should notify the COMSEC Custodian to expect delivery of the key so that it may be processed and distributed upon arrival. The best way of doing this is to provide a copy of the key order to the COMSEC Custodian, who can use the copy to verify that the received key matches the ordered key.

- *Check the Confirmation/Rejection Notice*. Before long, the EKMS will mail to the User Representative a "Confirmation/ Rejection Notice" for each key order. The User Representative verifies that the notice accurately reflects the ordered key. If the User Representative receives a notice for an order that was not submitted or if there is any discrepancy in the order, the User Representative should call the EKMS immediately at 1-800-635-5689.

ORDERING BLANK KSD-64As

If additional KSD-64As will be needed, now is a good time to order them (approximate cost: $25 each) from one of the two vendors: Datakey and CTS Corporation. (See inside back cover for further information.)

SELECTING THE VENDOR (CAP & COP)

If you are obtaining your STU-III as GFE — for instance, under the NSA/DIS Loan Program — or under a hand receipt, the equipment and vendor are selected for you. If, however, your method of obtaining the STU-III is either COP or CAP, then your facility will normally be allowed to select the vendor.

You should acquire brochures from AT&T, GE, and Motorola and talk with their representatives. Talk also with contractors who have STU-IIIs. You'll find some obvious differences, such as price, and others that are more subtle.

When you have decided on which STU-III unit to purchase, contact the vendor. Certify your facility's eligibility to the vendor and provide the following:

- Appropriate COMSEC account number.
- Contractor's shipping address.
- Address of the appropriate Central Office of Record.

Then issue the purchase order, and the vendor will send the STU-III to your facility.

STANDARD PRACTICE PROCEDURES

Next, decide on the security procedures for the facility's STU-IIIs, fill devices, master CIK(s), and CIKs and prepare the STU-III Standard Practice Procedures (SPP). Tailor the SPP to your specific operation. Remember that although the user will be briefed on the use of the STU-III and the security precautions for the unit, the user's primary source of information will be the SPP.

DIS has several STU-III SPPs to assist you. The next time your IS Representative comes by, discuss what you need – or make a call. To get you started, the contents might include:

1. Purpose and Introduction
2. Definitions
3. Security Education
4. Roles and Responsibilities
5. Clearances and Need-To-Know
6. Physical Storage
7. Access Controls
8. Safeguards During Use
9. Secure Data Transmission (Fax & AIS)
10. Accountability
11. COMSEC Incidents
12. Emergency Procedures

13. Attachments
    COMSEC briefing
    User Briefing or STU-III SPP Certification
    STU-III Terminal / KSD Hand Receipts
    STU-III Secure Call Log
    Fax Log

The SPP must address the following ISM requirements, as applicable:

STU-III with fax:

- No hard copy receipts need be exchanged for classified information transmitted.
- All other ISM requirements for classified documents apply (e.g., transmissions must be recorded in an accountability record or receipt and dispatch record, as applicable).
- Fax machine must be protected in the same manner as its associated STU-III.

STU-III with AIS:

- Treat STU-III as telecommunications equipment.
- Update AIS SPP to include use of STU-III.
- Apply procedures in ISM, Chapter 8.
- Maintain usual audit trails.

STU-III outside cleared facility:

- FSO must provide prior written approval of any installation or use of a STU-III outside a cleared facility and maintain record of approval for 2 years from the conclusion of the installation or use.
- STU-III may be located only in areas and under conditions appropriate for CCI.
- FSO must not approve installation in residence or vehicle for convenience of employees. FSO must educate user about hazards of these environments.
- No classified material (e.g., notes on conversation) may be introduced to the area.
- Specify emergency procedures and procedures if notes are taken inadvertently.
- No AIS system or fax can be connected to the STU-III.
- Procedures are the same for facilities with safeguarding capability at lower level than key.

STU-III in vehicle:

- Same procedures apply as for location outside cleared facility.
- Also, if vehicle unattended, the vehicle must be locked and all keys (CIK, terminal mounting mechanism key, and vehicle locking keys) must be removed.

- The CCI part of the STU-III installation (normally installed in the trunk of the vehicle) must be removed and properly safeguarded when the vehicle is to undergo maintenance or repair.

