

NTISSI No. 3012
27 November 1989

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR THE KY-71

Approved for Release by NSA on 09-25-2024, FOIA Case # 51573

~~FOR OFFICIAL USE ONLY~~

NTAISS

NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY

NATIONAL MANAGER

27 November 1989

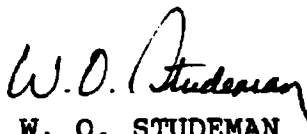
FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3012, "Operational Security Doctrine for the KY-71," provides security doctrine for the operational use of the KY-71 in all applications, but primarily for the Federal Secure Telephone Service (FSTS). This instruction supersedes NACSI No. 8109, "Operational COMSEC Doctrine for the TSEC/KY-71," dated 28 November 1984.

2. Once the transition from STU-II to STU-III has been accomplished, the only STU-IIs that will be retained are those for purposes of interoperability with NATO or other allies who will continue to use the STU-II in the future. There will also be STU-IIs retained for U.S.-only use for special purpose nets.

3. The responsibility for distributing and implementing this instruction to subordinate elements rests with the chiefs of the Military Services and the heads of the federal departments and agencies. These officials may request additional copies from:

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



W. O. STUDEMAN
Vice Admiral, U.S. Navy

OPERATIONAL SECURITY
DOCTRINE FOR THE KY-71

SECTION

PURPOSE AND SCOPE.....I
 REFERENCES.....II
 DEFINITIONS.....III
 EXCEPTIONS.....IV
 GENERAL SECURITY GUIDANCE.....V
 SYSTEM DESCRIPTION.....VI
 KEYING.....VII
 PHYSICAL SECURITY.....VIII
 EMERGENCY PROCEDURES.....IX
 REPORTABLE INCIDENTS.....X

SECTION I - PURPOSE AND SCOPE

1. This document provides minimum security requirements for operational use of the KY-71 secure telephone unit (STU-II) in all applications, but primarily in the Federal Secure Telephone Service (FSTS). This document includes classification, COMSEC accounting, cryptoperiods, reportable incidents, and emergency procedures. Guidance concerning COMSEC matters of a general nature is addressed by the references. The provisions of the instruction apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, and use the KY-71.

SECTION II - REFERENCES

2. Throughout this instruction, references applicable to both government and government contractors are included, separated by slashes, with the government reference listed first.

a. Government Departments and Agencies.

(1) NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.

(2) NACSI No. 2005, Communications Security (COMSEC) End Item Modification, dated 28 May 1981.

NTISSI No. 3012

(3) NACSI No. 4009, Protected Distribution Systems, dated 30 December 1981.

(4) NACSIM No. 5203, Guidelines for Facility Design and RED/BLACK Installations, dated 30 June 1982.

(5) NCSC-9, National COMSEC Glossary, dated 1 September 1982.

(6) NACSI No. 4008, Safeguarding COMSEC Facilities, dated 4 March 1983.

(7) NTISSI No. 4001, Controlled Cryptographic Items, dated 25 March 1985.

(8) NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.

(9) NTISSI No. 4000, Communications Security Equipment Maintenance and Training, dated 14 July 1986.

(10) NTISSI No. 4003, Reporting COMSEC Insecurities, dated 3 November 1986.

(11) NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

(12) NTISSI No. 7000, TEMPEST Countermeasures for Facilities, dated 17 October 1988.

(13) NTISSI No. 4006, Controlling Authorities for COMSEC Keying Material, dated 2 May 1989.

b. Government Contractors.

(1) U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual, dated 2 February 1986 (uncleared government contractors).

(2) COMSEC Supplement to the Industrial Security Manual (CSISM) for Safeguarding Classified Information, dated 17 March 1988 (cleared government contractors who are participants in the Defense Industrial Security Program [DISP]).

NTISSI No. 3012

(3) Cleared government contractors who are not participants in the DISP will use implementers of the government references provided by their government sponsors.

SECTION III - DEFINITIONS

3. Definitions contained in the National COMSEC Glossary NCSC-9/CSISM/CCI Manuals apply to this instruction with the exception that the term "COMSEC insecurity" is replaced by the term "COMSEC incident." For the purpose of this instruction the following definitions also apply:

a. Controlled Cryptographic Item (CCI). A secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified, but controlled. Equipment and components so designated shall bear the designator controlled cryptographic item or CCI.

b. Key. Information (usually a sequence of random binary digits) used to initially set up and to periodically change the operations performed in a crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter countermeasures (ECCM) patterns (frequency hopping or spread spectrum), or for producing other keys.

SECTION IV - EXCEPTIONS

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

4. Heads of departments and agencies and their contractors must submit requests to the Director, National Security Agency (DIRNSA, ATTN:) for exceptions to this doctrine where minimum standards cannot be met. Individual departments and agencies and their contractors may choose to implement more stringent controls, especially for highly sensitive and compartmented applications.

SECTION V - GENERAL SECURITY GUIDANCE

5. General security guidance applicable to the KY-71 may be found in the references. These include: physical security including access, accounting, storage, and transportation; keying material packaging, marking, and handling; and classification guidance for COMSEC information which includes all reports and releases of information relating to the KY-71 system and associated equipment.

NTISSI No. 3012

SECTION VI - SYSTEM DESCRIPTION

6. System Components. The KY-71 is used in conjunction with the Key Distribution Center (KDC-II) to provide secure telephone service to all KY-71 users. The KY-71 provides cryptographic security for voice and data transmissions and, when used with appropriately classified keys, is approved for the transmission of all classifications and categories of voice and data. The following items are used at user locations although not all items are used at all locations:

a. KY-71 Secure Telephone Terminal. The KY-71 terminal contains the voice and signal processing circuitry and cryptographic circuitry necessary for encryption/decryption of voice or data transmissions.

b. HYX-71 Desk Set. The telephone desk set used with the KY-71 terminal. The HYX-71 can be disabled to prevent unauthorized use during the authorized user's absence.

c. Z-AMX Junction Box. Required when a data set or more than one desk set is used with the KY-71 terminal.

d. KYK-71 Crypto-Ignition Key (CIK). Must be inserted in the KY-71 terminal when it is being keyed and when making or receiving a secure call.

e. KOI-18 General Purpose Tape Reader. Used to load hard copy key tapes into the KYK-13 or KY-71 terminal.

f. KYK-13 Electronic Transfer Device. Used to load electronic keys into a KY-71 terminal.

