

NTISSI No. 3011
13 October 1989



NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR

KY-57/58, KY-67 AND KYV-2/2A

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

13 October 1989

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3011, "Operational Security Doctrine for KY-57/58, KY-67, and KYV-2/2A," provides security doctrine for the KY-57/58 (VINSON), KY-67 (BANCROFT), and KYV-2/2A cryptosystems. Doctrine applicable to the use of the KY-58 equipment to protect the narrowband component of the Automatic Secure Voice Communications (AUTOSEVOCOM) Network is contained in NTISSI No. 3004.

2. This instruction supersedes NACSI No. 8102, "Operational Doctrine for VINSON and BANCROFT," dated February 1979 and NACSI No. 8104, "Operational Doctrine for KYV-2/TSEC and KYV-2A/TSEC Secure Voice Modules," dated 16 December 1980.

3. Requests for waivers to any of the provisions of this NTISSI must be submitted to the National Manager, NTAISS.

4. The principal differences between this instruction and its predecessors are:

a. Operational security doctrine for the KY-57/58, KY-67, and KYV-2/2A cryptosystems has been consolidated.

b. Revisions have been made throughout to reflect the declassification and CONTROLLED CRYPTOGRAPHIC ITEM (CCI) marking of the KY-57/58, KY-67, and KYV-2/2A equipment.

c. New doctrine for managing KY-57/58, KY-67, and KYV-2/2A key in electrical form is included, pending the promulgation of general doctrine in this area elsewhere.

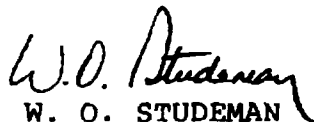
d. The previous requirement that KY-57/58 and KY-67 data applications be approved by the Director, National Security Agency on a case-by-case basis has been deleted.

~~FOR OFFICIAL USE ONLY~~

5. Extracts of this instruction may be made for official purposes; such extracts shall be marked FOR OFFICIAL USE ONLY.

6. 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
Vice Admiral, U.S. Navy

~~FOR OFFICIAL USE ONLY~~

NTISSI No. 3011

OPERATIONAL SECURITY DOCTRINE
FOR KY-57/58, KY-67 AND KYV-2/2A

	<u>SECTION</u>
PURPOSE AND SCOPE	I
REFERENCES	II
DEFINITIONS	III
SYSTEM COMPONENTS	IV
APPLICATION	V
CLASSIFICATION AND MARKING	VI
PHYSICAL SECURITY	VII
MANAGING KEY IN ELECTRICAL FORM	VIII
KEYING	IX
REPORTING COMSEC INCIDENTS	X

SECTION I - PURPOSE AND SCOPE

1. This instruction provides operational security doctrine for the KY-57/58, KY-67, and KYV-2/2A cryptosystems. Its provisions apply to all departments and agencies of the U.S. Government and their contractors.

SECTION II - REFERENCES

2. The following references are cited in this instruction:
- a. NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.
 - b. NCSC-9, National COMSEC Glossary, dated 1 September 1982.
 - c. NTISSI No. 4001, Controlled Cryptographic Items, dated 25 March 1985.
 - d. NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.
 - e. NTISSI No. 4003, Reporting COMSEC Insecurities, dated 3 November 1986.

~~FOR OFFICIAL USE ONLY~~

NTISSI No. 3011

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

g. NTISSI No. 3004, Operational Doctrine for AUTOSEVOCOM, dated 1 April 1987.

SECTION III - DEFINITIONS

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

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

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

c. Key Encryption Key (KEK). Key that is used in the encryption and decryption of other keys for transmission (rekeying) or storage.

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

SECTION IV- SYSTEM COMPONENTS

4. COMSEC material comprising the KY-57/58, KY-67, and KYV-2/2A cryptosystems is listed in Annex A.

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

NTISSI No. 3011

SECTION V - APPLICATION

5. The KY-57/58, KY-67, and KYV-2/2A crypto-equipment are [redacted] compatible with each other, [redacted] equipment. [redacted] through its net radio interface, and with the [redacted] secure digital net radio interface unit.

a. KY-57/58 and KY-67. The KY-57/58 and KY-67 cryptosystems provide security for half-duplex, push-to-talk, combat net radio circuits and tactical wirelines. The KY-57 and KY-58 are separate crypto-equipment, while the KY-67 is an integrated radio/crypto-equipment.

b. KYV-2/2A. The KYV-2/2A is a wideband crypto-equipment designed to secure the hand-held AN/PRC-68 VHF FM squad radio.

c. Traffic Classification. When used with appropriately classified key, the KY-57/58, KY-67 and KYV-2/2A crypto-equipment is approved for safeguarding all classifications and categories of voice traffic. This equipment is also authorized to protect all classifications and categories of data traffic.

d. Unclassified Traffic. When used with unclassified key, the KY-57/58, KY-67, and KYV-2/2A cryptosystems are authorized to protect only UNCLASSIFIED information.