RECEIPT OF SEED KEY

The COMSEC Custodian will take receipt of the seed key(s). Although seed key is UNCLASSIFIED CRYPTO, it can be received **only** by a COMSEC Custodian who is cleared to the level of the operational key to which the seed key will be converted. The COMSEC Custodian should:

- Ensure that seed key arrives by U.S. Registered Mail or Defense Courier Service (DCS).
- Inspect the shipping container and plastic bag(s) containing fill device(s) for damage or signs of tampering. If any tampering is evident, submit a COMSEC incident report. (Note that a reportable COMSEC security infraction is referred to as a **COMSEC incident**.)
- Compare the package contents with the contents as indicated on the shipping papers (SF 153). If everything is in order:
- Execute the "**COMSEC Material Report**," **SF 153**, and assign a **transaction number** to the key receipt action. Each report for a STU-III transaction is assigned an 8-digit number identifying the calendar year, the month, and a one-up number (YYMMXXXX). For example, 93010001 is the first STU-III key transaction number used in January 1993; the second transaction number for January 1993 is 93010002. Each month STU-III key transaction numbers must be changed to reflect the new month and revert to "0001" on the first of the month. STU-III key transaction numbers are assigned to all reports involving STU-III key (transfer, destruction, inventory, possession). *No other material can be listed on a report assigned a STU-III key transaction.* Note also that seed key is accountable by its registration number (ALC-1).
- Submit the original SF 153 to the **EKMS Central Accounting Office** (**EKMS/CAO**), and retain a copy for the contractor's records. The completed SF 153 is the official receipt for the key.
- Complete a "**COMSEC Material Record Card**," **L6061**, and file it alphanumerically by short title in the active section of the **COMSEC Register File**. A COMSEC Register File is an index card box in which the custodian places all L6061 cards. It should have an *active section* and an *inactive section*. The active section consists of the L6061 cards for COMSEC items on hand. The inactive section consists of the L6061 cards for COMSEC items that have been destroyed or transferred elsewhere during the past three years. All L6061s should be placed in the appropriate section as soon as possible (on the day received, transferred, etc.).

If there is any difficulty, call the EKMS immediately at 1-800-635-5689. Note the discrepancy on the SF 153, and send it to the EKMS/CAO.

Ensure that each seed key, which is UNCLASSIFIED CRYPTO, is left in its *unopened* plastic bag until use and is safeguarded by the *best means available at your facility* (e.g., GSA-approved security container) until it is loaded.

RECEIPT OF OPERATIONAL KEY, IF ANY

The COMSEC custodian takes receipt of any operational key as above for seed key, except:

- Ensure that operational key arrives by Defense Courier Service; however, TOP SECRET operational key may also arrive by a TOP SECRET-cleared, designated US Government or contractor employee (courier or handcarrier).
- Ensure that operational key is safeguarded as CRYPTO at the level of classification of the information that it can protect (e.g., SECRET CRYPTO). See *COMSEC Supplement*, para. 90.
- If TOP SECRET operational key, two-person integrity (TPI) is required. Both TPI participants must immediately place the key into TPI storage after the COMSEC Custodian has completed and signed blocks 14 and 15 of the SF 153.

RECEIPT OF BLANK KSD-64As, IF ANY

Take delivery of the additional KSD-64As, if any, that you ordered from a vendor. No special protection requirements apply to these blank devices, which will become CIKs. Once they become CIKs, however, they are locally accountable items.

RECEIPT OF STU-III

You or your designee may take receipt of the STU-III terminal(s).

- Ensure that the STU-III was transmitted by U.S. Registered Mail (or DoD/contractor courier or Commercial Constant Surveillance Service Carrier).
- Inspect the shipping container and the STU-III for damage or signs of tampering.
- Compare the serial number of the STU-III with that shown on the accompanying documentation.
- If everything appears to be in order:
  - Execute and dispatch to the vendor the "**Material Inspection Receiving Report**," **DD Form 250**.
  - Execute a "COMSEC Material Report," SF 153, and assign the STU-III receipt action a transaction number.

    Remember, each STU-III is a Controlled Cryptographic Item (CCI) (= accountable COMSEC). Note also that the NSA COR one-up transaction numbering system reverts to "1" every January 1. The numbering system applies to all reports (transfer, destruction, possession inventory) that do *not* list STU-III key. *STU-III key must be reported separately; see Receipt of Seed Key, above.*

- Submit the original SF 153 to the NSA COR, and retain a copy for the contractor's records.
- Complete a "COMSEC Material Record Card," L6061, and file it alphanumerically by short title in the active section of the COMSEC Register File.

Ensure that each unkeyed STU-III is safeguarded as a *high-value item* (i.e., as though it were a computer).

SETUP

The STU-III is easy to assemble and install. Just follow the directions the vendor provides. Attach the handset cord to the handset and main unit. Then insert the telephone cord into an RJ-11 jack (household telephone jack). Finally, supply the power (plug the unit into a 110V wall outlet). That's all there is to it.

You can now use the STU-III in its nonsecure mode just as you would any other telephone. With the STU-III assembled, you may enter phone numbers in its automatic dialer.

If the STU-III will be used for fax or AIS, insert the cable plug from the device into the *RS 232 port* at the rear of STU-III. The STU-III comes equipped with an *internal modem.* STU-III data port guidance was recently issued by the **National Security Telecommunications and Information Systems Security Committee** (**NSTISSC**) as Annex H to *NSTISSI 3013*. This annex provides guidance as to what security measures are needed when using the STU-III's data port. Specific data port and computer security requirements are provided by DIS. Copies of Annex H have been disseminated to all NSA-controlled contractor COMSEC accounts. You may also obtain an NSA STU-III fax report by calling (301) 766-8729.

