

~~SECRET~~

NTISSI No. 3010
19 July 1989

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR THE

KY-65A/75A (U)

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

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~SECRET~~

~~SECRET~~**NTAISS**NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY**NATIONAL MANAGER**

19 July 1989

FOREWORD

1. ~~(S)~~ In November 1987, all U.S.-held KY-65 and KY-75 equipment were redesignated as KY-65A and KY-75A equipment because of cryptographic modifications. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3010, "Operational Security Doctrine for KY-65A/75A," promulgates operational security doctrine for the KY-65A/75A equipment and supersedes National COMSEC Instruction (NACSI) No. 8101A, "Operational Doctrine for PARKHILL," dated February 1979.
2. (U) The most significant changes included in this update involve the removal of the usage restrictions in paragraph 5.a. of NACSI No. 8101A. Revisions reflect the declassification of and CONTROLLED CRYPTOGRAPHIC ITEM marking for the KY-65A/75A equipment, and revised foreign access requirements that are applicable to all controlled cryptographic item (CCI) equipment (paragraph 9.b.).
3. (U) This instruction is NOT RELEASABLE TO FOREIGN NATIONALS without the specific approval of the National Manager, NTAISS.
4. (U) Extracts of this instruction may be made for official purposes. Extracts of classified paragraphs shall be marked with the appropriate classification, and extracts of unclassified paragraphs shall be marked FOR OFFICIAL USE ONLY.
5. (U) Additional copies of this NTISSI may be requested from:

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

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~~~SECRET~~

~~SECRET~~

NTISSI No. 3010

OPERATIONAL SECURITY DOCTRINE FOR KY-65A/75A (U)

SECTION

PURPOSE AND SCOPE	I
REFERENCES	II
DEFINITIONS	III
SYSTEM ELEMENTS	IV
APPLICATION	V
CLASSIFICATION AND MARKING	VI
KEYING	VII
TRANSMISSION SECURITY	VIII
PHYSICAL SECURITY	IX

SECTION I - PURPOSE AND SCOPE (U)

1. (U) This instruction provides operational security doctrine for the KY-65A/75A cryptosystem. Its provisions apply to all departments and agencies of the U.S. Government and their contractors.

SECTION II - REFERENCES (U)

2. (U) The following references are cited in this instruction:

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

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

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

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

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

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~SECRET~~

NTISSI No. 3010

SECTION III - DEFINITIONS (U)

3. (U) Definitions contained in NCSC-9 apply. For the purpose of this instruction, the following definitions also apply:

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

b. (U) Foreign national. A person who is not a native or a naturalized citizen of the United States and is not categorized as a U.S. resident alien.

c. (U) Resident alien. A citizen of a foreign country who is legally residing in the United States on a permanent basis.

d. (U) Traffic Encryption Key (TEK). Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

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

SECTION IV- SYSTEM ELEMENTS (U)

4. (U) Annex A contains the COMSEC material of the KY-65A/75A cryptosystem.

SECTION V - APPLICATION (U)

5. (U) The KY-65A/75A is an analog speech security equipment that is approved for use on all types of narrowband voice radio and wireline circuits that cannot be secured by existing digital crypto-equipment. When used with appropriately classified key, KY-65A/75A equipment is approved for safeguarding all classifications and categories of tactical voice traffic. When used with unclassified key in networks involving uncleared operators, the system is authorized to protect only unclassified information. KY-65A/75A equipment is cryptographically incompatible with all other U.S. cryptosystems.

NTISSI No. 3010

SECTION VI - CLASSIFICATION AND MARKING (U)

6. (U) General COMSEC classification guidance is contained in NTISSI No. 4002. System-specific classification doctrine is expressed below:

a. (U) Correspondence. Technical or operational correspondence relating to the KY-65A/75A cryptosystem must be classified on the basis of content. Normally, information relating to the cryptographic functioning of the KY-65A/75A equipment must be classified at least CONFIDENTIAL. Information concerning cryptographic or TEMPEST vulnerabilities of the equipment must be classified at least SECRET and marked NOT RELEASABLE TO FOREIGN NATIONALS. COMSEC correspondence is not releasable to the Defense Technical Information Center.

b. (U) Unclassified Information. The following aspects of the KY-65A/75A cryptosystem are UNCLASSIFIED:

(1) (U) The fact that the system decrypts/encrypts voice communications.