SECTION VI - CLASSIFICATION AND MARKING

6. General COMSEC classification guidance is contained in NTISSI No. 4002. System specific classification guidance follows:

a. Publications and Correspondence. Technical or operational publications and correspondence relating to the KY-57/58, KY-67, and KYV-2/2A cryptosystems must be classified on the basis of content. Normally, information relating to the cryptographic functioning of the KY-57/58/67 and KYV-2/2A

NTISSI No. 3011

equipment must be classified at least CONFIDENTIAL.¹ Information concerning cryptographic or TEMPEST vulnerabilities of the equipment must be classified at least SECRET and marked NOT RELEASABLE TO FOREIGN NATIONALS. KY-57/58/67 and KYV-2/2A publications and correspondence are not releasable to the Defense Technical Information Center.

b. Unclassified Information. The following aspects of the KY-57/58, KY-67, and KYV-2/2A cryptosystems are unclassified:

- (1) The fact that the system decrypts/encrypts voice (and in the case of the KY-57/58/67, also data) communications.
- (2) Crypto-equipment/radio interface characteristics.
- (3) Secure voice radio range, intelligibility, and encrypted signal characteristics.
- (4) Electrical input and output characteristics of the equipment.
- (5) The fact that the equipment is interoperable with other secure voice equipment.
- (6) The key storage capacity of the equipment and associated fill devices.
- (7) The bit rate, total synchronization time, total preamble time, and total end of message time of the equipment.
- (8) Physical descriptions of the equipment, fill devices, and ancillaries.
- (9) The fact that the KY-57/58/67 and KYV-2/2A equipment and the KYK-13 and KYX-15, and KOI-18 fill devices are marked CONTROLLED CRYPTOGRAPHIC ITEM.
- (10) KY-57/58/KY-67 SARK (SAVILLE advanced remote keying) procedures.

¹ The cryptographic logic of the KY-57/58/67 and KYV-2/2A has not be declassified; see the definition given above for CCI.

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

NTISSI No. 3011

c. Key. KY-57/58, KY-67, and KYV-2/2A key is centrally produced in punched tape form

Key for these systems may be unclassified or classified at any level.

(1) Operational, exercise, test, and training key tapes are classified on the basis of the classification of the information they are intended to protect. They are regularly superseded, packaged in tamper-resistant plastic canisters, and marked CRYPTO.

(2) 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.

(3) Field-generated key in electronic form is classified on the basis of the classification of the information it is intended to protect.

SECTION VII - PHYSICAL SECURITY

7. Doctrine specifying minimum requirements for safeguarding the classified and unclassified CCI elements of the KY-57/58, KY-67, and KYV-2/2A cryptosystems is contained in NACSI No. 4005 and NTISSI No. 4001, respectively. Supplementary security doctrine is expressed below:

a. Access.²

(1) Access to classified key tapes; to KY-57/58, KY-67, KYV-2/2A equipment containing key; KYK-13 or KYX-15 fill devices containing classified key may be granted to military and civilian employees of the U.S. Government and its contractors

² Access requirements for the various elements of the KY-57/58, KY-67, and KYV-2/2A cryptosystems are stated in Annex A and summarized in Annex B.

NTISSI No. 3011

whose duties require such access and who possess appropriate security clearances.³ Access to key and keyed equipment or fill devices may also be granted to military and civilian employees of foreign governments and international organizations to which the crypto-equipment has been released, whose duties require such access, and who possess appropriate security clearances (e.g., NATO clearance for access to NATO key).

(2) Security clearances are not required for access to unkeyed KY-57/58, KY-67, or KYV-2/2A equipment, to unkeyed KYK-13 and KYX-15 fill devices, or to KOI-18 tape readers. Access to these items may be granted to the following categories of persons, provided their duties require such access:

(a) U.S. citizens and resident aliens who are civilian employees of the U.S. Government or its contractors, or are active duty or reserve members of the U.S. Armed Forces.

(b) Military and civilian employees of foreign governments or international organizations to which the equipment or device has been released.

(3) Uncleared U.S. or foreign persons may be allowed to talk on KY-57/58, KY-67, or KYV-2/2A secured circuits (or to use KY-57/58/67 secured data terminals) in the presence and under the supervision of appropriately cleared persons, provided the communications net has first been alerted to the situation.

(4) Subject to department, agency, or command policy, cognizant security authorities may grant waivers to permit foreign nationals unescorted access to installed U.S. KY-57/58/67 and KYV-2/2A equipment, irrespective of the release status of the equipment under the conditions listed below. The approval of the National Manager must be obtained prior to allowing such access by non-U.S. citizens of countries hostile or unfriendly to the U.S. Information concerning these countries may be obtained from DIRNSA (ATTN: S1).

³ Need-to-know and not security clearance is the criterion for access to unclassified key; to KY-57/58, KY-67, or KYV-2/2A equipment; KYK-13 or KYX-15 fill devices containing only unclassified key.

NTISSI No. 3011

(a) For unkeyed KY-57/58/67 or KYV-2/2A equipment:

1. 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.