NONSECURE MODE

To test the nonsecure operation of each unit, place a nonsecure call. While in the nonsecure mode, the STU-III operates as a **Plain Old Telephone System** (**POTS**).

LOADING SEED KEY

After terminating the nonsecure call, load seed key(s) into the appropriate STU-III(s). **Review the STU-III vendor's manual carefully before you start the keying sequence.** *Once you start the keying sequence you will have from three to ten minutes to complete the sequence and make your first CIK*. The amount of time available varies with each make of STU-III. The STU-III is programmed to shut down if the time is exceeded. If this occurs, you will lose your seed key. You would then be required to zeroize the STU-III and insert a new seed key. Remember, there is ample time to complete the keying process. Do not rush.

For each keyset to be established within the STU-III terminal:

- Mark down the STU-III serial number in the event you must enter the number during the keying sequence.
- Verify that the security classification and identification (ID) information on the **fill device card label** are appropriate for the terminal user(s).
- Check the *expiration date* on the fill device card label. If the key has expired (e.g., expiration date in 10/93 and current month is 1/94), a new fill device must be obtained. Dispose of the expired fill device in accordance with Section 8.9 of the *STU-III Key Management Plan*.
- Remove the seed key from its plastic bag.
- Follow the vendor's instructions to bring the keying program up in the display window of the STU-III.
- Insert the KSD-64A containing seed key and turn it 1/4 turn. As you continue following the vendor's instructions, seed key is automatically transferred (loaded) from the KSD-64A to the memory of the STU-III. The KSD-64A is now blank and may be made into and re-used as a master CIK or a regular CIK.
- Follow the vendor's instructions for viewing the ID information on the terminal's display and ensure that the information displayed matches the information of the seed key card label.
- Remove the card label from the fill device.
- Make a master CIK from the blank KSD-64A that contained seed key, if desired, following the vendor's instructions, ***or***
- Make a regular CIK from the blank KSD-64A that contained seed key, if desired, following the vendor's instructions.
- Make other CIKs as desired using additional KSD-64As on hand. You can make up to 7 CIKs per keyset if a master CIK is made; otherwise, you can make up to 8 CIKs per keyset. Each CIK you make is given a unique electronic "password" and will work only with this keyset of this STU-III terminal.
- Record on the back of the fill device card label, for local inventory purposes, the *name/organization of the user for each CIK* and *its corresponding KSD-64A serial number*. *We recommend that you also have the CIK user sign the back of the card label.* Record the *STU-III terminal serial number* on the front of the card label. (Instead of the fill device card label, you may use another type of record that provides the same information, such as the CIK Hand Receipt form shown at Issuing CIKs to Users, below.)
- Leaving the last CIK inserted, call the **EKMS rekey number: 1-800-635-6301**. ***The EKMS electronically converts the seed key to operational key***. The EKMS downloads the Compromise Information Message/Compromised Key List (CIM/CKL) to the STU-III. The CIM/CKL is a list of keys that have been compromised or are suspected of being compromised. If your STU-III should ever contact a terminal on the CIM/CKL, your STU-III will reject going secure with that terminal. When the rekeying (conversion) is complete, the EKMS will automatically disconnect the call.

LOADING OPERATIONAL KEY, IF ANY

After checking the nonsecure operation of the unit(s) to be filled, load operational key(s), if any, into the appropriate STU-III(s). For each keyset to be established within the STU-III terminal, follow the *same procedures provided for loading seed key*. Once the STU-III is loaded with operational key and a CIK is inserted and turned in it, the STU-III can operate in the secure mode immediately. While it is not necessary to call the EKMS rekey number (1-800-635-6301), you are urged to do so. Calling the rekey number will allow the EKMS to 1) send a new operational key to the STU-III, and 2) send the latest Compromise Information Message/Compromised Key List (CIM/CKL) to the STU-III.

ACCOUNTABILITY: CIKs AND KEY

Have the COMSEC Custodian establish local accountability for the CIKs created (see paragraph 8.5.1, *STU-III Key Management Plan*) and maintain accountability records for them. The local accountability records may be either the fill device card label (yellow CRYPTO ID card) supplied with the key, or another type of record that provides the same information (see Issuing CIKs to Users, below). When using the yellow card, ensure that both sides are completed. Local CIK account-ability records must be retained until the terminal(s) is zeroized.

For each seed key [and/or operational key] loaded, have the COMSEC Custodian complete the final disposition portion of its L6061 card (e.g., date, conversion or zeroization) and file it alphanumerically in the inactive section of the COMSEC Register File. When zeroization is performed, also enter the EKMS STU-III key transaction number.