(2) (U) Crypto-equipment/radio interface characteristics.

(3) (U) Secure radio range, intelligibility, and encrypted signal characteristics.

(4) (U) Electrical input and output characteristics of the KY-65A/75A equipment.

(5) (U) The fact that the KY-65A and KY-75A interoperate with each other, but are incompatible with other crypto-equipment.

(6) (U) The key storage capacity of the KY-65A/75A equipment and associated fill devices.

(7) (U) Physical descriptions of the KY-65A/75A equipment fill devices and ancillaries.

(8) (U) The fact that the KY-65A/75A equipment and the KYK-13 and KOI-18 fill devices are marked CONTROLLED CRYPTOGRAPHIC ITEM.

NTISSI No. 3010

c. (U) Key. KY-65A/75A key is centrally produced in punched tape form and may be unclassified or classified depending on operational use of the key.

(1) (U) Operational, exercise, test, and training key tapes are classified on the basis of the classification of the traffic they are intended to protect. They are regularly superseded, packaged in protective plastic canisters, and marked CRYPTO. Normally, operational tapes are SECRET, and exercise, test, and training tapes are CONFIDENTIAL.

(2) (U) Maintenance key tapes (for in-shop or back-to-back testing) are unclassified. They are packaged in clear plastic boxes, and their segments may be reused until they become unserviceable.

SECTION VII - KEYING (U)

7. (U) Doctrine relating to keying of KY-65A/75A equipment is expressed below:

a. (U) Keying Methods.

(1) KY-65A/75A key in punched tape form may be loaded directly in KY-65A/75A equipment by means of a KOI-18 tape reader or inserted into a KYK-13 electronic transfer device and then loaded into KY-65A/75A equipment. Key in electronic form must be loaded into KY-65A/75A equipment from a KYK-13

(2) In operational situations where tactical maneuver units must interoperate, but do not hold key in common, KY-65A/75A key may be generated in the field or converted from tape to electronic form; the key may then be transferred electrically to user sites by KG-84A/C or KY-57/58-protected circuits or KW-46 (fleet broadcasts).

b. (U) Security Limitations.

(1) (U) KY-65A/75A key may not be stored in KYK-13 devices as a substitute for canister storage of key tape. However, key may be temporarily held in KYK-13s for up to 12 hours, in support of planned or scheduled rekeying operations.

(2) (U) Key tape segments must not be removed from their canisters until immediately ready for use and may not be issued to users as extracts.

~~SECRET~~

NTISSI No. 3010




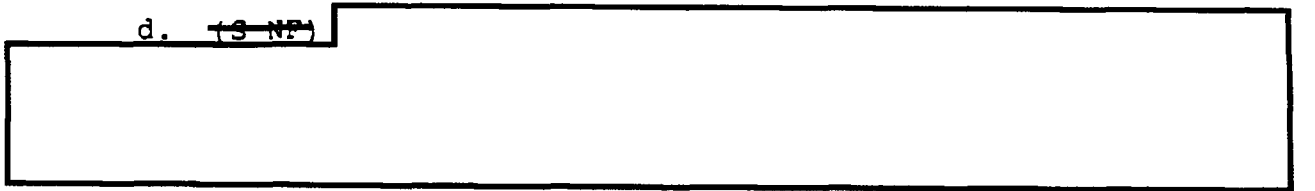
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

c. (U) Cryptoperiod. Each KY-65A/75A cryptoperiod is limited to 24 hours. In emergency situations where resupply of key is impossible, controlling authorities may extend cryptoperiods up to 24 additional hours. Longer cryptoperiod extensions must be approved by DIRNSA. Any unauthorized extensions are reportable as COMSEC incidents.

d. (U) Cryptonet Size. There is no maximum size for KY-65A/75A cryptonets. However, operational considerations, such as the potential impact of key compromises, dictate that the number of stations holding identical KY-65A/75A key be kept as low as operationally feasible.