2. The crypto-equipment is installed within a facility which is a U.S. controlled facility or a combined facility with a permanent U.S. presence (not a host nation facility), even though the primary staffing is by host nation personnel.

3. 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 unclassified information, is acceptable, in light of the local threat and vulnerability and the sensitivity of the information being protected, as indicated by its classification, special security controls, and intelligence life.

(b) For keyed KY-57/58/67 or KYV-2/2A equipment, in addition to all of the requirements for unkeyed equipment, the following apply for unescorted access or use by foreign nationals:

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

2. The foreign nationals hold a clearance at least equal to the highest level of keying material.

3. The equipment remains U.S. property and responsibility for the equipment is overseen by a U.S. citizen. It is recommended that the presence of such equipment be verified monthly, although no reporting will be required.

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

5. U.S. users communicating with such terminals are made aware of the foreign national status of the user.

NTISSI No. 3011

(c) Normally, keying of KY-57/58/67 and KYV-2/2A equipment with classified U.S. key must be done by U.S. personnel, but waivers may be granted by DIRNSA (ATTN: S13). Keying of equipment with allied key or unclassified U.S. key may be done by foreign personnel authorized access to keyed equipment.

(d) If a KY-57/58/67 or KYV-2/2A 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 paragraphs (4) (a) and (b), above, special security measures may be required, e.g., vault areas, locking bars, safes, and alarms. Each such installation must be approved in advance by DIRNSA (ATTN: S13), on a case-by-case basis.

(e) KY-57/58/67 or KYV-2/2A equipment 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. If such action is an operational necessity, it must receive the prior approval of the cognizant security authority and all such CCIs must be examined by qualified COMSEC maintenance personnel for signs of tampering. Any evidence of tampering shall be reported as a COMSEC incident⁴, and the equipment removed from operational use, pending notification from DIRNSA.

b. Routine Equipment Disposal. Unreparable or excess KY-57/58/67 or KYV-2/2A equipment; KYK-13, KYX-15, or KOI fill devices; and KY-57/58, KY-67 or KYV-2/2A ancillaries and components must be disposed of in accordance with NTISSI No. 4004.

c. Emergency Procedures. Safeguarding of KY-57/58, KY-67, and KYV-2/2A cryptosystem elements under emergency conditions is a responsibility of holders and must be provided for in emergency action plans (see NTISSI No. 4004). The following guidance also applies:

(1) When capture or overrun of a KY-57/58 or KY-67 station appears imminent, the threatened operator should notify the net controller. The operator should then destroy all key tape and zeroize the crypto-equipment and keyed KYK-13s and conduct essential communications in-the-clear.

⁴ The term COMSEC insecurity is now referred to as COMSEC incident, but the associated definition remains unchanged.

NTISSI No. 3011

(2) When capture or overrun of a KYV-2/2A station appears imminent, the threatened operator should notify the net controller, destroy all key tape, and zeroize keyed KYK-13s. The operator should then detach the crypto-equipment from its associated AN/PRC-68 transceiver and remove and zeroize the KYV-2/2A. The transceiver should then be reconnected to the battery case and essential communications conducted in-the-clear.

(3) Reasonable efforts should be made to recover crypto-equipment and supporting documentation lost through catastrophe or hostile action; however, human life must not be jeopardized in such recovery efforts.

d. Guards. Military or civilian guards and security patrols who provide area protection for unattended locations where unkeyed KY-57/58, KY-67, or KYV-2/2A equipment is installed need not be cleared.

SECTION VIII - MANAGING KEY IN ELECTRONIC FORM

8. Effective management of key in electronic form not only facilitates secure communications, but also ensures the availability of accurate holder information which responsible authorities require to evaluate reported COMSEC incidents affecting such key. Individuals who use KY-57/58 or KY-67 equipment to generate key (or who convert tape key to electronic form) for distribution to other users must know the current holders of that key, and must ensure that such key be furnished only to authorized terminals and persons.

a. Electronic Key Transfer. Stations which use KY-57/58 or KY-67 equipment to transfer TEKs electronically must maintain informal records of such transfers, until the affected key is superseded.

b. Physical Key Transfer. Where key in electronic form is transferred physically (e.g., in keyed crypto-equipment or fill devices), issuers must identify and verify "need-to-know" for recipients, and must maintain informal records of such issues until the affected key is superseded.

c. Courier Requirements. Individuals assigned to transport key in electronic form (in keyed crypto-equipment or fill devices) must be cleared to the highest classification level of the key involved and must be instructed regarding the

NTISSI No. 3011

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

security importance of the courier function. If TOP SECRET electronic key is involved, it must be transported under two-person integrity safeguards. Couriers must also be informed of the identity and/or position of each authorized person to whom key may be transferred.