DESTRUCTION REPORTS

Destruction reports will seldom be required. However, the COMSEC Custodian must submit an SF 153, completed as a **destruction report**, to the EKMS in each of these cases:

- ***Seed key loaded but not converted*** (the STU-III system shuts down before it makes the first CIK).
- ***Seed key not loaded - KSD-64A destroyed.*** The KSD-64A should not be physically destroyed by breaking or smashing the device as this does not guarantee destruction of the key stored in the device. Besides, the KSD-64A can be reprogrammed. For proper procedures, refer to Annex A of the *STU-III Key Management Plan*.
- ***Expired unused seed key (or operational key) zeroized.*** Zeroize the seed key by following this program function of your STU-III terminal as described in your vendor manual.
- ***Operational key loaded.*** Note, however, that conversion of seed key to operational key through the EKMS does *not* require a destruction report prepared by the COMSEC Custodian. A destruction report, in the form of a **Key Conversion Notice** (**KCN**), is automatically generated and mailed to the COMSEC account of record (= COMSEC Custodian) by the EKMS when the seed key is replaced electronically by operational key. The KCN indicates the serial number of the terminal into which the seed key was loaded, the KMID number of the seed key converted, and the date of the conversion. The COMSEC Custodian should verify that this is the terminal in which the key was loaded

and ensure that all seed keys listed have, in fact, been converted. Any discrepancies must be immediately reported as a COMSEC incident. Delay in reporting constitutes a reportable COMSEC incident.

PROTECTING KEYED STU-IIIs

Protect each keyed STU-III (unit that contains key **and** that has a CIK inserted in it) *at the highest security level of the information that the operational key can protect.*

MAKING A SECURE CALL

To test the secure operation of each unit, place a secure call.

- Check to see that no unauthorized person can overhear the phone call or view the message window. Remember, *with a functional CIK inserted, the CIK/STU-III combination becomes a classified item.* ***Like a classified document, it must be kept under the constant surveillance of an authorized user.***
- With a CIK inserted, place a nonsecure call to a government or contractor entity having a STU-III and an appropriate facility clearance and need-to-know as required for the keyset in use. Verify the identity of the distant party; if classified information will be discussed, both you and the distant party must have clearances at or above the level of such information ***and*** a need-to-know. If you have any doubt about the clearance level or need-to-know of the distant party, terminate the call.
- Ensure that the party called has inserted and turned a CIK in the STU-III.
- Tell the party called that you are going to go secure.
- Press the SECURE button of the STU-III. Every time you go secure the electronic "password" stored in your CIK is changed to a new electronic "password." The new "password" is also stored in the STU-III. The new CIK and STU-III "passwords" will be compared the next time you want to go secure and must be identical.
- Stand by for 15 seconds while the STU-III ensures that:

  - It is in touch with another STU-III.
  - The distant STU-III is not on the CIM/CKL.
  - The distant STU-III has the same CIM/CKL or, if not, the unit with the more recent CKL updates the other unit.
  - Both units together generate a unique key for this secure call and synchronize their coding functions.
  - Both units display the highest classification common to both units. The highest common security classification level (e.g., SECRET) is displayed on the first line of the message window throughout the secure call. ***Both users must not discuss classified information which is at a higher level.***

- Each unit displays the identifying data of the user of the other unit. Up to three lines of information identifying the distant party will be displayed on lines 2 though 4 of the message window. The first line of the identification will be displayed for the duration of the secure call. At any time during the secure call either user can scroll through the distant party's identifying information.

If the message window:

Displays CIM PRESENT, the distant unit has compromised key. Hang up immediately, and call NSA at 1-800-328-STU3 (1-800-328-7883).

Displays identification information (authentication data) other than that of the supposed distant party, hang up. If you placed the call, try dialing the number again.

Indicates that the key of the distant unit expired more than 2 months ago, advise the party called to: hang up, call the EKMS to rekey the unit, then call you back.

Indicates that the distant unit has a code edition other than BB, advise the party called to: hang up, call the EKMS to rekey the unit, then call you back.

If the display is not working, terminate the call immediately.

- If the displays are in order, proceed with your classified or sensitive discussion. If you have other *unrelated* unclassified and nonsensitive business to discuss, you may ask the party called to return with you to the nonsecure mode. To do so, both parties must press the NONSECURE button on their units. ***There is, however, the danger that while in the nonsecure mode someone might inadvertently discuss classified or sensitive information. Therefore, we recommend that you remain in the secure mode for the entire conversation.***
- After the call, hang up and wait at least two seconds after the display has cleared. **Then** remove the CIK, and safeguard it properly (see Protecting CIKs, below). Reason: At the end of each secure call the information in your CIK is updated. If you remove the CIK too quickly from the terminal, the information will not be updated properly, and the CIK will no longer work.

HANDLING MASTER CIKs

Ensure that any master CIK(s) created **only** to enable/disable some security functions of the STU-III are deleted from the terminal immediately after such use. Ensure also that any master CIK(s) retained are stored at the converted classification level of the seed key (= the highest classification level that the operational key can protect). *If this level is TOP SECRET, then you must have TOP SECRET storage capability*. You do *not*, however, need to impose two-person integrity (TPI) on a TOP SECRET master CIK.