NOTE: As used herein, the term KY-71 COMSEC material will include the KY-71 terminal, associated ancillary equipment, and other supporting COMSEC material, e.g., operating instructions, maintenance manuals, etc.)

NTISSI No. 3012

SECTION VII - KEYING

7. Keys. The following types of keys are used with the KY-71.

a. Unique Key (Vu). The Vu is a key encryption key (KEK) unique to each individual KY-71 terminal. It is used only for protecting per-call keys (Vcalls) and is held only at the KY-71 terminal and the KDC-II. The Vu is never used to protect traffic. A KY-71's Vu may be updated; however, a simultaneous update must be done at all KDC-IIs in order for the KY-71 terminal to continue to operate in the KDC mode with all KDC-IIs. Individual Vus may not be used at more than one KY-71 terminal without the specific prior approval of the controlling authority. Vus will be classified at the highest classification of information authorized for transmission over a specific terminal, or at a minimum of SECRET CRYPTO.

b. Per-Call Key (Vcall). The Vcall is a traffic encryption key (TEK) electronically generated by a KDC-II. A Vcall is generated upon request of the calling KY-71 and is transmitted in encrypted form to the calling KY-71, which then automatically transmits it to the called KY-71. The Vcall protects traffic between these two KY-71s, and is not retained by the KDC-II. Up to 20 Vcalls, protected by the Vu, can be stored in a KY-71 terminal and used for subsequent calls to the same KY-71. Since the distribution of the Vcall is so limited, and the Vcall appears only in electronic form, its use provides the most secure KY-71 operating mode. Vcalls are classified at the highest classification of information authorized for transmission during a specific call or at a minimum of SECRET CRYPTO.

c. Net Key (Vn). The Vn is a TEK held in common by a number of KY-71 terminals. In operational use, the Vn is intended to provide a back-up capability to allow for secure communications among KY-71s when no stored Vcalls are available and communications with the KDC-II are disrupted; or in other special cases authorized by DIRNSA. It may also be used when KDC-II service is otherwise not available. There can be separate UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET, and compartmented Vns. Vns are classified at the highest classification of the information authorized for transmission over the cryptonet.

NTISSI No. 3012

d. Authentication. The FSTS is self-authenticating to the SECRET level, but can pass information that is classified above that level when both participants in the conversation have proper clearances and appropriately classified key. All persons who are allowed uncontrolled access to system telephones must have at least a SECRET security clearance. When discussing TOP SECRET or compartmented information, it is each user's responsibility to determine the clearance of the other party to receive that information. This may be done by means of an NSA-produced authentication system, or positive voice recognition, in cases where the individual's clearance level is already known.

8. Key Tapes. Vus and Vns are generated by NSA and provided in punched tape form. They may be loaded into a KY-71 terminal only by using a KOI-18 or a KOI-18 in combination with a KYK-13.

9. 

10. Classification of Keying Information. NTISSI No. 4002 states that the implementation date of a single item of keying material is classified CONFIDENTIAL and that lists containing such information are classified a minimum of CONFIDENTIAL. Listings of specific KY-71 terminal identification numbers are unclassified, and bear the caveat FOR OFFICIAL USE ONLY (FOUO). This includes single equipment listings and multiple listings up to and including the complete government listing. Inclusion of effective dates, however, would make such listings CONFIDENTIAL. As an exception, in instances where a KY-71 initially fails to key or rekey properly, and telephone troubleshooting assistance from KDC-II personnel is required to restore its secure operational capability, transmission in the clear of the keying material identification information, terminal identification number, and terminal error display code is permitted. Transmission in the

NTISSI No. 3012

clear of this information under such circumstances is not a reportable incident, although an appropriate secure transmission means should be used whenever available.

11. Cryptoperiods. The cryptoperiods for the KY-71 keys are as follows:

a. Vu. Three months. The controlling authority may authorize extensions of up to seven days. Vus will be updated whenever directed by the controlling authority either to facilitate recovery from a compromise, or in special circumstances when there is a high risk of loss of a keyed terminal and previous communications must be protected; e.g., an embassy anticipating being overrun.

b. Vcall. One call. The Vcall may also be stored and used for all calls to the same KY-71 for the length of the Vu cryptoperiod, if the identification number of the called KY-71 associated with a specific Vcall has been included in the stack of stored Vcalls in the KY-71 terminal.

c. Vn. One month. The controlling authority may authorize extensions up to 48 hours in accordance with NTISSI No. 4006/CSISM/CCI Manual. It is essential to maintaining security that effective Vns be updated daily at all KY-71 terminals. Before securing the KY-71 for a holiday, a weekend, or longer, the Vn is to be updated one time. When the KY-71 is to be used again, the appropriate number of updates are to be performed to bring each location holding a Vn up to the current date. The Vn, however, must be updated at least once every seven days. Failure to do so is a reportable incident. As an exception, the controlling authority for a Vn may waive the weekly update requirement for specific installations where the user may be absent for longer than one week; e.g., residence installations, provided the CIK is returned to the COMSEC custodian or other separate secure facility for safekeeping and the Vn is updated immediately after the CIK is returned to the user. Because Vns are superseded monthly, daily updating will result in the effective Vn update setting matching the calendar day of the month; i.e., setting 1 is used on the 1st of the month, setting 2 on the 2nd, etc. Vn updates must be done at the KY-71s using the local update procedure.