SECTION IX -- KEYING

9. KY-57/58 and KY-67 equipment embody considerable keying versatility, in that up to [redacted] and key can be accepted in electronic or punched tape form. When under the control of a KYX-15 net control device, KY-57/58 and KY-67 equipment can [redacted]

The simpler KYV-2/2A modules are designed to store only one key and to resist extraction of that key.

a. Key Use. KY-57/58 and KY-67 equipment employ key for both traffic encryption and key encryption purposes. [redacted] purposes, to accommodate short-notice movements of tactical units between widely separated geographic areas or changes in command affiliation. KYV-2/2A modules use only traffic encryption keys (TEKs).

b. Keying Methods.

(1) Key in tape form is loaded into KY-57/58 and KYV-2/2A equipment and in KYK-13 and KYX-15 fill devices by pulling tape segments through connected KOI-18 tape readers.

(2) Key in electronic form is either converted from tape form or generated by KY-57/58/67 equipment controlled by KYX-15 net control devices. Key stored in a KYX-15 may be transferred directly into a KY-57/58/67 or KYV-2/2A equipment or KYK-13 or KYX-15 fill device. [redacted]

[redacted] equipment which holds a key encryption key (KEK) in common with the transmitting net controller. Keyed KYK-13 electronic transfer devices may be used to key KY-57/58, KY-67, or KYV-2/2A equipment or KYX-15 or other KYK-13 fill devices.

(3) In tactical applications, KY-57/58 and KY-67 users should strive to make maximum use of field-generated key and should use key tape only when the use of field-generated key is impracticable.

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

NTISSI No. 3011

c. Security Limitations.

(1) In KY-57/58/67 and KYV-2/2A equipment, TEKs may be superseded physically, by rekeying from tape or keyed KYK-13 or KYX-15 devices. In KY-

[Redacted]

(2) Except in emergencies, KEKs must be superseded physically; i.e., rekeyed by means of key tape or key in electronic form inserted directly into the crypto-equipment.

[Redacted]

(3)

[Redacted]

Other uses of such key are prohibited.⁵

[Redacted]

(5) KY-57/58, KY-67, and KYV-2/2A key may not be routinely stored in KYK-13 or KYX-15 devices as a substitute for canister storage of key tape.

(6) Key tape segments must not be removed from their canisters until immediately prior to use and may not be issued to users as extracts.

(7) After successfully filling the KYV-2/2A, the operator must exercise one additional push-to-talk (PTT) before removing the fill device.

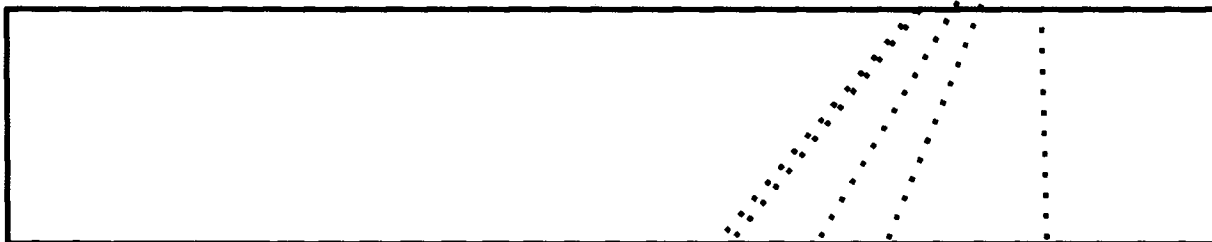
d. Compartmenting KY-57/58/67 Nets.

(1) KEKs serve not only to encrypt TEKs for

[Redacted]

⁵ This restriction is waived when key is generated and distributed in accordance with NAG-16/TSEC, "Field Production and Distribution of Electronic Key In Support of Short-Notice Operations."

NTISSI No. 3011



(2) When the same KEK is used in a cryptonet encompassing more than one radio net, the potential security impact of compromise increases. For this reason, high copy count KEKs (e.g., corps common keys) should be used only when there is no operationally acceptable alternative.

e. Cryptoperiods.

(1) Each KY-57/58 and KY-67 KEK has a maximum cryptoperiod of [redacted]. However, under emergency conditions, the controlling authority may extend a cryptoperiod [redacted]. Longer extensions are reportable as COMSEC incidents.

(2) Each KY-57/58, KY-67, and KYV-2/2A TEK, whether generated in tape or electronic form, has a maximum cryptoperiod [redacted]. However, under emergency conditions, the controlling authority (or net controller) may extend a cryptoperiod [redacted] additional hours. Longer extensions are reportable as COMSEC incidents.

f. Cryptonet Size. There is no maximum size for KY-57/58, KY-67, and KYV-2/2A cryptonets. However, operational considerations, such as the potential impact of key compromises, dictate that the number of stations holding identical TEKs be kept as low as operationally feasible.

SECTION X - REPORTING COMSEC INCIDENTS

10. A general listing of reportable COMSEC incidents and reporting standards is contained in NTISSI No. 4003. Specific incidents affecting KY-57/58/67 equipment are stated below:⁶

⁶ No "system unique" reportable COMSEC incidents affect the KYV-2/2A cryptosystem.