PROTECTING CIKs

Ensure that each regular CIK is protected as required.

- The CIK may be kept in the *personal possession of the authorized holder*, who may even take the CIK home at close of business.
- When a CIK and the STU-III it enables are kept in the same room, the CIK must be protected at the *highest classification level of the information that the STU-III is authorized to protect.*
- If the CIK is stored in a different room, however, it is sufficient if the CIK is stored *in a locked cabinet or desk*.

USER BRIEFING

You (the FSO), the COMSEC Custodian, or the Alternate Custodian gives the terminal users a user briefing, to include their reading the STU-III SPP and certifying in writing that they have read and understood the SPP. The briefing must cover at least the following:

The need for sound security practices in protecting information transmitted over the STU-III.

The specific security requirements associated with the STU-III.

The security reporting procedures in the event of STU-III terminal malfunction or COMSEC incidents.

What constitutes an unauthorized action with regard to a STU-III utilization.

SAMPLE USER BRIEFING

Substantial amounts of classified and sensitive unclassified information have leaked to our adversaries over nonsecure telecommunications circuits. Correct use of the STU-III can reduce this vulnerability. All STU-III users must follow sound, consistent security practices in order to prevent the compromise of classified material and communications by hostile intelligence services and other unauthorized persons. The following procedures are provided as general operational guidelines to ensure the proper use of the STU-III:

Both CIKs and STU-III terminals are accountable items and are tracked by their serial numbers. If you wish to move a terminal from one area to another, you must coordinate the relocation through the FSO with documentation from the custodian.

A keyed terminal is created when the CIK is inserted into the STU-III. You must protect the keyed terminal at the highest classification level the inserted CIK can protect. For example, if the CIK can be used to protect SECRET information, then the joining of the CIK and the STU-III creates a SECRET item, which requires safeguarding at the SECRET level just like any SECRET document you possess. When personnel in the area are not cleared to the level of the keyed terminal, it must be under the direct operational control and within view of the CIK custodian.

Observe the terminal authentication display carefully to ensure that the approved level of the call and person using the distant terminal are proper and correct. Do not discuss classified information if:

Any validity question arises (e.g., the display does not accurately represent the party called).

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

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

The display fails.

Do not permit a terminal to be taken from the facility for use at a residence or in any unauthorized business environment.

Only CIK custodians and terminal users may use the system in a secure mode. Any exceptions to this condition must be reviewed with the FSO or Command Authority.

STU-III STANDARD PRACTICE PROCEDURES
CERTIFICATION

I have read and fully understand the security measures for the Secure Telephone Unit, Third Generation Type 1, or STU-III, set forth in the STU-III Standard Practice Procedures.

I accept the responsibility of being entrusted with a CIK (Crypto Ignition Key). I am aware that when the CIK is inserted into a STU-III unit, the STU-III/CIK unit becomes classified to the level of the key and must be protected at that level.

I will immediately report the loss of a CIK or a STU-III to the COMSEC Custodian or Alternate COMSEC Custodian.

_____/_____
SIGNATURE DATE

_____
PRINTED NAME

_____/_____
SIGNATURE OF COMSEC CUSTODIAN DATE

NOTE: Copies of this certification will be maintained by the Facility Security Officer in the individual's personnel security folder and by the COMSEC Custodian in a separate COMSEC folder.

ISSUING CIKs TO USERS

If provided for in the STU-III SPP, have the COMSEC Custodian issue CIKs to the terminal users and have them each sign either the reverse of the CIK's yellow Crypto ID card or a "CIK Hand Receipt."

CIK Hand Receipt

I, _____, an employee
(Printed Full Name)

of _____, acknowledge
(Organization)

receipt of one CIK (Crypto Ignition Key) having the serial number _____
and associated with the STU-III terminal having the serial number _____

I have read and fully understand the STU-III Standard Practices Procedures regarding my responsibilities and agree to abide by them.

_____/_____
SIGNATURE OF CIK RECIPIENT DATE

_____/_____
SIGNATURE OF COMSEC CUSTODIAN DATE

NOTE: Copies of this certification will be maintained by the Facility Security Officer in the individual' s personnel security folder and by the COMSEC Custodian in a separate COMSEC folder.

REPORTS TO NSA

Ensure that the COMSEC Custodian reports to NSA:

- Loss of a STU-III.
- Loss of seed key.
- Loss of operational key.
- Connection with a STU-III on the CIM/CKL.

Send reports to NSA at this address:

DIRNSA
ATTN: X712
9800 Savage Road
Ft. Meade, MD 20755-6000

Send information copies of reports to NSA to the EKMS at this address:

EKMS Central Facility
P.O. Box 718
Finksburg, MD 21048-0718

SECURITY EDUCATION PROGRAM

Establish a continuous program of STU-III security education.

