~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87
Date: 22 October 1987

NTISS
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

ADVISORY MEMORANDUM

ON

TRI-TAC KEYING CONCEPTS (U)

~~CLASSIFIED BY DIRNSA (NATIONAL MANAGER, NTISSC)~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S~~
~~DETERMINATION REQUIRED~~

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~CONFIDENTIAL~~

NTAISS
NATIONAL TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

NATIONAL MANAGER

22 October 1987

FOREWORD

1. (U) National Telecommunications and Information Systems Security Advisory/Information Memorandum (NTISSAM) COMSEC/1-87 "TRI-TAC Keying Concepts," supersedes National COMSEC Information Memorandum (NACSIM) 8000, "TRI-TAC Keying Concepts," dated November 1982. This advisory memorandum provides definitions of the keys used in TRI-TAC and explanations of the procedures involved in keying and rekeying the TRI-TAC equipment. The information is presented in nontechnical terms and is designed as a supplement to KAO-193A/TSEC, "Guidelines for the Use and Operation of TRI-TAC COMSEC Equipment (U)", dated October 1982. Several significant changes to TRI-TAC keying concepts which have occurred since the publication of NACSIM 8000 have been included in NTISSAM COMSEC/1-87, as well as the standard terminology for keys as promulgated by the National Security Agency.

2. (U) NTISSAM COMSEC/1-87 was developed for use by COMSEC operators, switch operators, installers, couriers, and COMSEC custodians and should be retained as a ready guide for such personnel. Heads of departments and agencies are responsible for dissemination of this advisory memorandum within their respective departments and agencies. Additional copies may be obtained from:

Executive Secretariat
National Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, Maryland
20755-6000

3. (U) Extracts from this advisory memorandum may be made if necessary. Such extracts should reflect the appropriate classification and shall not be made available to the general public.

Wm E Odom

WILLIAM E. ODOM
Lieutenant General, USA

C O N T E N T S

NTISSAM COMSEC/1-87

TRI-TAC KEYING CONCEPTS (U)

CHAPTER I - INTRODUCTION

1. (U) Purpose: The purpose of this document is to explain, in nontechnical terms, the various keying/rekeying schemes used in the TRI-TAC system.

2. (U) Scope: This document is intended primarily for personnel involved in key management matters, e.g., COMSEC operators, switch operators, installers, couriers, and COMSEC custodians. Operator instructions and procedures for keying/rekeying in the TRI-TAC system are discussed, and short nontechnical descriptions of each key and associated equipment are provided. Detailed operating instructions and additional information on TRI-TAC keying/rekeying options and COMSEC doctrine are provided in the references.

3. (U) References:

a. (U) KAO-184A/TSEC, Guidelines for the Use and Operation of the TSEC/KG-84, dated December 1981.

b. (U) NACSI No. 8107, Operational Doctrine for the TSEC/KG-84 Dedicated Loop Encryption Device in non-TRI-TAC Applications, dated May 1982.

c. (U) National Communications Security (COMSEC) Glossary, dated 1 September 1982.

d. (U) KAO-193A/TSEC, Guidelines for the Use and Operation of TRI-TAC COMSEC Equipment, dated October 1982.

e. (U) NACSI No. 8108, Operational COMSEC Doctrine for the TRI-TAC System, dated May 1984.

f. (U) Letters of Instruction (LOIs), USCINCRED/RCJ6-0, subjects:

(1) Inter/Intratheater Paired Switch Concept for the AN/TTC-39.

(2) Pair-Wise Unique Concept for the AN/TYC-39.

4. (U) Definitions: The following definitions are those commonly used when discussing TRI-TAC keying and rekeying

concepts. For definitions of other, more generic, COMSEC terms, see Reference c.

a. (U) **Alternate COMSEC Parent Switch (Alt CPS)** - A circuit switch designated as a backup to a parent switch for use in the event the parent switch fails or an alternate routing has occurred from the subordinate switches.

b. (U) **Autonomous Message Switch (AMS)** - A message switch having the inherent capability to generate, store, and provide keys. Only the TYC-39 can serve as an AMS.

c. (U) **COMSEC Parent Switch (CPS)** - A circuit switch charged with the responsibility of generating and distributing rekeying keys, Trunk Encryption Device (TED) traffic keys, network traffic keys, network reentry keys, and per-call keys for each COMSEC subordinate switch, their associated subscribers, and local subscribers. The parent switch is also responsible for call completion between incompatible cryptonetworks and for furnishing keys to network-associated message switches.

d. (U) **COMSEC Subordinate Switch (CSS)** - A circuit switch not having integral COMSEC components for key generation and distribution.

e. (U) **Hardened Unique Store (HUS)** - The long-term storage memory area in the HGX-83 component of the TTC-39/TYC-39 switches, the TSQ-111, and in the KGX-93 component of the TTC-42.

f. (U) **Initialize** -

(1) KG-83/KGX-93 - Performing a sequence of steps to randomize the key generator.

(2) KG-82, KG-84 - Performing key loading procedures without a fill device attached.

(3) In other TRI-TAC COMSEC equipment, initialization is automatically performed in conjunction with the actual loading of key.

g. (U) **Manual Command** - Manual actions or procedures performed by the operator from the front panel of the HGX-83 or KGX-93, such as loading and extracting keys into or out of the HUS, changing the Z key, or alarm checking the Z key generator.

~~CONFIDENTIAL~~

h. ~~(C)~~

i. (U) **Noncooperative Remote Rekeying** - The process of automatically rekeying subscriber terminals or other switches from a distant COMSEC parent switch without requiring the cooperation of the terminals or switches being rekeyed.

j. ~~(C)~~

k. (U) **Semi-Autonomous Message Switch (SAMS)** - A message switch that does not possess the inherent capability to generate, store, and distribute keys, but does have associated loop and trunk encryption equipment.