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

NTISSI No. 3011

a. Replacing KEKs. [redacted]

b. Misuse of Cryptosystem. [redacted]

2 Enclosures:

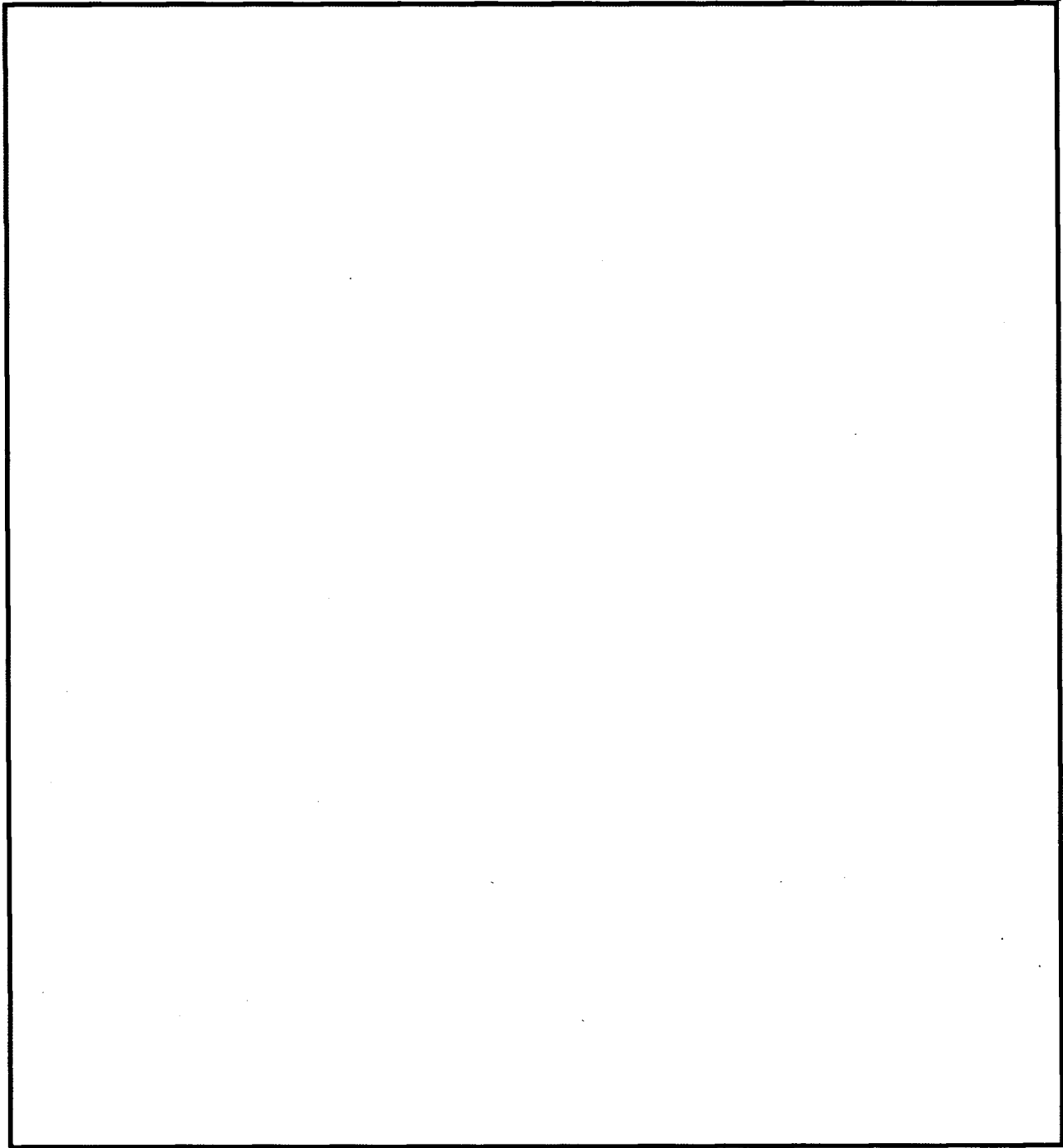
Annex A - Components of KY-57/58, KY-67 and KYV-2/2A
Cryptosystems