- Use posters.
- Place a placard near each STU-III unit.
- Ask STU-III users questions during inspections, audits, visits, and so forth.
- Promote secure electronic transmissions by stressing the economic advantages of STU-III use. STU-III calls save time and money and avoid lost sales.

CONTINUING ACCOUNTABILITY

Be sure that each month the COMSEC Custodian compares all seed keys received with all those on hand, those destroyed, and each monthly "Key Conversion Notice" from the EKMS.

In the event that a CIK is lost, have the COMSEC Custodian delete the lost CIK from the appropriate keyset and from its terminal's CIK list. (NOTE: Do *not* notify the EKMS or NSA COR of the loss of a CIK unless there is an indication of espionage or sabotage.)

Be sure that the COMSEC Custodian conducts the required **COMSEC inventory** every six months. NSA COR is responsible for all accounting related to the STU-III equipment itself. You will receive an inventory sheet for your STU-III from NSA COR every six months. Report any deficiencies. EKMS/CAO, which is responsible for all accounting related to STU-III key, will likewise send an inventory sheet every 6 months.

Inspect STU-III equipment and usage as part of your facility self-inspection. DIS industrial security representatives will audit contractor SOCAs as part of their regular industrial security inspections. DIS SOCA inspections replace audits by the NSA COR.

ANNUAL REKEY

Ensure that, for each STU-III, a terminal user performs at least annually an *electronic rekey* (replacement of operational key with new operational key by means of a telephone call to the EKMS). Although the requirement is to rekey once a year, the EKMS encourages rekeying from two to four times a year. During the rekey call the EKMS will send the STU-III the latest CIM/CKL. The user should note the following:

- Ensure that an appropriate CIK is turned in the STU-III before you place the call. *Only one rekey call per keyset is required; it is not necessary to make a rekey call with each CIK.*
- The EKMS rekey number is 1-800-635-6301. When the call goes through, your STU-III will automatically go secure, and the EKMS will automatically rekey your STU-III. The call will take less than one minute. The EKMS will accept your call and rekey the keyset even if you are a month or two late.
- After reaching the EKMS, you should not have to wait for a rekey longer than two minutes. A recorded voice message instructs you through the rekey process. Observe the secure message window until it indicates the rekeying is complete.
- Consult the vendor's manual for directions on how to view the terminal's display to see that the expiration date has increased by one year. The new date verifies the success of the rekey call.

Ensure that, if needed, the COMSEC Custodian performs a *physical rekey* of the STU-III (replacement of operational key with new operational key by means of a fill device, KSD-64A). An electronic rekey call to the EKMS should also be made to ensure that the STU-III terminal receives the most recent CIM/CKL.

ZEROIZING AND REFILLING TERMINALS

Zeroize and refill the STU-III as needed. The STU-III battery backup allows power to be removed, as in a power failure or unplugging the unit to move it, without losing the encryption data. The zeroization button bypasses this backup and erases the encryption data. After zeroization, the STU-III must be re-keyed and the CIKs must be remade. The STU-III is zeroized:

In an Emergency. - If the STU-III is ever in danger of falling into hostile hands, zeroize it to prevent the adversary from obtaining a functional unit.

For Transfer or Code Change. - If you need to transfer the STU-III to another entity of your organization or if you wish to change the DAO code (identifier), zeroize the STU-III and refill it using the new seed key [or operational key].

By Accident. - The accident usually follows an employee's curiosity. The employee starts playing with the buttons and zeroizes the unit. Be sure to brief your employees on the importance of not pressing or playing with the zeroization button. Refill the STU-III using a new seed key [or operational key].

For Shipment. - If you are required, for maintenance or other reasons, to return the STU-III to the vendor, DIS, or other government agency, you should normally zeroize it.

RELOCATING A TERMINAL

Ensure that no STU-III is moved without the prior approval of the COMSEC Custodian.

Ensure too that if the STU-III is ever shipped from the facility, no CIK that enables it is ever shipped with it. The CIK must be packaged and shipped separately.

USER REPRESENTATIVE CHANGES

Ensure that the Command Authority monitors the User Representative(s) and keeps the EKMS informed of any changes in personnel or privileges. The "User Representative Registration Form" also serves as the means of notifying the EKMS of such changes.

NEW CCI CONTROL AGREEMENT

Ensure that your company executes a new CCI Control Agreement when necessary:

1. In the event that the name of the company changes. Any change in a company name invalidates a CCI Control Agreement, and

2. In the event that your facility is covered under a corporate CCI Control Agreement and has been "bought out" by another company whose corporate headquarters does not have an agreement on file with NSA.

COMSEC CLOSEOUT

Have the COMSEC Custodian close the COMSEC account if it is no longer required.