SECTION VIII - TRANSMISSION SECURITY (U)

8. (U) Transmission security considerations affecting the KY-65A/75A cryptosystem are expressed below:

- a. ~~(S)~~ 
- b. ~~(S)~~ 
- c. ~~(S)~~ 
- d. ~~(S NF)~~ 

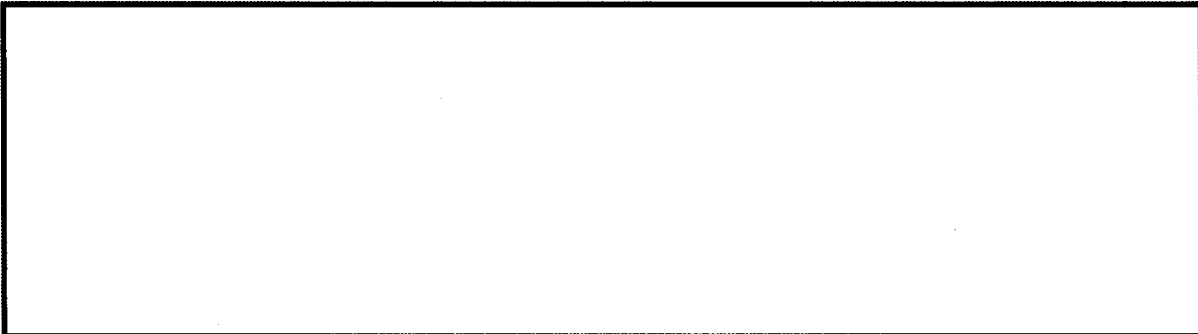
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

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

~~SECRET~~

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

NTISSI No. 3010

SECTION IX - PHYSICAL SECURITY (U)

9. (U) Doctrine for safeguarding the classified material and unclassified-CCI elements of the KY-65A/75A cryptosystems is contained in NACSI No. 4005 and NTISSI No. 4001, respectively. Supplementary security doctrine is expressed below:

a. (U) Uncleared and Foreign National Users. Uncleared U.S. or foreign nationals may be allowed to talk on KY-65A/75A-secured circuits in the presence and under the supervision of appropriately cleared persons, provided the communications net (or the distant party) has first been alerted to the situation.

b. (U) Foreign Access. Subject to department, agency, or command policy, cognizant security authorities may grant waivers to permit foreign nationals unescorted access to installed KY-65A/75A equipment, regardless of the release status of the equipment, under the conditions listed below. Approval of the National Manager must be obtained prior to allowing such access by foreign nationals of countries hostile or unfriendly to the United States.²

(1) (U) For unkeyed KY-65A/75A equipment:

(a) (U) Such access is in conjunction with building maintenance, custodial duties, or other operational responsibilities normally performed by such persons unescorted in the area containing the equipment, and

¹ Available from the National Security Agency,

² A listing of hostile and unfriendly countries may be obtained from the National Security Agency, (ATTN:)

~~SECRET~~

NTISSI No. 3010

(b) (U) The crypto-equipment is installed within a facility that is a U.S.-controlled facility or a combined facility with a permanent U.S. presence (not a host nation facility); and

(c) (U) The cognizant security authority has determined that the risk of tampering with the equipment which could result in compromise of U.S. classified or sensitive information, is acceptable in light of the local threat, vulnerability, and the sensitivity of the information being protected, as indicated by its classification, special security controls, and intelligence life.

(2) (U) For keyed KY-65A/75A equipment, in addition to all of the requirements for unkeyed equipment, all the following apply for unescorted access or use by foreign nationals:

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

(b) (U) The foreign nationals hold a clearance at least equal to the highest level of keying material or information being processed;

(c) (U) The equipment remains U.S. property and responsibility for the equipment is overseen by a U.S. citizen;

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

(e) (U) U.S. users communicating with such terminals are made aware of foreign national-user status.

(3) (U) Keying of KY-65A/75A equipment with classified U.S. key must be done by appropriately cleared U.S. citizens, but waivers may be granted by DIRNSA (ATTN:). Keying of equipment with allied key or unclassified U.S. key may be done by authorized foreign nationals.

(4) (U) Where there is an operational necessity to install and operate a KY-65A/75A in a foreign country at a facility which is either unmanned or manned entirely by foreign nationals, the installations must be approved in advance by DIRNSA (ATTN:).