NTISSI No. 3012

d. CIK Update. CIKs in operational use must be updated at least once a week by going off-hook and on-hook with the CIK inserted into the terminal. Except as authorized in paragraph 8.c. above, failure to update weekly is a reportable incident.

12. Cryptonet Size. The cryptonet size limitations for the KY-71 keys are as follows:

a. Vu. One KY-71 terminal and all KDC-IIIs.

b. Vcall. Two KY-71 terminals. (The KDC-II generates Vcalls, but does not retain them once they have been transmitted to the KY-71s.)

c. Vn. Vns may be used in contingency and other applications. The following guidance applies:

(1) Contingency Vns. In the event of a failure of the Vcall mode affecting a community of KY-71s, the controlling authority can activate a contingency Vn mode of operation. The contingency Vn cryptonet should be kept to the minimum number of holders necessary to support essential communications.

(2) Other Vns. Cryptonets for other noncontingency communications applications should be kept small to minimize the risk and impact of a Vn compromise. Vn cryptonets among KY-71s involved in long-distance calls (most likely using microwave or satellite communications links), and multiple COMSEC accounts (where more people will be involved in Vn distribution), are more vulnerable to intercept and increased risk of HUMINT exploitation. Non-contingency Vn cryptonets should, therefore, be limited to communications using only cable, wireline, or fiber optic communications links, normally supported by one COMSEC account, e.g., for use for local calls among KY-71s operating behind the same PBX or PABX. Vn cryptonets, other than contingency cryptonets, should not be larger than 30 holders. Exceptions to any of the above non-contingency Vn applications or cryptonet size restrictions may be approved only by the Vn controlling authority on a case-by-case basis. A copy of all such approvals shall be provided to DIRNSA (ATTN:).

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

NTISSI No. 3012

SECTION VIII - PHYSICAL SECURITY

13. Access, Storage, and Transportation of Uninstalled KY-71s. Uninstalled KY-71s and supporting CCIs shall be safeguarded in accordance with the access, storage, and transportation requirements of NTISSI No. 4001/CSISM/CCI Manual. Keying material and associated classified documentation shall be safeguarded in accordance with the access, storage, and transportation requirements of NACSI No. 4005/CSISM/CCI Manual. The KY-71 terminal and associated CIKs should be zeroized prior to transport, storage, and maintenance.

14. Access to Installed KY-71s.a. Unkeyed.

(1) An unkeyed terminal must be safeguarded in accordance with NTISSI No. 4001/CSISM/CCI Manual. It may be used for unclassified and nonsensitive calls by persons who meet the access requirements of NTISSI No. 4001/CSISM/CCI Manual.

(2) Subject to department, agency, or command policy, cognizant security authorities may grant waivers to permit foreign nationals unescorted access to an unkeyed, installed terminal, regardless of the terminal's release status, if all of the following conditions are met. Under all these conditions, foreign nationals may also be allowed to use the STU-II as an unsecure commercial telephone. Approval must be obtained from DIRNSA (ATTN:) prior to allowing such access by personnel of Communist bloc or other countries hostile to U.S. interests.

(a) Such access is in conjunction with building maintenance, custodial duties, or other operational responsibilities normally performed by such personnel unescorted in the area before the terminal is installed;

(b) The terminal is installed within a U.S.-controlled facility or a combined facility with permanent U.S. presence;

(c) The cognizant security authority has determined that the risk of tampering with the terminal by foreign nationals, which could result in compromise of U.S. information that is classified or unclassified, but sensitive,

NTISSI No. 3012

is acceptable in light of the local threat and vulnerability, and the information is receiving the protection warranted by its classification, special security controls, and intelligence life; and

(d) All associated CIK(s) are in protective custody or storage.

b. Keyed.

(1) When the terminal is keyed, it must be afforded protection commensurate with the classification of the key it contains, as required by NACSI No. 4005/CSISM/CCI Manual. Normally, no unescorted foreign national access will be allowed to the keyed terminal. If operationally required, authorized persons may permit others not normally authorized to use the keyed terminal (e.g., persons not assigned to the organization and foreign nationals) under the following conditions:

(a) The foreign nationals are civilian employees of the U.S. Government or assigned to a combined facility.

(b) The foreign nationals hold an equivalent clearance comparable to the highest classification of keying material.

(c) The CCI remains U.S. property and a U.S. citizen is responsible for it.

(d) The communications to be protected are determined to be essential to the support of U.S. or combined operations.

(e) Keying of CCIs with classified U.S. key is performed by U.S. personnel. (Waivers may be granted by DIRNSA (ATTN:). Keying of CCIs with allied key or unclassified U.S. key may be done by authorized foreign nationals).

(2) If a terminal is to be installed and operated in a foreign country at a facility which is either unmanned or manned entirely by foreign nationals, in addition to the requirements of subparagraphs (a) and (b), above, special