- When a contract closes, request disposition instructions or advice from the User Agency (UA). Request the UA to advise the appropriate material support activity(ies) and/or controlling authority(ies) to delete the contractor from distribution lists.
- Take other action as needed to ensure that additional material is not forwarded to the account or that material is redirected to a different account.
- When the COMSEC account is holding no material, so certify in the request to close the COMSEC account submitted to the NSA COR.

FACILITY CLEARANCE TERMINATION

If the contractor's facility clearance is being terminated, a SOCA is in effect, and one or more NSA/DIS STU-III Loan Program terminals are located at the facility, ensure that the following actions are taken:

- The Command Authority must submit to the EKMS a "User Representative Registration Form" deleting the User Representative. This deletion will cancel all current and future key order requests.
- The COMSEC Custodian must do the following:
  - Zeroize all STU-III terminals.
  - Destroy electronically, return to the supporting COMSEC account, or return to the EKMS all unused key and all KSD-64As that you no longer require.
  - Transfer all STU-III terminals out of the facility in accordance with disposition instructions provided by the government.
  - Inform the DIS Industrial Security Field Office that services the facility.
  - If applicable, notify the COR and the EKMS of the closure of the account.

DEFINITIONS

ACCESS: The ability and opportunity to obtain knowledge of classified or sensitive information, equipment, or other materials; or the ability and opportunity to have unrestricted use, handling, or physical control thereof. The particular requirements for access to different categories of COMSEC materials are detailed in the *COMSEC Supplement to the ISM* and other official documents.

ACOUSTIC SECURITY: Security practices relating to the prevention of unauthorized overhearing of discussions involving classified or unclassified but sensitive information.

ALTERNATE COMSEC CUSTODIAN: The individual designated by proper authority to perform the duties of the COMSEC Custodian during the temporary absence of the COMSEC Custodian.

AUTOMATED INFORMATION SYSTEM (AIS): An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

CENTRAL ACCOUNTING OFFICE (CAO): The part of the Electronic Key Management System (EKMS) that provides accounting support to Central Offices of Record (CORs) and COMSEC Custodians for STU-III key.

CENTRAL OFFICE OF RECORD (COR): A central office which keeps records of all accountable COMSEC material received by or generated within elements subject to its oversight. Usually within a government department or agency, its duties include establishing and closing COMSEC accounts, maintaining records of COMSEC Custodian and Alternate Custodian appointments, performing COMSEC inventories, and responding to queries concerning account management. NSA serves as the COR for most government contractors.

CIK: A key storage device (KSD) that must be plugged into a COMSEC equipment to enable secure communications. It contains an electronic "password" used to lock and unlock a terminal's secure mode. The secure mode is unlocked when the CIK is inserted and turned, locked when it is removed. CIK is the abbreviation for Crypto Ignition Key.

COMMAND AUTHORITY (CA): Individual responsible for managing STU-III key assets for a department, agency, or organization. The Command Authority determines the DAO Description and appoints User Representatives, assigning to them their key ordering privileges.

COMMUNICATIONS SECURITY (COMSEC): COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the US Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information and also includes the application of physical security measures to COMSEC information or materials.

COMPROMISE: The disclosure of classified information to persons not authorized access thereto.

COMPROMISED KEY LIST (CKL): A list of compromised STU-III keys distributed by the EKMS to terminals during rekey calls.

COMSEC ACCOUNT: An administrative entity responsible for maintaining custody and control of COMSEC material and identified by a 6-digit account number.

COMSEC CUSTODIAN: The individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account.

COMSEC SUPPLEMENT TO THE ISM (CSISM): A section of the Industrial Security Manual published separately as DoD 5220.22-S. It establishes policies, procedures, and responsibilities for the control of COMSEC material furnished to, generated or acquired by US industry. It covers the safeguarding controls for classified and unclassified COMSEC material and equipment resident at cleared industrial facilities.

CONTROLLED CRYPTOGRAPHIC ITEM (CCI) A secure telecommunications or information handling equipment, or associated cryptographic component or ancillary device which is unclassified when unkeyed (or when keyed with UNCLASSIFIED key) but controlled. Equipment and components so designated shall bear the designator "Controlled Cryptographic Item" or "CCI."

CRYPTO: A marking or designator identifying all COMSEC key used to secure or authenticate telecommunications carrying classified or sensitive but unclassified government or government derived information, the loss of which could adversely affect the national interest.

DEPARTMENT/AGENCY/ORGANIZATION (DAO) CODE: A 6-digit identification number assigned by the EKMS to a DAO description and used by the User Representative when ordering key.

DEPARTMENT/AGENCY/ORGANIZATION (DAO) DESCRIPTION: A one or two line designation of the user's parent department, agency, or organization. The Command Authority determines the DAO Description, which forms the first part of the terminal user's identification information (authentication data) and appears in the distant terminal's display during a secure call.

DESTRUCTION REPORT: Documentation on an SF 153 of the physical or electronic destruction of COMSEC material by NSA-authorized means.

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS): The STU-III system, administered by the EKMS Central Facility, that provides all keying services to the user community.