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

NTISSI No. 3010

[redacted], on a case-by-case basis. U.S. citizens will be required to install and control the equipment. Special security measures will be required (e.g., equipment locking bars, alarms, vault areas, safes, etc.) for these types of installations in order to prevent unauthorized access to the equipment by foreign nationals.

(5) (U) KY-65A/75A equipment should not be moved from an environment where there has been foreign-national access, to a more sensitive environment where the risk is unacceptable. If such a move is an operational necessity, it must receive the prior approval of the cognizant security authority and all equipment must be examined by qualified COMSEC maintenance personnel for signs of tampering. Any evidence of tampering shall be reported as a COMSEC incident, and the equipment removed from operational use pending notification by DIRNSA.

10. (U) Routine and Emergency Destruction. NTISSI No. 4004 describes the routine and emergency destruction requirements for CCIs.

11. (U) A general listing of reportable COMSEC insecurities and the standards for their reporting are contained in NTISSI No. 4003.

Encl:

Annex, Components of KY-65A/75A Cryptosystem

ANNEXCOMPONENTS OF KY-65A/75A CRYPTOSYSTEM (U)

<u>ITEM</u>	<u>ACCOUNT- ABILITY</u>	<u>CLASS./ MARKING</u>	<u>CLEARANCE FOR ACCESS</u>	
			<u>UNKEYED</u>	<u>KEYED</u>
KY-65A Manpack, Portable, Vehicular Crypto- equipment	ALC-1	UNCL-CCI	Not Required	Same as Key
KY-75A Airborne, Shipboard Crypto-equipment	ALC-1	UNCL-CCI	Not Required	Same as Key
KYK-13 Electronic Transfer Device	ALC-2	UNCL-CCI	Not Required	Same as Key
KOI-18 Tape Reader	ALC-2	UNCL-CCI	Not Required	Does Not Retain Key
HYX-60 PARKHILL Commercial Telephone Adapter	ALC-4	UNCL	Not Required	
HYX-65-1 PARKHILL Tactical Tele- phone Adapter (Remote Unit)	ALC-4	UNCL	Not Required	
HYF-65 PARKHILL Suitcase Tele- phone Adapter	ALC-4	UNCL	Not Required	
Z-AKE AC/DC Power Supply	ALC-4	UNCL	Not Required	
Z-AKF Vehicular (DC) Power Supply	ALC-4	UNCL	Not Required	
Z-AGK Battery Pack	ALC-4	UNCL	Not Required	

ANNEX TO
NTISSI No. 3010

~~FOR OFFICIAL USE ONLY~~

<u>ITEM</u>	<u>ACCOUNT- ABILITY</u>	<u>CLASS./ MARKING</u>	<u>CLEARANCE FOR ACCESS</u>	
			<u>UNKEYED</u>	<u>KEYED</u>
Z-AKR Remote Control Unit I	ALC-4	UNCL	Not Required	
Z-AKS Remote Control Unit IIIA	ALC-4	UNCL	Not Required	
Z-AKT Remote Control Unit IIIB	ALC-4	UNCL	Not Required	
Z-AKV Remote Control Unit IIA	ALC-4	UNCL	Not Required	
Z-AKW Remote Control Unit IIB	ALC-4	UNCL	Not Required	
Z-AKX Aircraft Interface Device	ALC-4	UNCL	Not Required	
ON 500900 KY-65 Wireline Adapter and Ringing Protector	ALC-4	UNCL	Not Required	
KAO-154 Operating Instructions TSEC/KY-65/75 and KY-65A/75A	ALC-1	CONF	CONFIDENTIAL	
KAM-333 Limited Maintenance Manual TSEC/KY-65A	ALC-1	CONF	CONFIDENTIAL	
KAM-334 Limited Maintenance Manual TSEC/KY-75A	ALC-1	CONF	CONFIDENTIAL	
KAM-335 Depot Maintenance Manual TSEC/KY-65A/75A	ALC-1	S	SECRET	