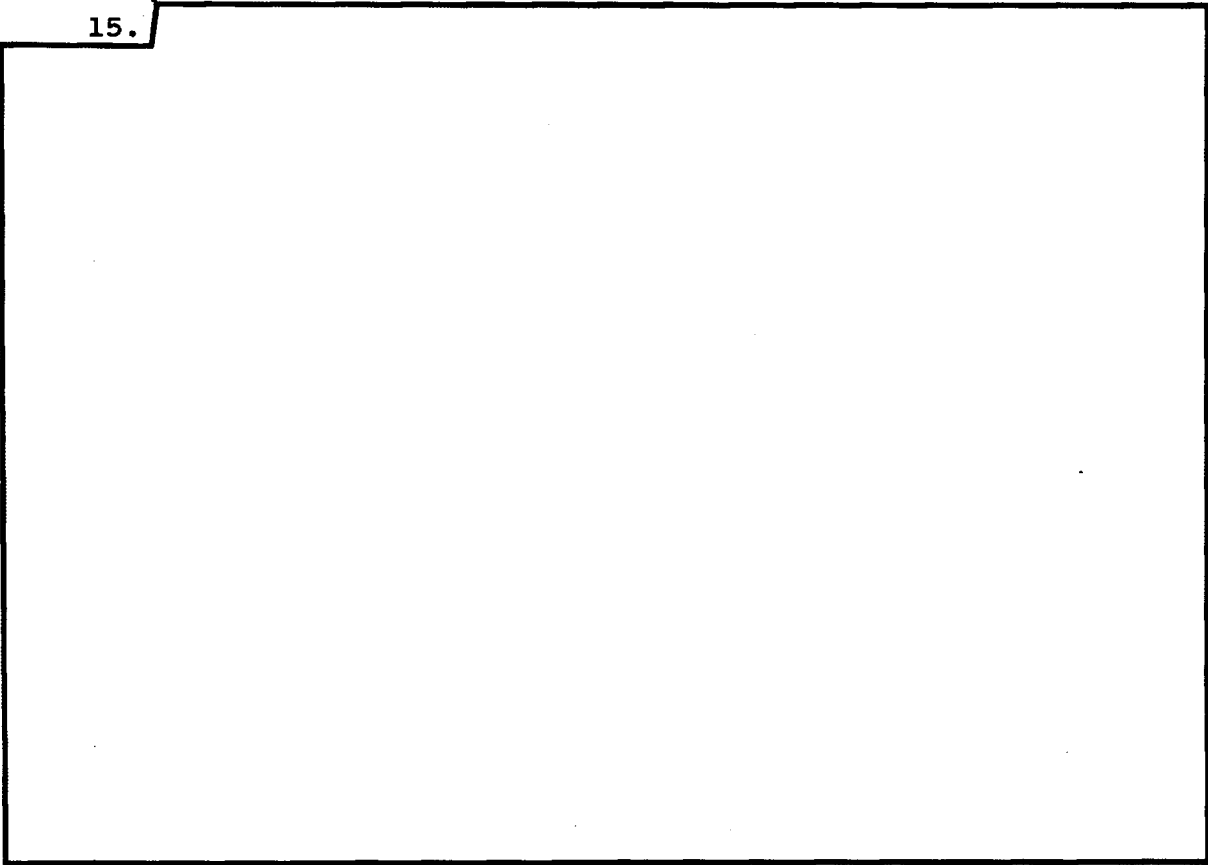
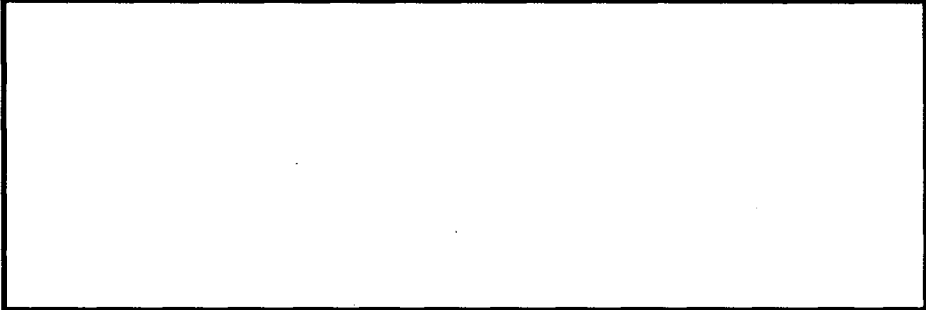
(b) (3) - P.L. 86-36

NTISSI No. 3012

security measures may be required: vault areas, locking bars, safes, alarms, etc. Each such installation must be approved in advance by DIRNSA (ATTN:) on a case-by-case basis.

NOTE: KY-71 terminals normally should not be moved from an environment where the tampering risk presented by foreign national access is acceptable, to a more sensitive environment where the risk is not acceptable.

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



NTISSI No. 3012

16.

a.

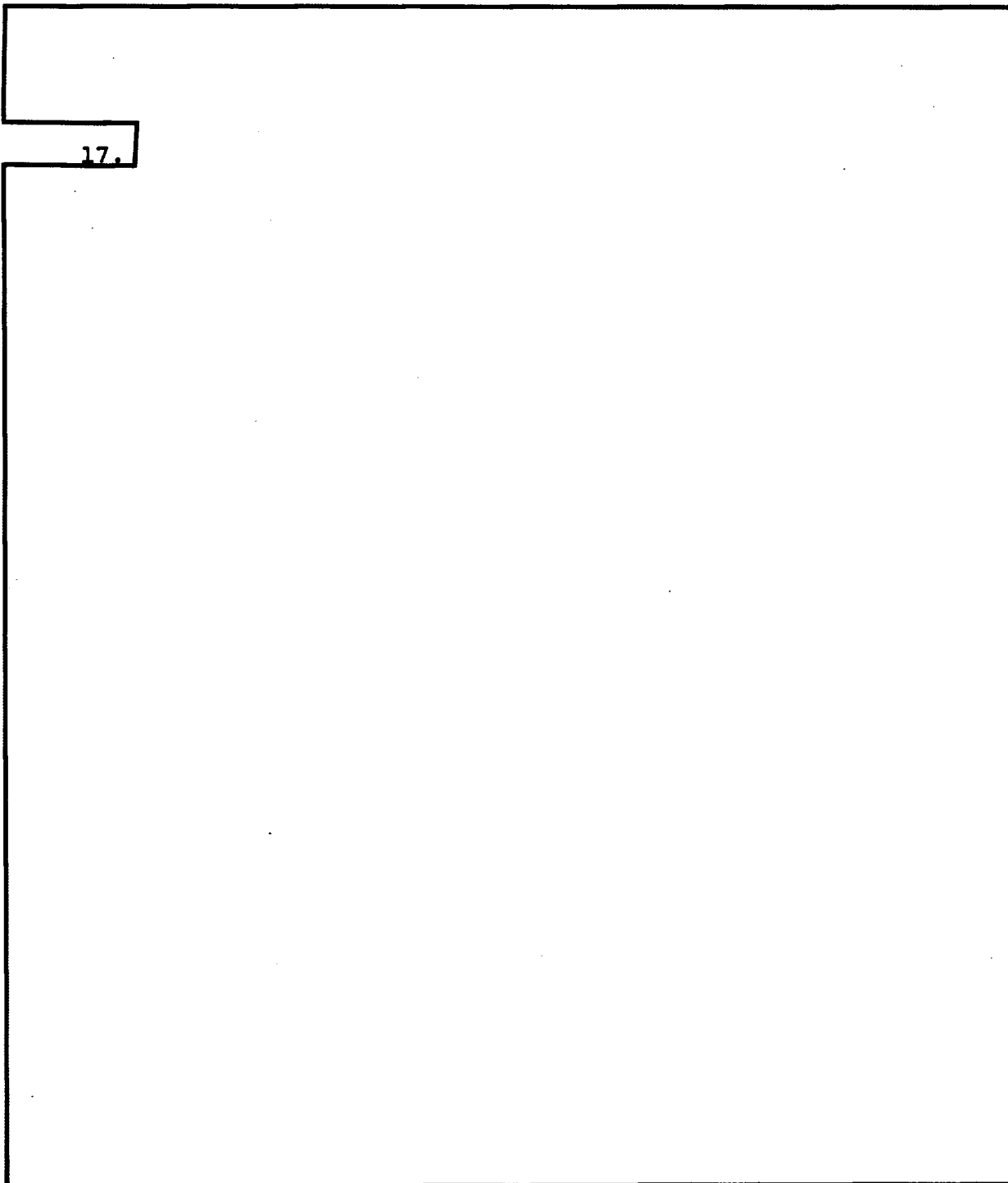
b.