FILL DEVICE: Any one of a family of devices developed to read in, transfer, or store encryption key (e.g., Key Storage Device, KSD-64A).

GOVERNMENT FURNISHED PROPERTY (GFP): Property in the possession of or directly acquired by the government and subsequently made available to a contractor but of which the Government retains ownership. GFP includes Government Furnished Equipment (GFE).

HAND RECEIPT (HR): A document used to record local or temporary transfer of material from a custodian to a user and acceptance by the user of the responsibility for the material.

KEYED: Containing cryptographic key. In applications employing a CIK, the crypto-equipment is considered keyed when an enabling CIK is inserted in the unit.

KEY STORAGE DEVICE (KSD): The device that can be used as a fill device and also as a CIK for STU-III terminals. It is small, shaped like a key, and contains passive memory (ROM). When it is used to carry key to a terminal it is called a fill device; when it is used to protect encryption key that has been loaded into terminals, it is called a CIK.

KEY MANAGEMENT PLAN: NSA guidance (EKMS-702.01) for managing the accounting and handling procedures for STU-III key.

OPERATIONAL KEY: Encryption key sufficient to enable a STU-III that has been unlocked by an appropriate CIK to make direct secure calls up to a predesignated level of classification with other keyed STU-IIIs.

PERSONNEL (SECURITY) CLEARANCE (PCL): An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the PCL being granted.

SECURE TELEPHONE UNIT, THIRD GENERATION (STU-III): The STU-III Type 1 terminal is a dual-purpose telephone capable of transmitting voice and data. It may be used as an ordinary telephone that operates over the public telephone network. It may also be used as a secure telephone to communicate through the public telephone network with other STU-III Type 1 terminals (classified and unclassified but sensitive information) and with Type 2 terminals.

SEED KEY: Key that is loaded into a STU-III terminal by a fill device to enable the terminal to electronically obtain its operational key of a predetermined classification during a rekey call to the NSA Electronic Key Management System.

TELECOMMUNICATION: The preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

UNKEYED: Containing no key or containing a key which has been protected from unauthorized use by removing the CIK.

USER REPRESENTATIVE (UR): An individual or office that operates as the agent of the Command Authority authorized to order key for a particular department, agency, or organization.

ZEROIZE: To remove or eliminate the key from a crypto-equipment or fill device.

LIST OF LETTERS AND FORMS

- Contractor Letter to NSA Requesting Eligibility to Procure STU-III Equipment as Contractor Acquired Property
- Contractor Letter to NSA Requesting Eligibility to Procure STU-III Equipment as Plant Equipment (Contractor Owned Property)
- Contracting Officer Authorization to Purchase CCI Equipment as Contractor Acquired Property
- Controlled Cryptographic Item (CCI) Control Agreement
- NSA/DIS Memorandum of Loan Agreement
- COMSEC Material Hand Receipt, A-1721
- Contractor Letter to NSA Requesting Establishment of COMSEC Account (SOCA or Regular)
- NSA Notification of Establishment of COMSEC Account
- Contractor Command Authority Appointment Letter
- Confirmation of Command Authority Appointment Letter
- STU-III User Representative Registration Form
- Confirmation of User Representative Registration Letter
- STU-III User Representative Key Order Authorization Form
- STU-III Key Order Request

- Confirmation/Rejection Notice
- COMSEC Material Report, SF 153
- COMSEC Material Record Card, L6061
- Material Inspection Receiving Report, SF 250
- Fill Device Card Label
- Key Conversion Notice
- Inventory Lists (STU-III and STU-III Key)

ADDRESSES & TELEPHONE NUMBERS

NSA CENTRAL OFFICE OF RECORD

National Security Agency (301) 688-8110
Operations Bldg. Nr. 3
ATTN: Y131
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

NSA STU-III PROGRAM OFFICE

NSA STU-III Program Office 1-800-328-STU3/7883
ATTN: X24 (410) 684-7073
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

EKMS CENTRAL FACILITY

EKMS Central Facility 1-800-635-5689 (Key Assistance)
P.O. Box 718 1-800-635-6301 (Rekey)
Finksburg, MD 21048-0718 (301) 526-3200 (Rekey)

DEFENSE INVESTIGATIVE SERVICE

Defense Investigative Service (703) 325-6057
ATTN: V0432
1340 Braddock Place
Alexandria, VA 22314-1651

STU-III VENDOR HELP LINES

AT&T	GE/RCA	Motorola
1-800-243-7883	1-800-521-9689	1-800-922-4357
(919) 279-3411	(609) 727-5282	(602) 437-2822

KSD-64A VENDORS

DATAKEY
407 West Travelers Trail
Burnsville, MN 55337-2554
(612) 890-6850
1-800-328-8828
fax (612) 890-2726

CTS Corporation
9210 Science Center Drive
New Hope, MN 55428-3635

(612) 533-3533
fax (612) 553-3037