Annex B - Summary of Access Requirements

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

ANNEX A

COMPONENTS FOR KY-57/58, KY-67, AND KYV-2/2A CRYPTOSYSTEMS

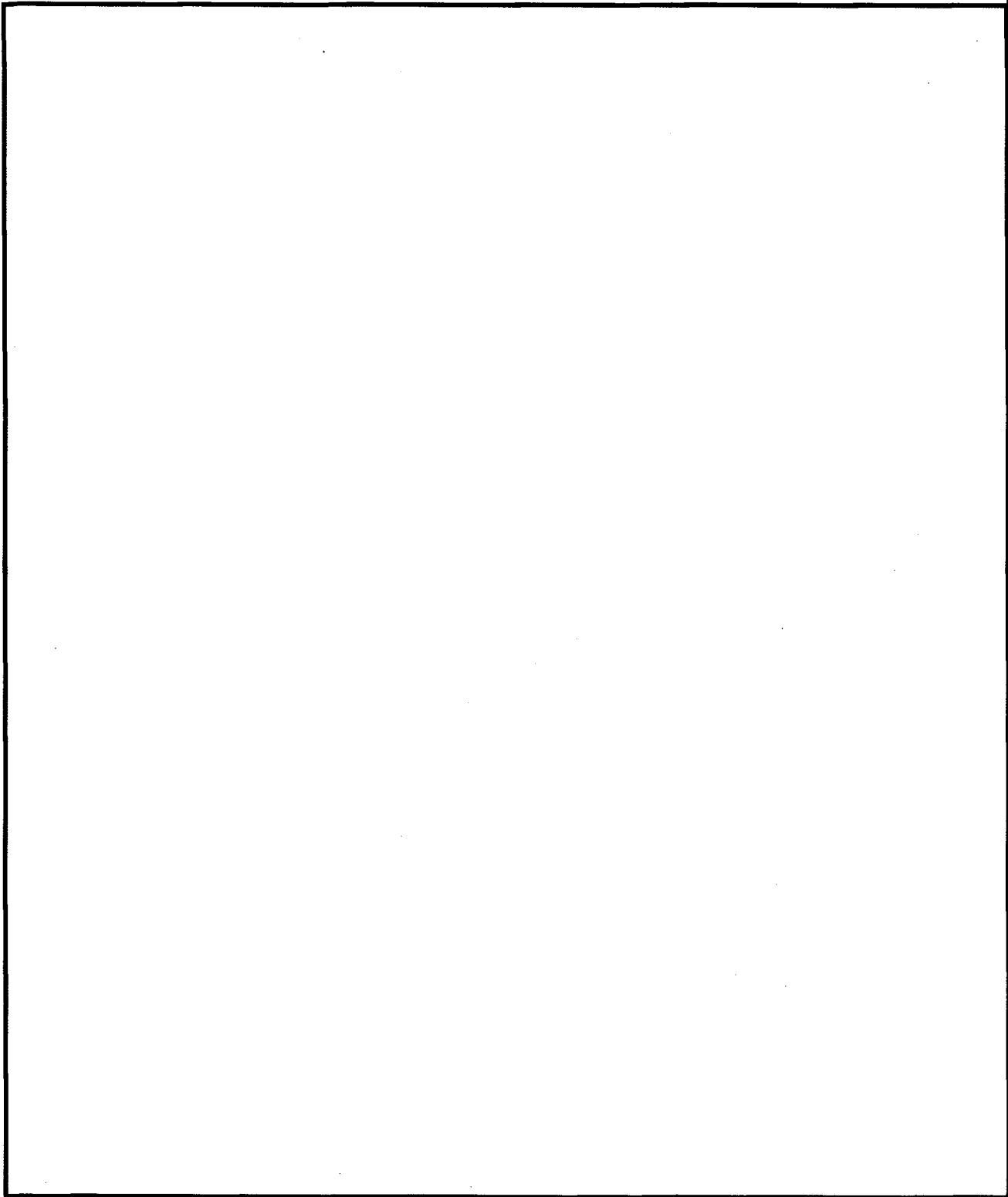


* accounting legend code

ANNEX A to
NTISSI No. 3011