ANNEX TO
NTISSI No. 3010

<u>ITEM</u>	<u>ACCOUNT- ABILITY</u>	<u>CLASS./ MARKING</u>	<u>CLEARANCE FOR ACCESS</u>	
			<u>UNKEYED</u>	<u>KEYED</u>
Operational Key Tape	ALC-1 CRYPTO	TS/S/C/U-	Same as Key	
Exercise Key Tape	ALC-1	S/C/U- CRYPTO	Same as Key	
Test Key Tape	ALC-1	CONF-CRYPTO	Same as Key	
Maintenance Key Tape	ALC-4	UNCL	None	
Training Key Tape	ALC-4	UNCL	None	

ANNEX TO
NTISSI No. 3010

A-3

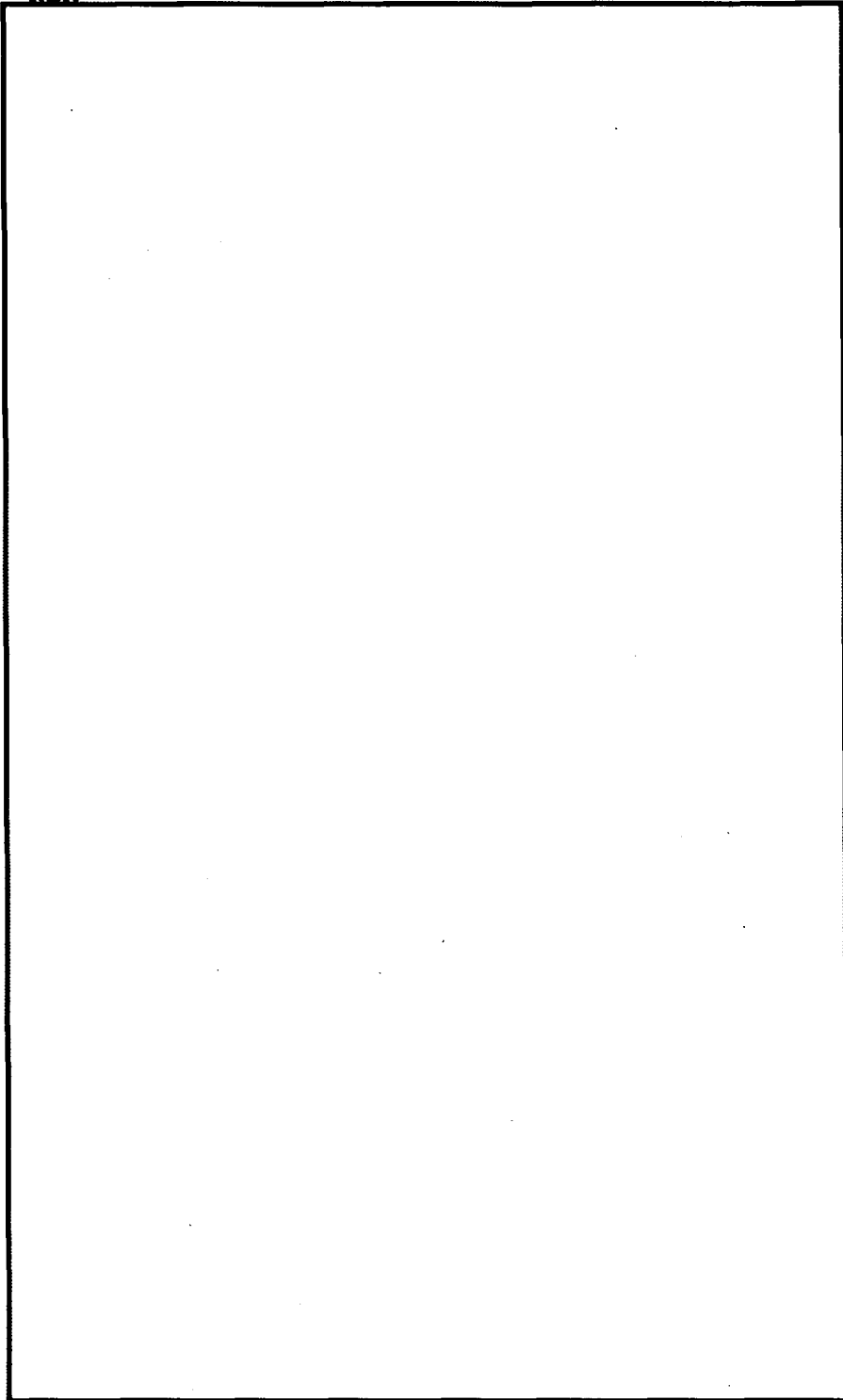
~~FOR OFFICIAL USE ONLY~~

NTISSI No. 3010

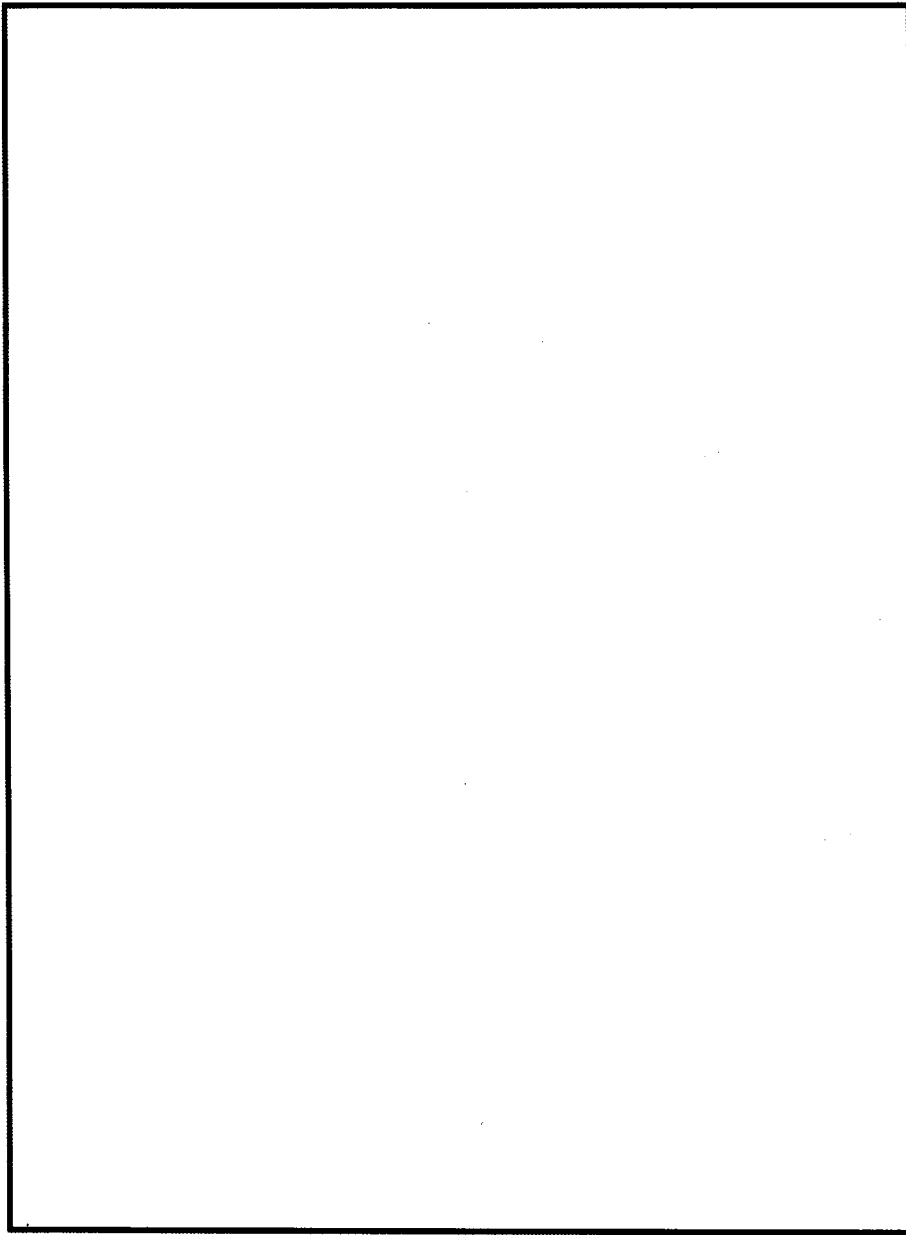
DISTRIBUTION:

NSA

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



NTISSI No. 3010



~~SECRET~~

NTISSI No. 3010

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~SECRET~~