c.

d.

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

NTISSI No. 3012



17.

NTISSI No. 3012

18. Enable Code. The enable code for the HYX-71 desk set is generated locally and protected as SECRET information. In order to prevent unauthorized use of a keyed terminal through the desk set enable code, the enable code should be changed monthly. If the KY-71 terminal and associated desk set(s) are located in an area where access is strictly limited to appropriately cleared persons, the enable code does not have to be changed on a regular basis.

19.

a.

b.

NTISSI No. 3012

SECTION IX - EMERGENCY PROCEDURES

20. An emergency action plan shall be prepared in accordance with the guidance of NTISSI No. 4004/CSISM/CCI Manual. The standard priority for destruction of COMSEC material should be followed for KY-71 COMSEC material with the following additions:

a. Operational CIKs. Operational CIKs should be zeroized by removing the CIK battery when it is no longer necessary to maintain secure communications.

b. 

SECTION X - REPORTABLE INCIDENTS

21. A general listing of reportable COMSEC incidents and the standards for their reporting are contained in NTISSI No. 4003/CSISM/CCI Manual. Additional incidents, specific to the KY-71, follow:

a. Reportable Cryptographic Incidents.

(1) Use of a contingency Vn without the prior authorization of the controlling authority.

(2) Failure to update a Vn at least weekly (unless an exception has been approved by the controlling authority).

(3) Failure to update a CIK at least weekly (unless an extension has been authorized by the cognizant security authority).

b. Reportable Physical Incidents.

(1) Unauthorized, unescorted operational use of a HYX-71 desk set.

(2) Unauthorized extraction or loading of keys.

NTISSI No. 3012

(3)



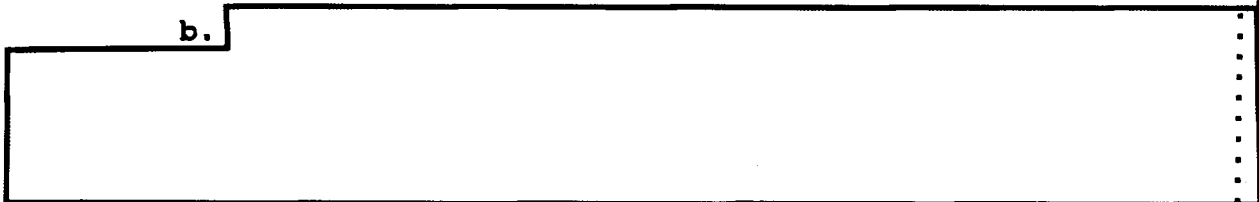
- (4) Failure to disable a desk set when not under the control of an authorized user.

22. Controlling Authority Functions. The controlling authority and evaluating functions contained in NTISSI No. 4006/CSISM/CCI Manual and NTISSI No. 4003/CSISM/CCI Manual are modified for the KY-71 as follows:

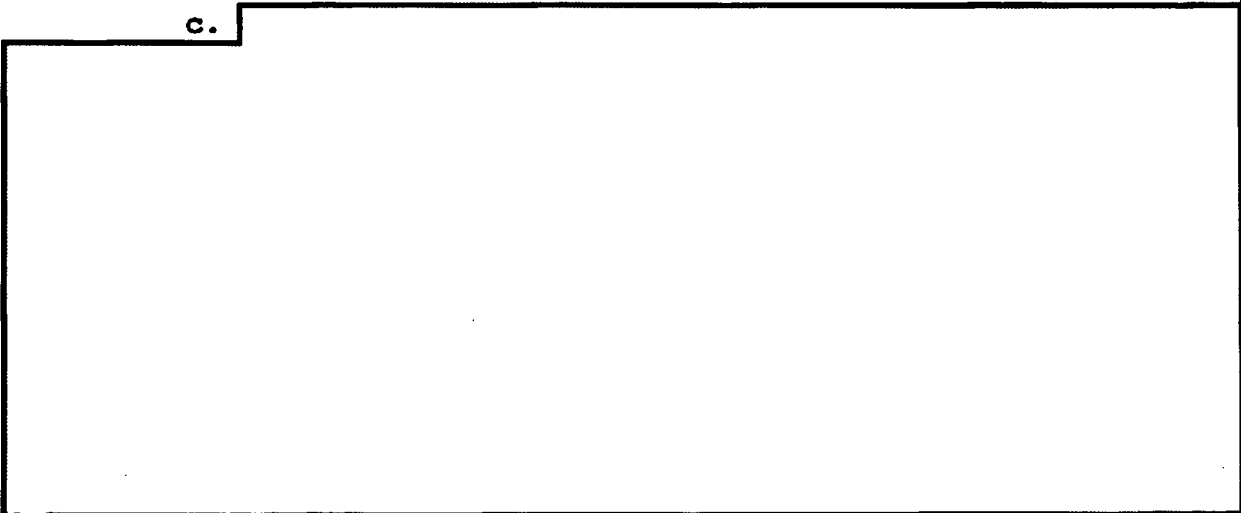
a.



b.



c.