~~FOR OFFICIAL USE ONLY~~

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

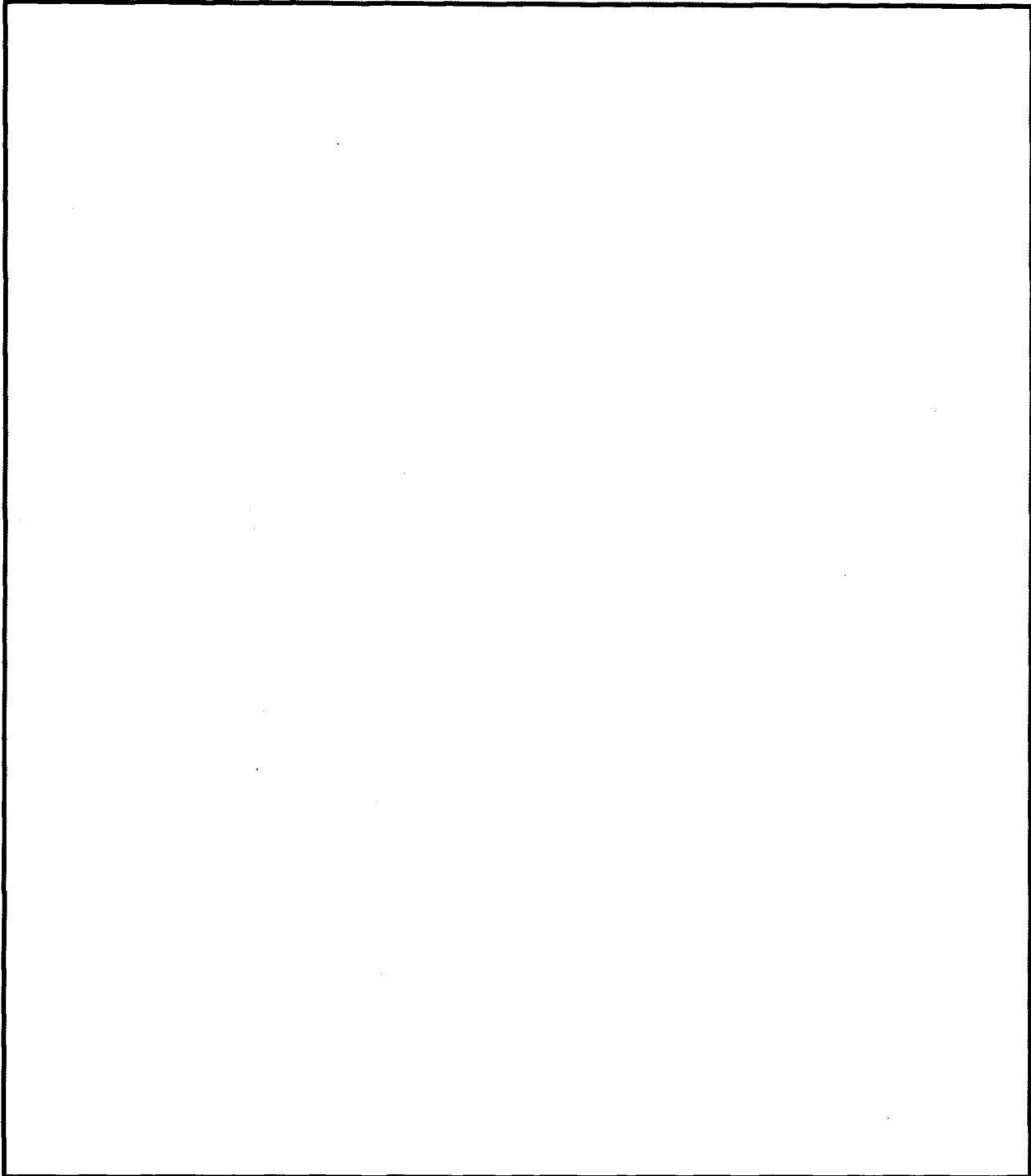


A2

ANNEX A to
NTISSI No. 3011

~~FOR OFFICIAL USE ONLY~~

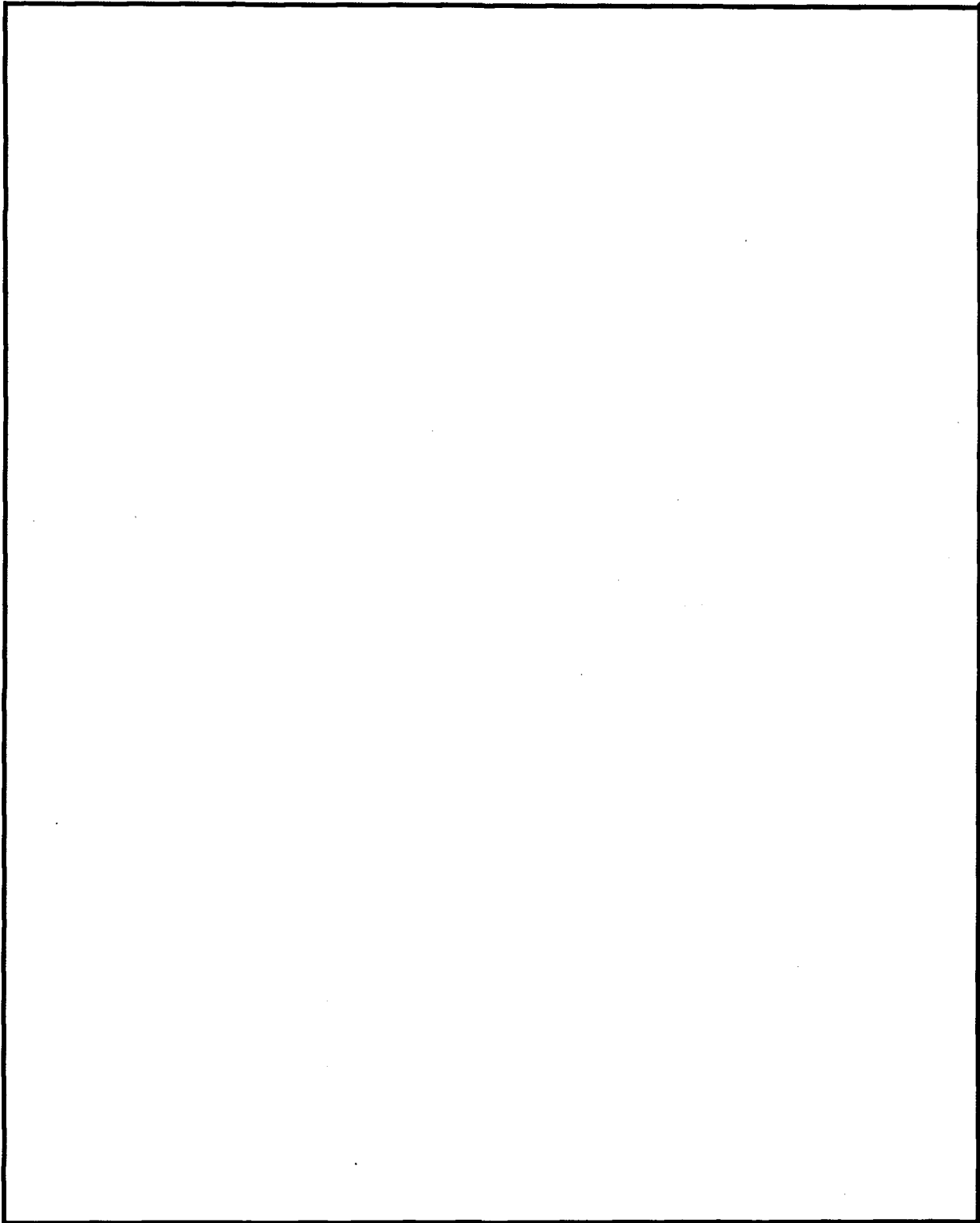
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