5. (U) Equipment Description: This section contains descriptions of only those TRI-TAC equipments primarily involved in the keying/rekeying process.

a. (U) AN/TTC-39, Circuit Switch - The TTC-39 is a large, mobile, automatic, 300- or 600-line telephone central switch that operates under processor control. The COMSEC and multiplexing equipment are integral to the switch. The TTC-39 is referred to as a COMSEC parent switch (CPS).

b. (U) AN/TTC-42, Circuit Switch - The TTC-42 is a mobile automatic, 75- or 150-line tactical, medium-level, telephone central switch that operates under processor control. COMSEC and multiplexing equipment are integral to the TTC-42 which is referred to as a COMSEC parent switch (CPS).

c. (U) SB-3865, Automatic Telephone Switchboard - The SB-3865 is a 30-line, automatic, digital switchboard designed for small unit tactical headquarters. COMSEC equipment is not

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

integral to the SB-3865, thus the encryption/decryption on Digital Transmission Groups (DTGs) between switches is performed by an external source, e.g., the KG-93. The SB-3865 is referred to as a COMSEC subordinate switch (CSS).

d. (U) AN/TYC-39, Message Switch - The TYC-39 is a large mobile, 25- or 50-line automatic store and forward message switch for handling data and record traffic. The TYC-39 operates under processor control and the COMSEC and multiplexing equipment are integral to the switch. The TYC-39 is referred to as an autonomous message switch (AMS).

e. ~~(C)~~

f. (U) AN/TSQ-111, Communications Nodal Control Element (CNCE) - The TSQ-111 is a mobile, shelterized, modular-constructed, automatic technical control facility capable of managing and controlling large communications nodes. Although possessing integral COMSEC components and a key-generating capability for its own purposes, the TSQ-111 cannot fully duplicate a CPS's functions because it does not have a switching matrix.

g. (U) TSEC/KY-68/78, Digital Subscriber Voice Terminal (DSVT) - The KY-68 is a ruggedized, full-duplex telephone subscriber terminal with built-in audio processing, signaling, and encryption/decryption capability. The KY-68 is the primary voice security equipment used in TRI-TAC and is a subscriber terminal to the TTC-39, TTC-42, and SB-3865 circuit switches. The KY-78 is the office version of the KY-68.

h. (U) TSEC/KG-84, Dedicated Loop Encryption Device (DLED) - The KG-84 is the primary TRI-TAC equipment used for encrypting/decrypting record and data traffic. It is a subscriber terminal to the TYC-39 and GYC-7 message switches.

i. (U) TSEC/KG-84A, General Purpose Encryption Equipment (GPEE) - A follow-on version of the KG-84, the KG-84A is capable of storing up to four (4) keys.

j. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

[redacted]

k. (U) TSEC/KG-81, Trunk Encryption Device (TED) - The KG-81 is a full-duplex, on-line key generator used for bulk encryption/decryption of multichannel data links.

l. (U) TSEC/KG-82, Loop Key Generator (LKG) - The KG-82 is a full-duplex, on-line key generator used at the switch end of a loop primarily to synchronize calls between KY-68s, and to encrypt/decrypt message traffic to and from KG-84s.

m. (U) HGX-82/TSEC, Loop Key Generator Common Unit (CU) - The HGX-82 contains all the support electronics common to a group of up to eight KG-82s, and provides the interface between the KG-82 and the HGX-83.

n. ~~(C)~~ [redacted]

o. (U) HGX-83/TSEC, Automatic Key Distribution Center/ Rekeying Control Unit (AKDC/RCU) - The HGX-83's principal function is to store and distribute keys upon command by the TTC-39, TYC-39, and TSQ-111 processors.

p. (U) HGX-84/TSEC, Interface Control Unit (ICU) - The HGX-84 is a signal buffering unit that acts as an interface between the switch processor and the KG-81, KG-82, HGX-82 and the HGX-83.

q. (U) TSEC/KG-93, Trunk Encryption Device (TED) - The KG-93 is a ruggedized, stand-alone, all-weather trunk encryption device. It is similar to and interoperable with the KG-81, but is optimized for slower speed of operation than the KG-81.

r. (U) TSEC/KG-94, Trunk Encryption Device (TED) - The KG-94 is a fixed-plant version of the KG-93.

~~CONFIDENTIAL~~

s. (U) KGX-93/TSEC, Automatic Key Distribution Center (AKDC) - The KGX-93 combines the functions of the HGX-82, HGX-83, HGX-84, and the KG-83. The KGX-93 functions are similar to the HGX-83 (but with less memory space) and is currently planned for use in the TTC-42 circuit switch.

t. (U) KYK-13/TSEC, Electronic Transfer Device (ETD) - The KYK-13 is a fill device having six memory locations. It is used to store and physically distribute keys, and to key/rekey COMSEC equipment.

u. (U) KYX-15/TSEC, Net Control Device (NCD) - The KYX-15 is a fill device having sixteen memory locations. It is used to store and physically distribute keys, key/rekey COMSEC equipment, and, when connected to appropriate crypto-equipment, electronically transfer keys in certain remote rekeying operations.

v. (U) KOI-18/TSEC, Tape Reader - The KOI-18 is a hand-held, key tape-reading device for transferring keys from tape to a compatible fill device (KYK-13 or KYX-15), or directly into a crypto-equipment.

CHAPTER II - KEYS

1. (U) Introduction: This chapter describes the various types of keys used in the TRI-TAC system. All keys are fixed length sequences of random binary digits and are generated either at the switch or TSQ-111 (by either the KG-83 or the KGX-93) or produced as hard copy tapes by the National Security Agency. Unless specified by service/CINC or NSA doctrine, the decision to use KG-83- or KGX-93-generated key or hard copy key tape is left to the user. The TRI-TAC COMSEC is designed to provide significant system flexibility by allowing on-demand generation of key; and the capability for employing per-call keys and electronic rekeying of COMSEC equipment provides high level security. These advantages should be weighed against operational requirements which may demand the prepositioning of some hard copy tapes. While general concepts governing the use of keys are the same for both electronically generated and hard copy key tapes, there are specific differences concerning handling and storage which will be addressed in this chapter.

> NOTE: (U) TRI-TAC key terminology was defined and published prior to promulgation of the NSA Standard Key Terminology, and cannot in every case be made to conform to the standard terms without causing some confusion. Wherever possible, however, the appropriate standard terminology has been included in parentheses following the TRI-TAC key terminology.

2. (U) Keys:

a. (U) Standard Terminology -

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

(2) Key Encryption Key (KEK) - A key that is used in the encryption/decryption of other keys for transmission or storage.

(3) Traffic Encryption Key (TEK) - A key that is used in the encryption/decryption of plaintext or previously encrypted information.

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

b. ~~(C)~~

NOTE: (U) If all KY-68 subscribers to a CPS are in the same subnetwork, a separate RH key may not be necessary, and its use becomes optional dependent on operational preferences.

c. ~~(C)~~

NOTE: ~~(C)~~

d. ~~(C)~~

NOTE: ~~(C)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

e. ~~(C)~~

(1)

(2)

(a)

(b)

(c)

(d)

f. ~~(C)~~

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

NTISSAM COMSEC/1-87

g. ~~(C)~~

h. ~~(C)~~

i. ~~(C)~~

j. ~~(C)~~

k. ~~(C)~~

l. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

(1)

(2)

m.

n.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

CHAPTER III - AN/TTC-39 AND AN/TTC-42 (U)

1. (U) Introduction: The TTC-39 and TTC-42 are both known as COMSEC Parent Switches (CPSs), and because their keying/rekeying concepts are virtually the same, both are included in this chapter. In the overall TRI-TAC network, various TTC-39/42 switches are designated as parent switches for the subnetworks contained in the overall network.