23. Actions For Compromise Recovery. Actions taken for recovering from a compromise involving KY-71 COMSEC material will be in accordance with the guidance of NTISSI No. 4006/CSISM/CCI Manual. The following specific guidance also applies:

NTISSI No. 3012

a.

b.

(1)

(2)

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

NTISSI No. 3012



- 2 Encls:
- Annex A - Classification, Marking, and Minimum Accounting Legend Codes
 - Annex B - System Security Guidance

ANNEX ACLASSIFICATION, MARKING, AND MINIMUM ACCOUNTING LEGEND CODES

The following classifications and minimum Accounting Legend Codes (ALC) apply to the TSEC/KY-71 COMSEC materials:

| <u>COMSEC EQUIPMENT/MATERIAL</u> | <u>CLASSIFICATION MARKING</u> | | <u>ALC</u> |
|--|---|------------------------|------------|
| | <u>UNKEYED</u> | <u>KEYED</u> | |
| KY-71A/B Terminal | UNCL CONTROLLED CRYPTOGRAPHIC ITEM (CCI) | Same Class. as Keys | 1 |
| KYK-71 | UNCL (CCI) | UNCL (CCI) | 2 |
| HYX-71 | N/A | N/A | 4 |
| Z-AMX | N/A | N/A | 4 |
| KYK-13, Common Fill Device | UNCL (CCI) | Same Class. as Keys | 2 |
| KOI-18, Tape Reader | UNCL (CCI) | N/A | 2 |
| KAO-191, Operating Instructions for KY-71 | CONF | N/A | 1 |
| KAM-429, Type I Maintenance Manual | CONF | N/A | 1 |
| KAM-430, Type IV Maintenance Manual | SECRET | N/A | 1 |
| Unique Key (Vu) | SECRET CRYPTO or TOP SECRET CRYPTO | N/A | 1 |
| Net Key (Vn) | UNCL, CONF, SECRET or TOP SECRET CRYPTO | N/A | 1 |

ANNEX A to
NTISSI No. 3012

| <u>COMSEC EQUIPMENT/MATERIAL</u> | <u>CLASSIFICATION MARKING</u> | | <u>ALC</u> |
|----------------------------------|-------------------------------|--------------|------------|
| | <u>UNKEYED</u> | <u>KEYED</u> | |
| E-EJQ KY-71A/B Board | UNCL (CCI) | UNCL (CCI) | 2 |
| E-FFV KY-71A/B Board | UNCL (CCI) | UNCL (CCI) | 2 |
| F-EBN KY-71A/B Board | UNCL (CCI) | UNCL (CCI) | 2 |

ANNEX A to
NTISSI No. 3012

A-2

~~FOR OFFICIAL USE ONLY~~

ANNEX BSYSTEM SECURITY GUIDANCE

The fundamental purpose of the KY-71 is to provide a readily available, easy to use, secure telephone capability for personnel who have a need to discuss and transmit classified or sensitive information. The greatest security threat to telephone communications is their vulnerability to hostile intercept and exploitation during transmission over the telephone network. Users should be aware, however, that incorrect use of the terminal and desk set may introduce security breaches, which could affect not only their own communications, but the integrity of communications of other STU-II system users as well. Therefore, the following guidance is provided to cover those areas where doctrine is not prescribed, but where local security measures should be implemented.

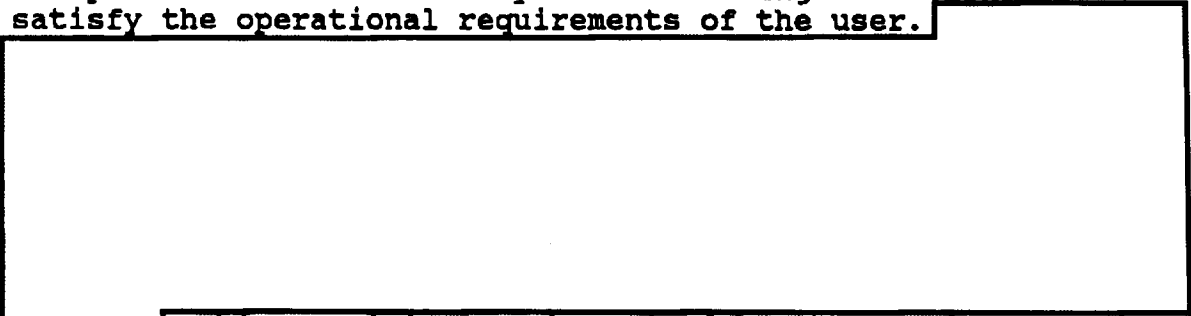
1. Acoustic Security. The cognizant security authority should implement a common-sense approach to acoustic security concerns since introduction of the KY-71 into an area should not change those requirements normally implemented in areas used for classified or sensitive operations. Ideally, all persons assigned to an area where classified work is carried out would have the same clearance and need-to-know. Where this is not possible, local procedures should be implemented to prevent uncleared persons not authorized access to the information from overhearing classified telephone conversations.

2. Installation in Residences. Installation of KY-71s in the residences or quarters of U.S. military or civilian officials may be authorized on a case-by-case basis by the cognizant military or civilian authority. There is no general requirement to store the KY-71 terminal in a security container. However, in cases where there is a threat of penetration or a physical security problem, the KY-71 terminal should be stored in an NSA-approved KY-71 security container or other appropriate security container; e.g., a security container obtained from the Federal Supply System, a specially

ANNEX B to
NTISSI No. 3012

~~FOR OFFICIAL USE ONLY~~

designed security container which has been approved by DIRNSA for storage of cryptomaterial, or in accordance with the security container requirements of NACSI No. 4005/CSISM/CCI Manual. Each installation must be evaluated on its individual security merits since most residences do not provide a high degree of inherent security. For this reason, placing a secure telephone in a residence may involve taking some risks to satisfy the operational requirements of the user.



This provision may be waived by the cognizant security authority if the unoccupied residence is considered adequately secure to preclude any reasonable chance of theft. The KY-71 should be used only by the person for whom it is installed. All of the security requirements should be observed for preventing unauthorized access to the keyed KY-71 terminal and to classified and sensitive information. Users should be aware of the vulnerability of their residences to clandestine electronic surveillance.

3. Safeguarding Desk Sets, Junction Boxes, Wirelines, and Fiber Optics.

a. All desk sets, junction boxes, and inter-connecting wirelines comprise a secure subscriber facility and must be installed to meet the requirements of NACSIM No. 5203. Users should consult the appropriate security regulations for additional guidance on the protection of classified information, including restrictions on conducting classified discussions outside of secure areas. When using a facsimile or personal computer with the KY-71, refer to NTISSI No. 7000 for the level of countermeasures protection your system requires. Specific questions by users and installers regarding department or agency-unique requirements should be directed to

ANNEX B to
NTISSI No. 3012

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

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

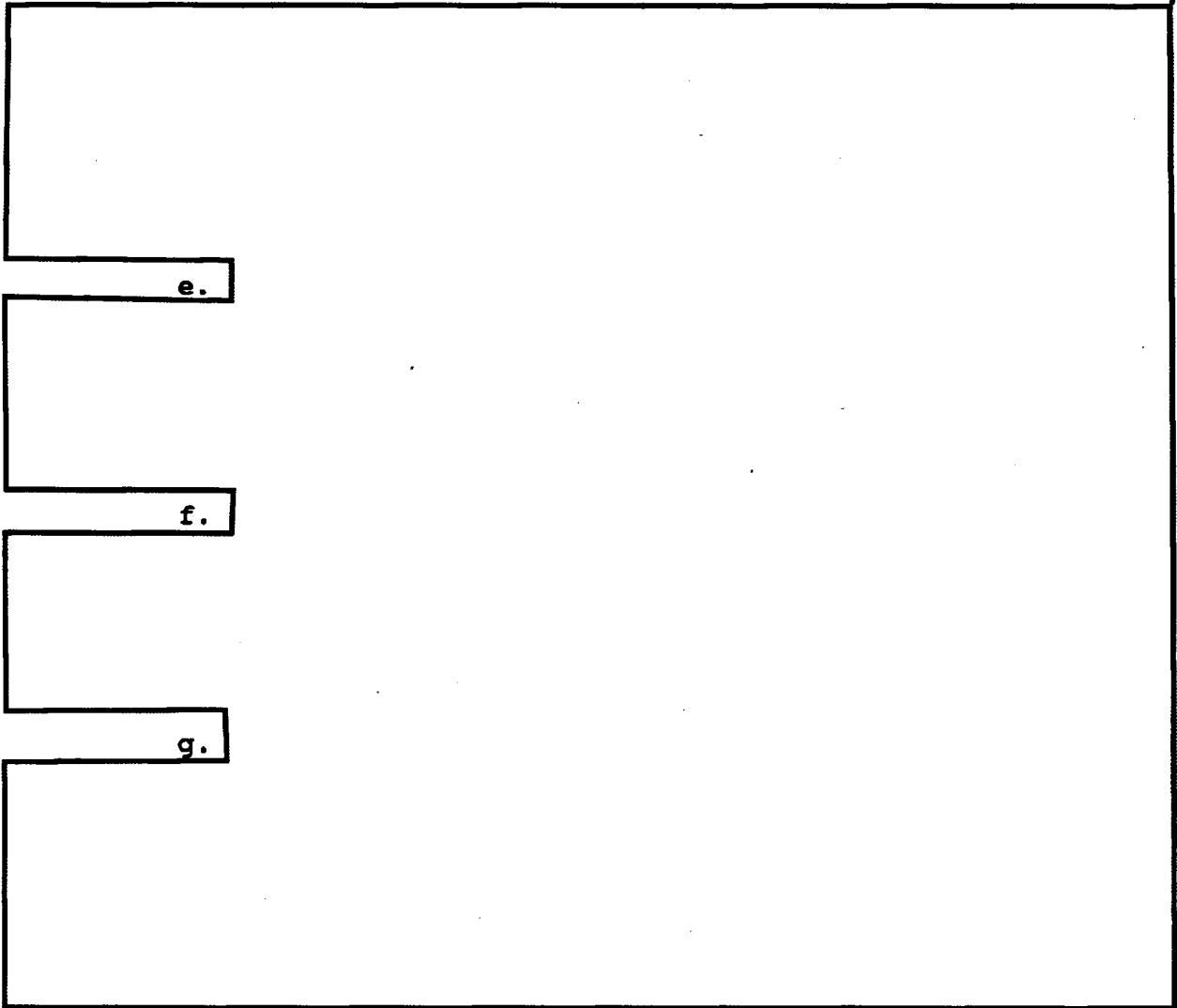
their local security officer or their organization's Countermeasures Advisory Panel member, whichever is more appropriate for their organization. All installers and users should direct their questions to their own department or agency's security office. Each department or agency may have its own installation and security requirements, which would apply in addition to this minimum guidance.

b.

c.

d.