2. (U) Keys: The following keys are involved in the keying/rekeying process at the CPSs (See Figure III-1 on page 19).

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

e. ~~(C)~~

f. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

g. ~~(C)~~

(1)

(2)

(3)

(4)

h. ~~(C)~~

i. ~~(C)~~

j. ~~(C)~~

(1)

(2)

(3)

(4)

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

(5)

3. (U) Cold Start Procedures:

a. ~~(C)~~

(1)

NOTE: ~~(C)~~

(2)

(3)

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

NOTE: ~~(c)~~

(4)

(5)

b.

(1)

(2)

(3)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

4. (U) Rekeying Procedures:

a. ~~(C)~~

(1)

NOTE: (U) This transfer capability has not been implemented in current switch software, but is expected to be available in the future.

(2)

(3)

NOTE: ~~(C)~~

b. ~~(C)~~

(1)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

(2)

(3)

c. ~~(C)~~

d. ~~(C)~~

NOTE:

e. ~~(C)~~

f. ~~(C)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

g. ~~(C)~~

h. ~~(C)~~

i. ~~(C)~~

j. ~~(C)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

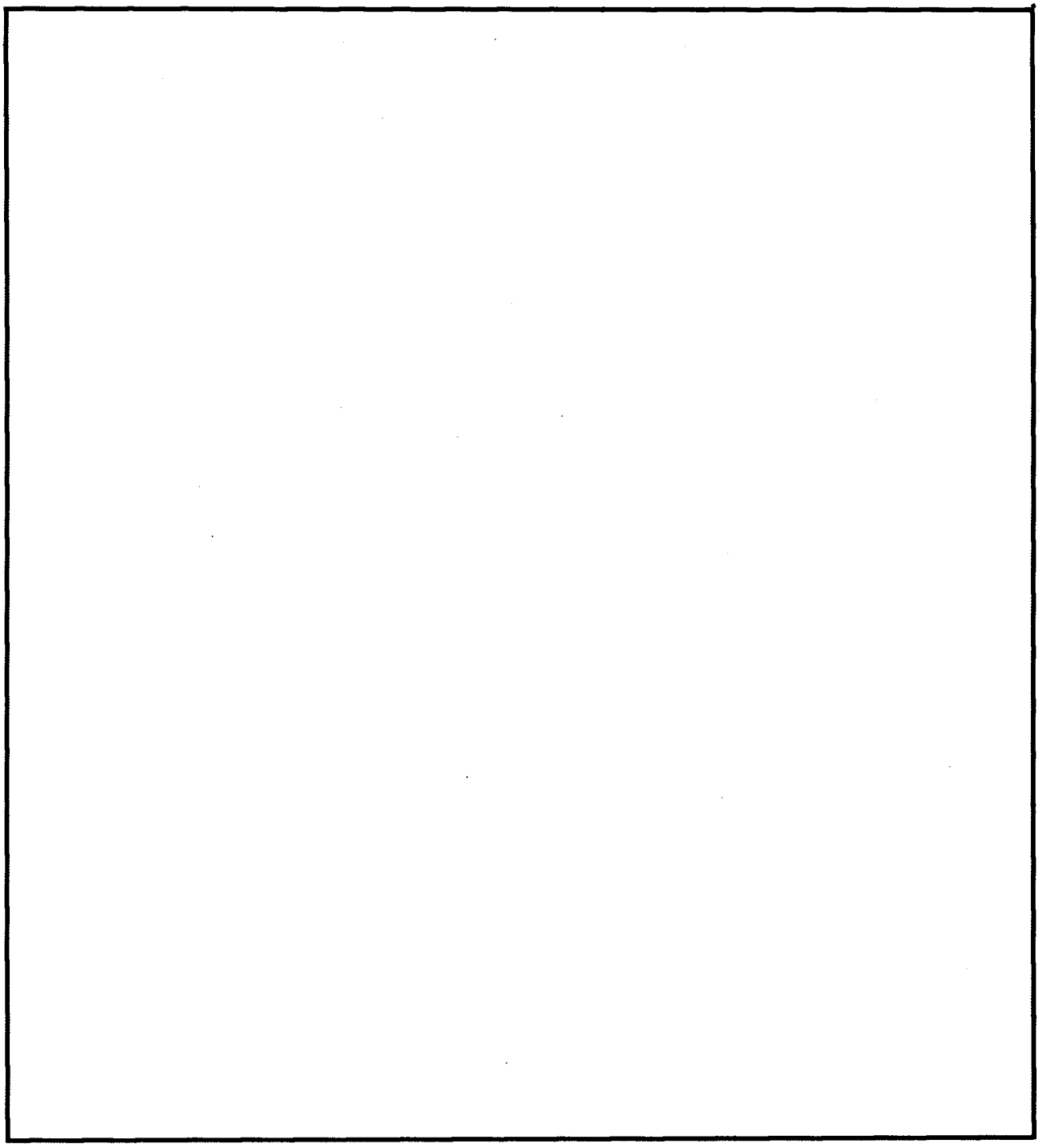


Figure III-1

~~CONFIDENTIAL~~

CHAPTER IV - SB-3865 SUBORDINATE TO A TTC-39/TTC-42 (U)

1. (U) Introduction: When an SB-3865 switchboard is subordinate to a TTC-39 or TTC-42 CPS, the keys used by subscribers off the SB-3865 are managed by the CPS. Once keys are received from a CPS, SB-3865 personnel are normally responsible for further distribution to the actual subscribers.

2. (U) Keys: The following keys are involved in the keying/rekeying process at an SB-3865 subordinate to a CPS (See Figure IV-1 on page 23):

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

e. ~~(C)~~

f. ~~(C)~~

g. (U) A KY-68 will be located at the SB-3865 for operator use and will require R, U, and X keys.

3. (U) Cold Start Procedures:

a. (U) A courier will deliver a fill device to the SB-3865 containing the T key and the UIRV, if needed for use at the

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

switch, and the U and RH keys for all KY-68 subscribers off the SB-3865 and the KY-68 located at the SB-3865.

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

4. (U) Rekeying Procedures:

a. ~~(C)~~

(1)

NOTE: ~~(C)~~

(2)

b. ~~(C)~~

c. (U) RH Keys: (Same procedure as for new U keys above.)

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

d. ~~(C)~~

e. ~~(C)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

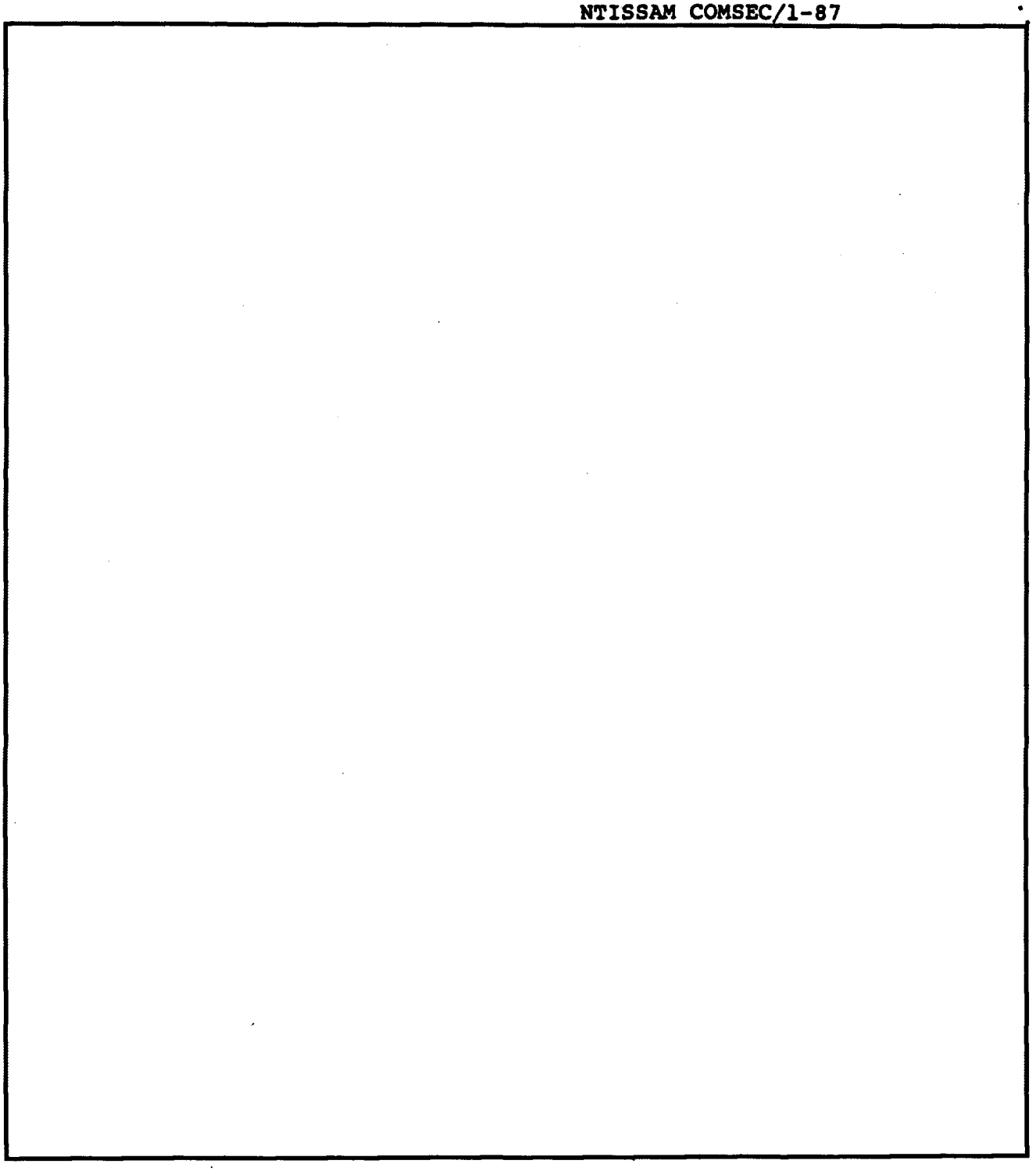


Figure IV-1

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

CHAPTER V - SB-3865 NOT SUBORDINATE TO A TTC-39/TTC-42 (U)

1. (U) Keys: The following keys are involved in the keying/rekeying process at an independent SB-3865 (See Figure V-1 on page 26):

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

2. ~~(C)~~

3. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

(2)

d. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

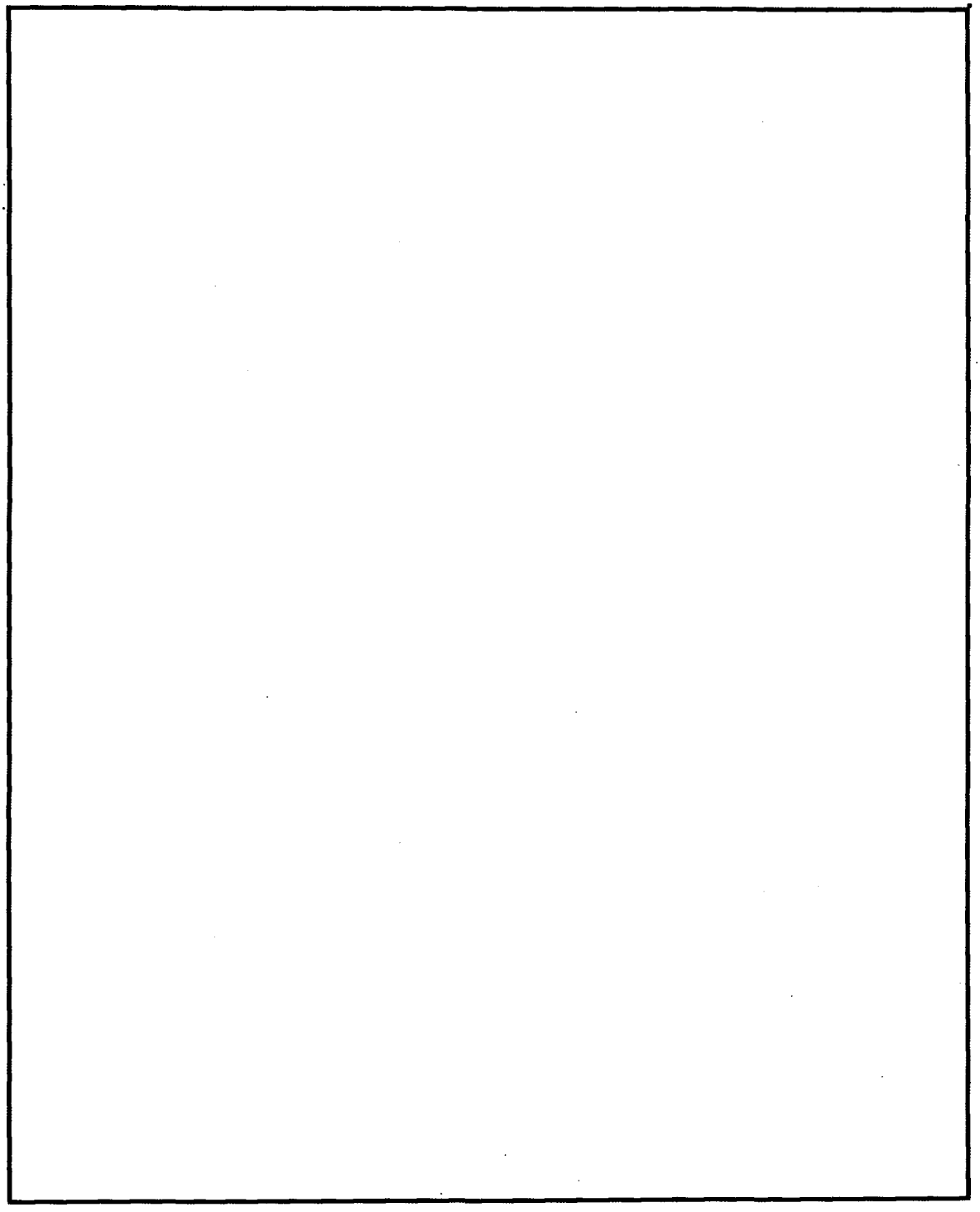


Figure V-1

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

CHAPTER VI - KY-68/78

1. ~~(FOUO)~~

a. (U) Subscriber U Key (KEK) - A U key will be used for rekeying the KY-68.

b. ~~(C)~~

c. ~~(C)~~

NOTE: ~~(C)~~

d. ~~(C)~~

e. ~~(C)~~

f. ~~(C)~~

2. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

3. (U) Rekeying Procedures:

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

(1)

(2)

(3)

e. ~~(C)~~

f. ~~(C)~~

4. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

CHAPTER VII - AN/TSQ-111 CNCE (U)

1. (U) Keys: The following keys are involved in the keying/rekeying process at the CNCE (See Figure VII-1 on page 35):

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

(1)

(2)

d. ~~(C)~~

(1)

(2)

e. ~~(C)~~

f. ~~(C)~~

g. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

h. ~~(C)~~

i. ~~(C)~~

j. ~~(C)~~

2. (U) Cold Start Procedures:

a. ~~(C)~~

b. ~~(C)~~

c. ~~(C)~~

d. ~~(C)~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NOTE:

e. ~~(C)~~

f. ~~(C)~~

g. ~~(C)~~

3. (U) Rekeying Procedures:

a. ~~(C)~~

(1)

(2)

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

NOTE: ~~(c)~~

b. ~~(c)~~

c. ~~(c)~~

(1)

(2)

(3)

d. (U) Z Key: The Z key is changed by performing the proper Change Z manual commands on the HGX-83.

e. ~~(c)~~

f. ~~(c)~~

g. ~~(c)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

h. ~~(C)~~

i. ~~(C)~~

NOTE: ~~(C)~~

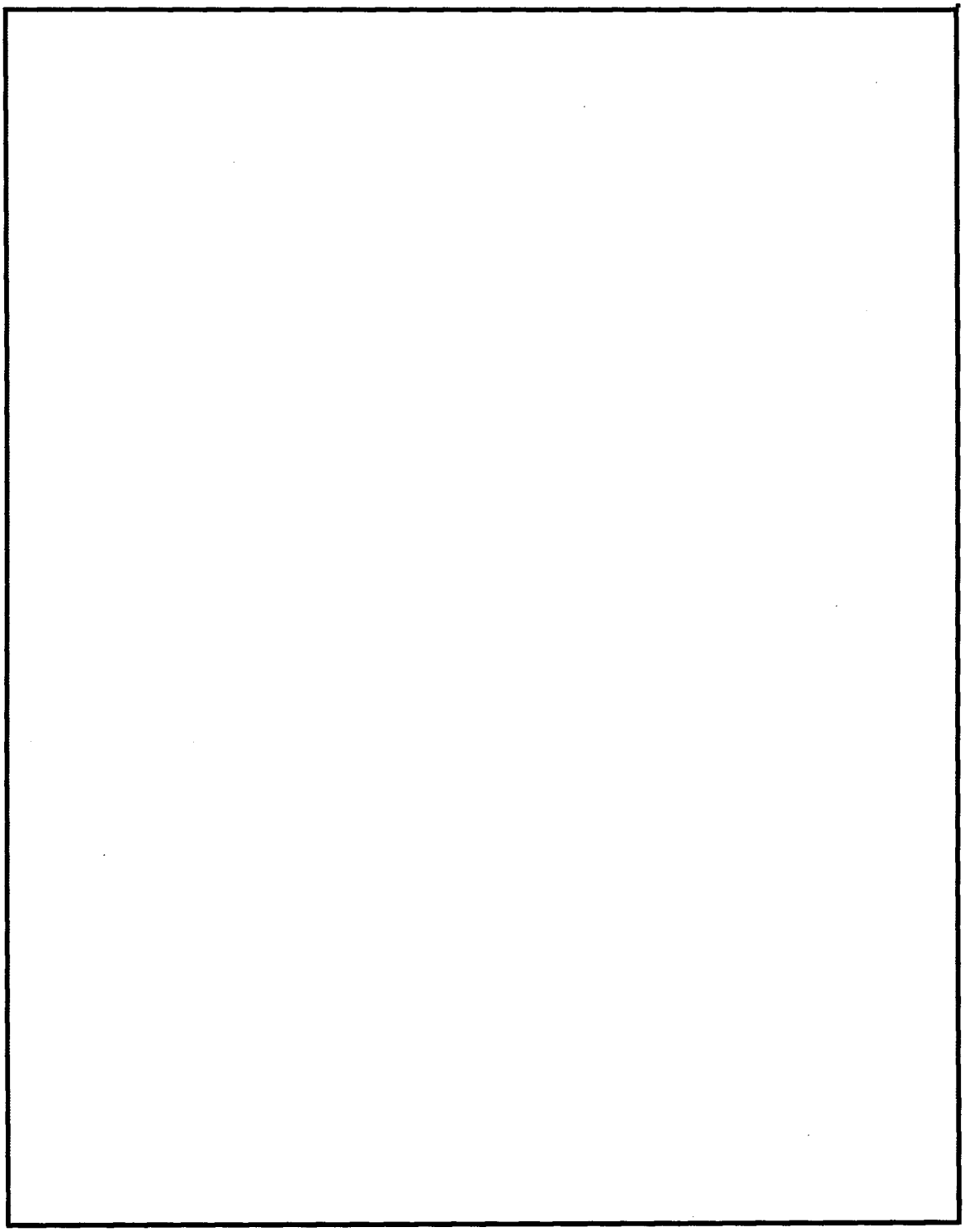


Figure VII-1

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

CHAPTER VIII - KG-81, KG-93, KG-94 (U)

1. ~~(FOUO)~~

2. (U) Keys:

a. ~~(C)~~

b. ~~(C)~~

3. ~~(C)~~

4. (U) Rekeying Procedures:

a. ~~(C)~~

(1)

(2)