ANNEX B to
NTISSI No. 3012



h. Whenever desk sets are left unattended by appropriately cleared personnel, they shall be disabled in accordance with the operating instructions, unless security measures in force are adequate to ensure that unauthorized persons cannot have access to them.

ANNEX B to
NTISSI No. 3012

i. For the FSTS users, there are two classifications of key available. It is the responsibility of the user to determine whether SECRET or TOP SECRET key is necessary for the terminal. Net users must determine the classification of key they require.

j. The KY-71 is designed to encrypt synchronous 2400 bps data. If users plan to attach asynchronous data terminals that operate at a lower speed, they must obtain prior permission from DIRNSA (ATTN:).

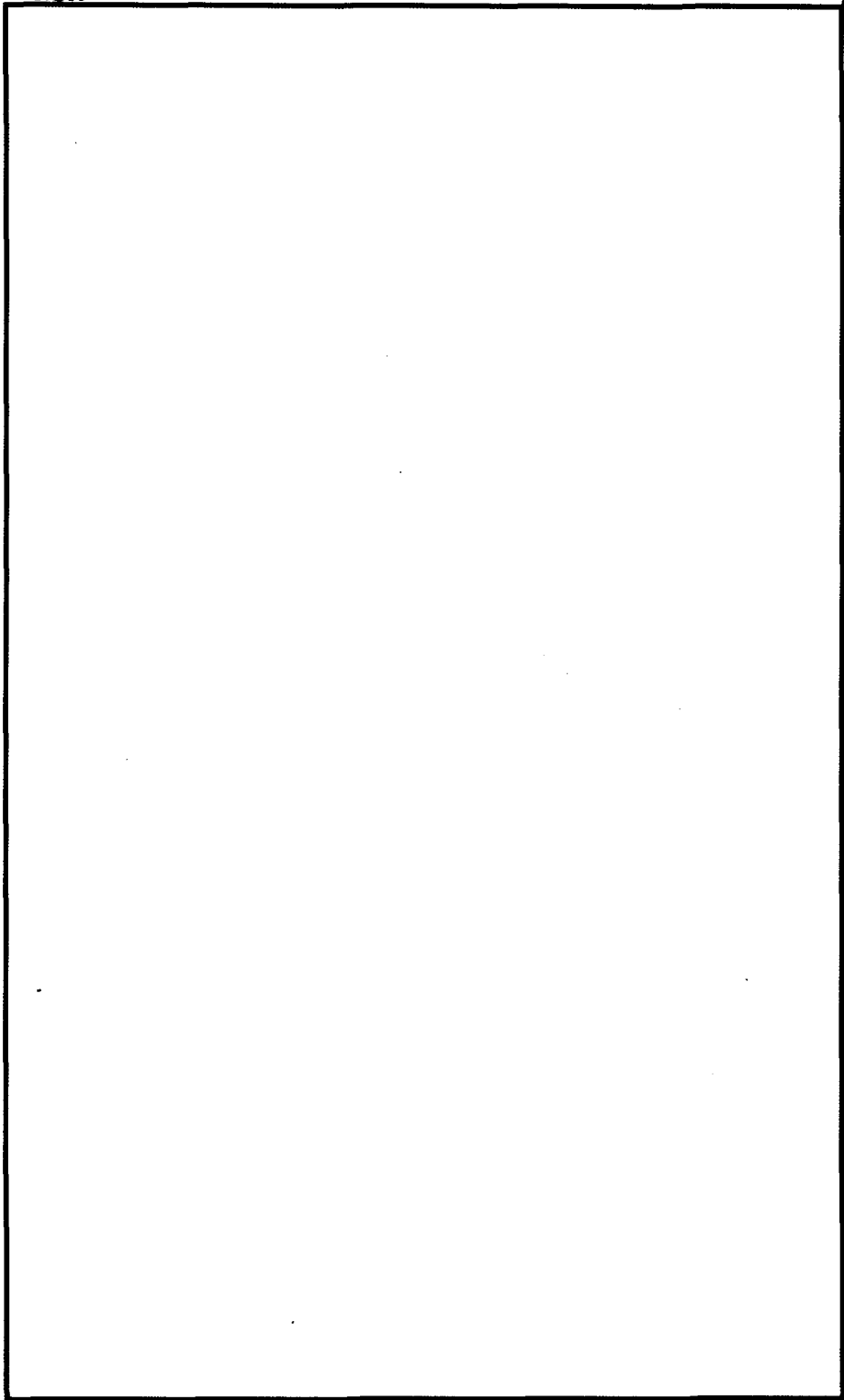
4. HYX-71 Use Criteria. Normally, unescorted access to or use of enabled HYX-71 desk sets of FSTS KY-71s shall be limited to U.S. citizens or resident alien employees of the U.S. Government or members of the U.S. Armed Forces who are properly cleared. Use of the HYX-71 desk sets may be granted to a U.S. or foreign national (who is not already an authorized KY-71 user) provided that individual's official duties require such use. An authorized KY-71 user must initiate the secure call, identify the calling party to the called party (including nationality, if appropriate), and stipulate the classification limit of that call. Identification of the person desiring to speak to the called party and stipulation of the classification limit of that call should take place only after secure communications have been established. Normally, whenever such an individual uses the HYX-71 to make a KY-71 secure call, that individual must be under the escort of an authorized KY-71 user. The cognizant commander or civilian official may waive this escort requirement when circumstances are such that it would clearly be inappropriate; e.g., a foreign dignitary at a U.S. embassy, or a foreign general at a joint or combined command. Under no circumstances should such users have unescorted access to the keyed KY-71 or associated classified COMSEC material. The HYX-71 and the area should be checked for technical surveillance devices after such unescorted use.

ANNEX B to
NTISSI No. 3012

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

NTISSI No. 3012

DISTRIBUTION:
NSA



NTISSI No. 3012