(3)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

NTISSAM COMSEC/1-87

NOTE: ~~(C)~~

b. ~~(C)~~

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

CHAPTER IX - AN/TYC-39 (U)

1. ~~(C)~~

2. (U) Keys: The following keys are involved in the keying/rekeying process at the TYC-39 AMS (See Figure IX-1 on page 44):

a. ~~(C)~~

b. ~~(C)~~

(1)

(2)

NOTE: ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

c. ~~(C)~~

(1)

(2)

(3)

d. ~~(C)~~

e. ~~(C)~~

f. (U) If there is a KY-68 located at a TYC-39 that is a subscriber to a circuit switch, its U and X keys will be provided and managed by the circuit switch.

g. ~~(C)~~

3. (U) Cold Start Procedures:

a. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

b. ~~(C)~~

c. ~~(C)~~

NOTE:

d. ~~(C)~~

e. ~~(C)~~

NOTE: ~~(C)~~

f. ~~(C)~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

g. ~~(C)~~

NOTE:

h. ~~(C)~~

4. (U) Rekeying Procedures:

a. ~~(C)~~

b. ~~(C)~~

(1)

(2)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

NTISSAM COMSEC/1-87

c. ~~(C)~~

(1)

(2)

(3)

(4)

(5)

d. ~~(C)~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

e. ~~(C)~~

f. ~~(C)~~

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

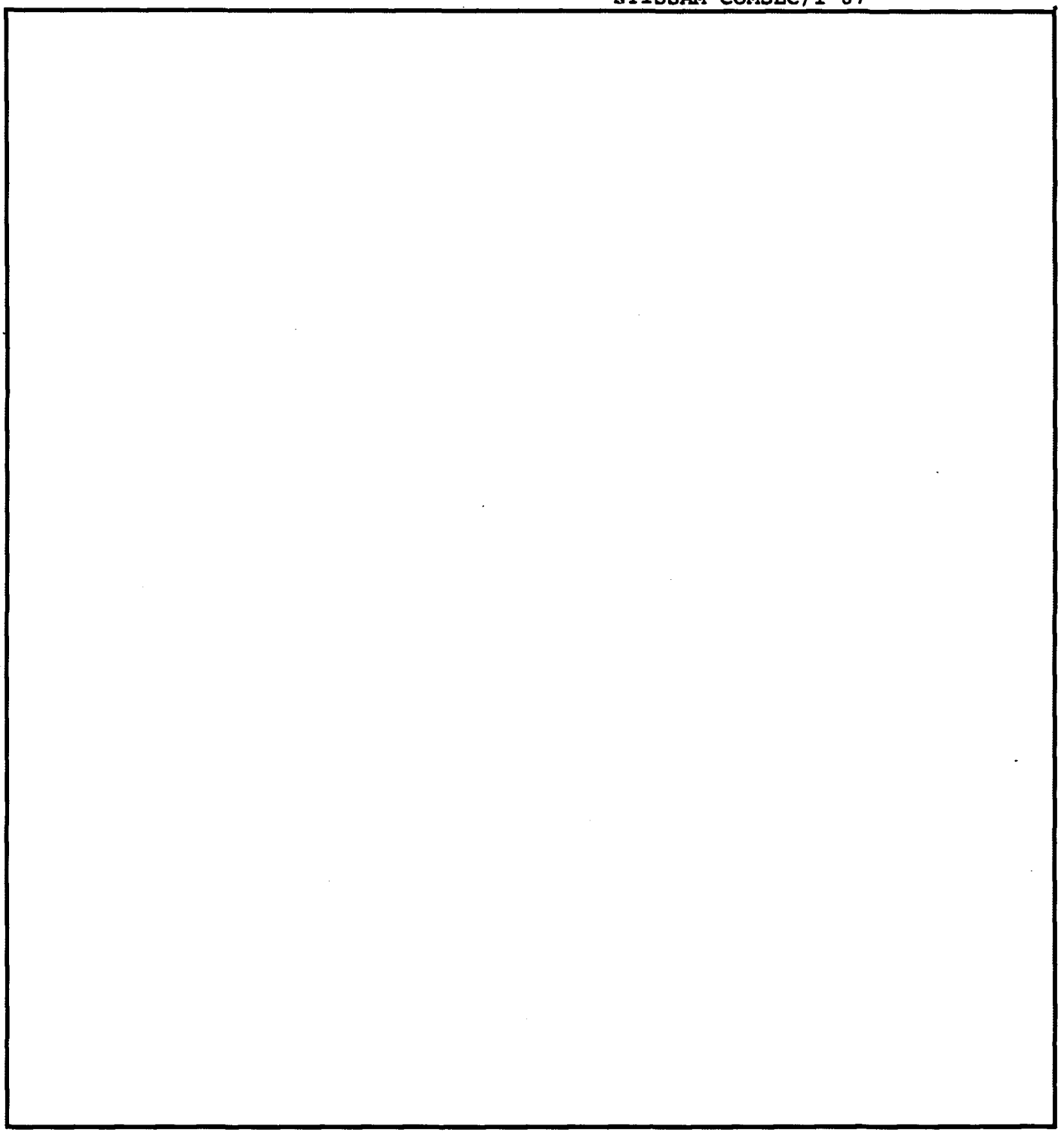


Figure IX-1

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

CHAPTER X - KG-84 (U)

1. ~~(FOUO)~~

2. (U) Keys:

a. ~~(C)~~

b. ~~(C)~~

3. (U) Cold Start Procedures: Following a power up from a Cold Start or zeroized condition, the following procedures apply:

a. ~~(C)~~

b. ~~(C)~~

4. (U) Rekeying Procedures:

a. ~~(C)~~

b. ~~(C)~~

(1)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

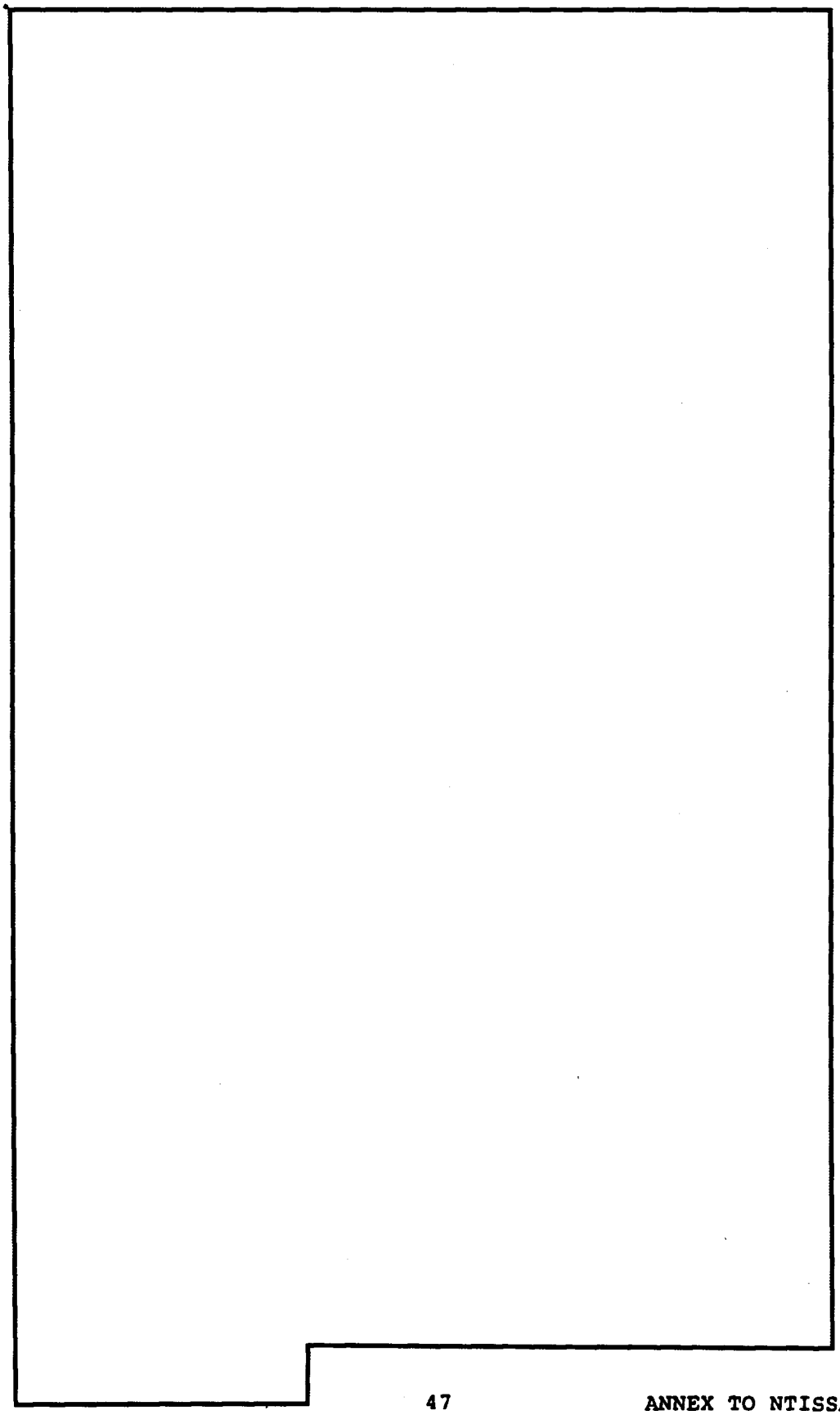
NTISSAM COMSEC/1-87

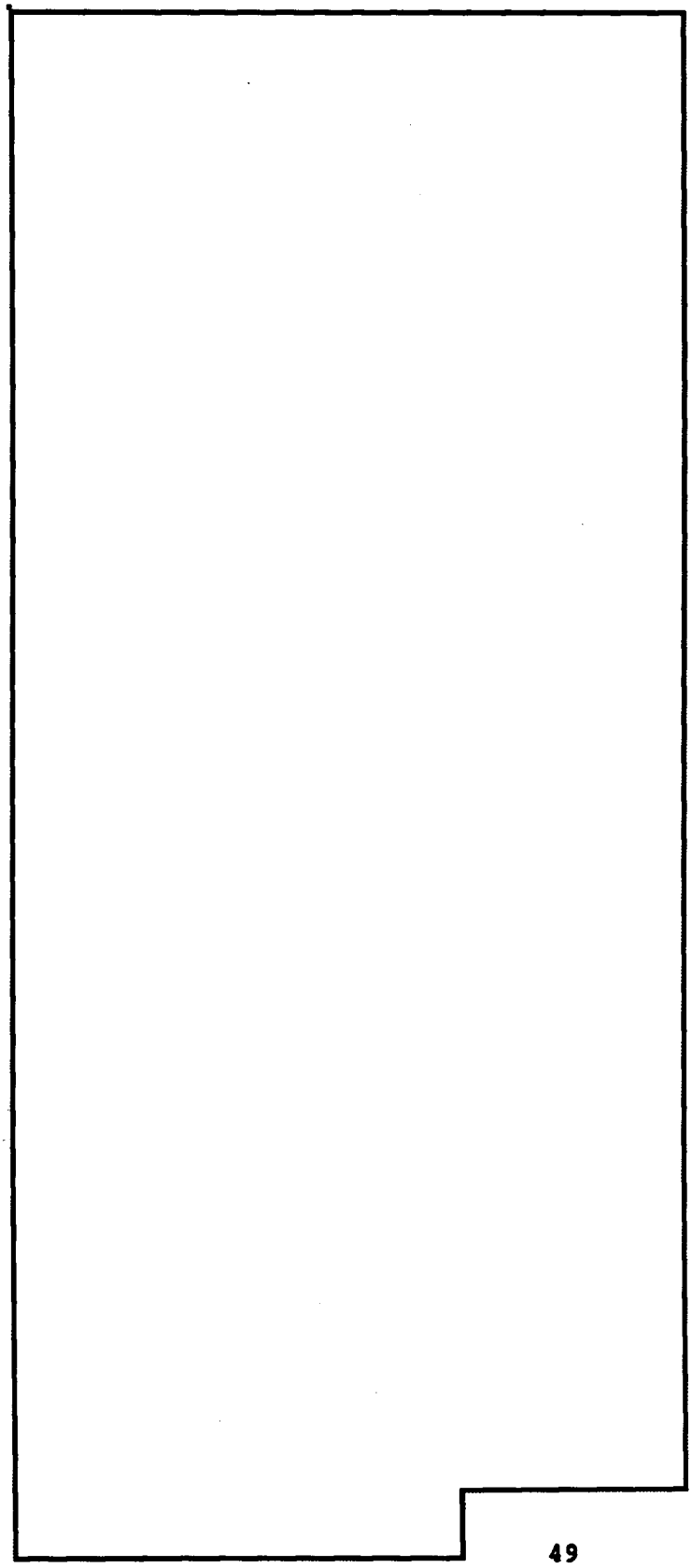
(2)

NOTE:

(3)

(4)



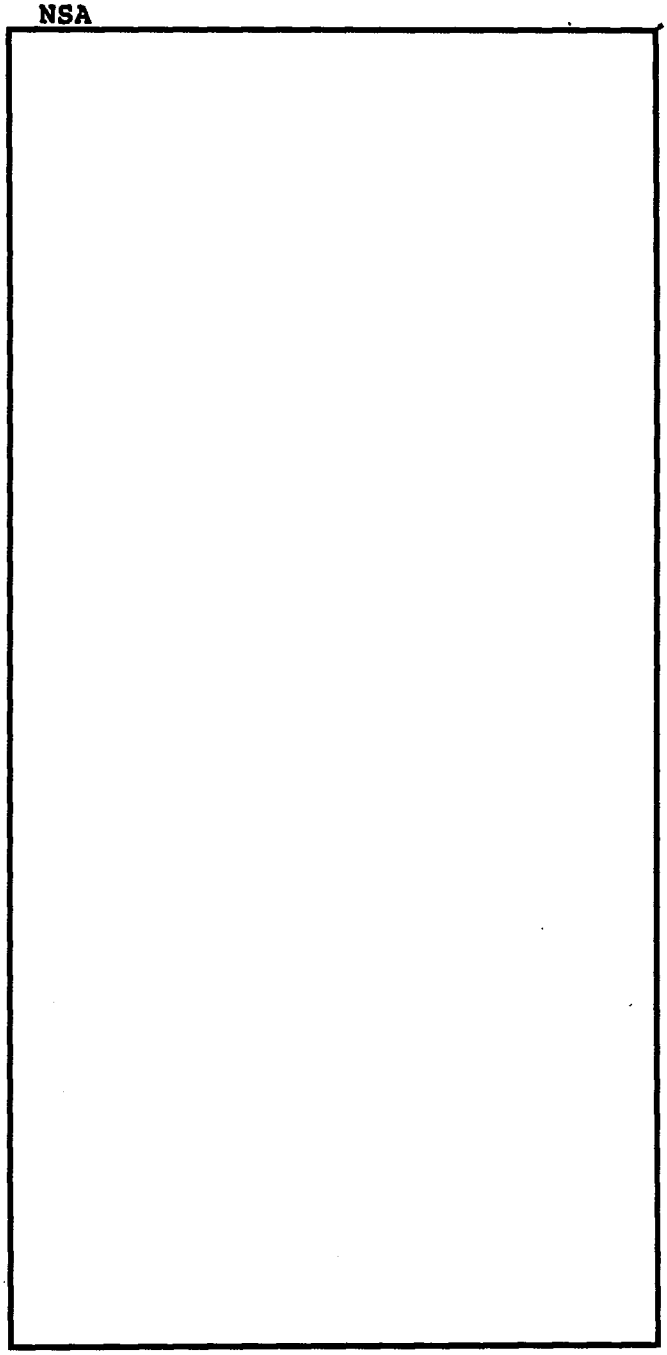


UNCLASSIFIED

(b)(3)-P.L. 86-36

NTISSAM COMSEC/1-87

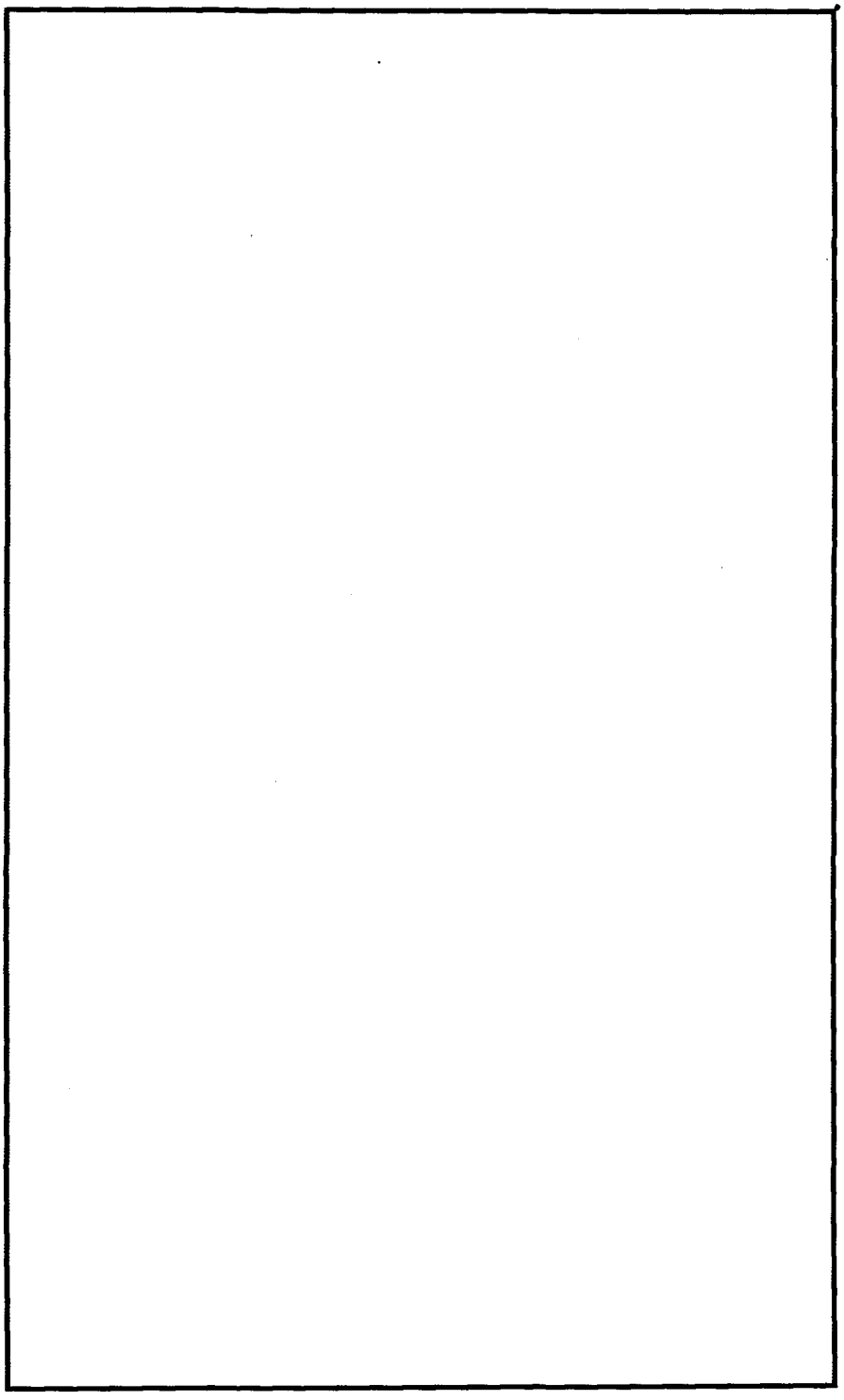
DISTRIBUTION:
NSA



UNCLASSIFIED

UNCLASSIFIED

NTISSAM COMSEC/1-87



UNCLASSIFIED

~~CONFIDENTIAL~~

NTISSAM COMSEC/1-87

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~CONFIDENTIAL~~