ANNEX A to
NTISSI No. 3011

A3

~~FOR OFFICIAL USE ONLY~~

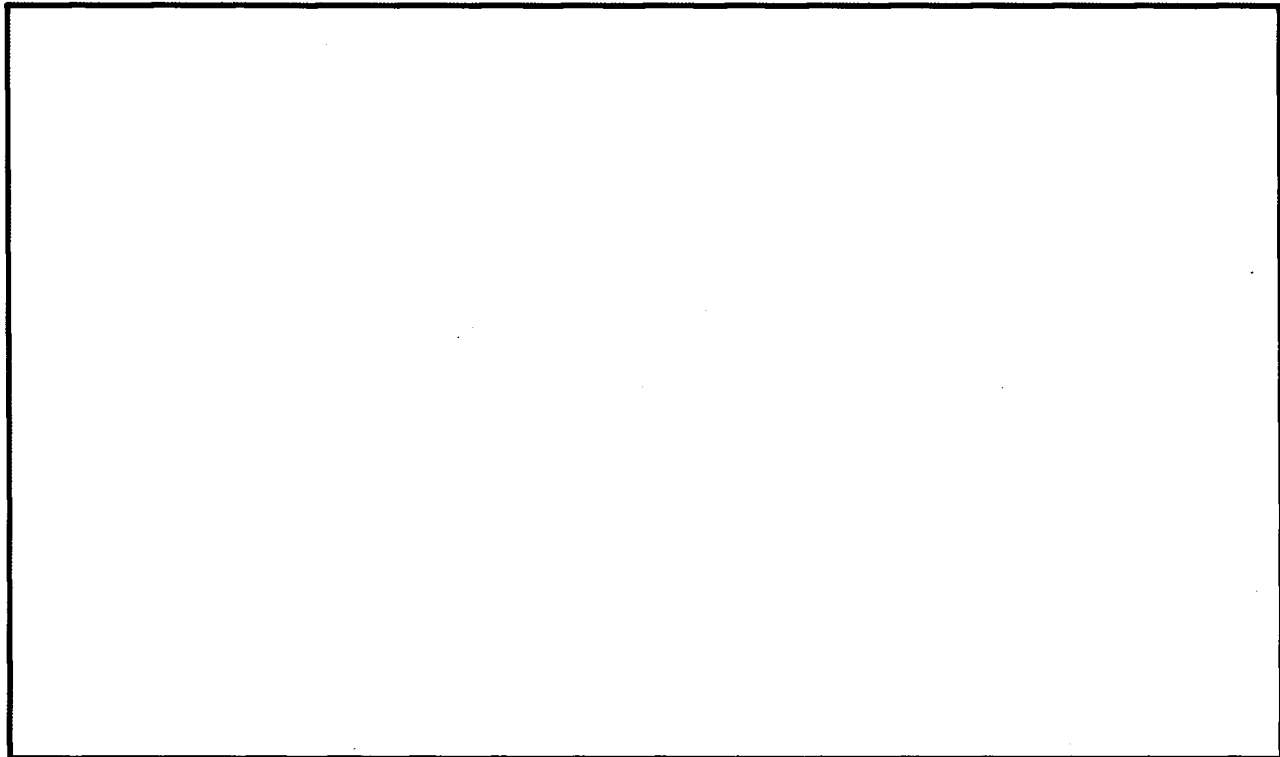


ANNEX A to
NTISSI No. 3011

A4

~~FOR OFFICIAL USE ONLY~~

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



A5

ANNEX A to
NTISSI No. 3011

~~FOR OFFICIAL USE ONLY~~

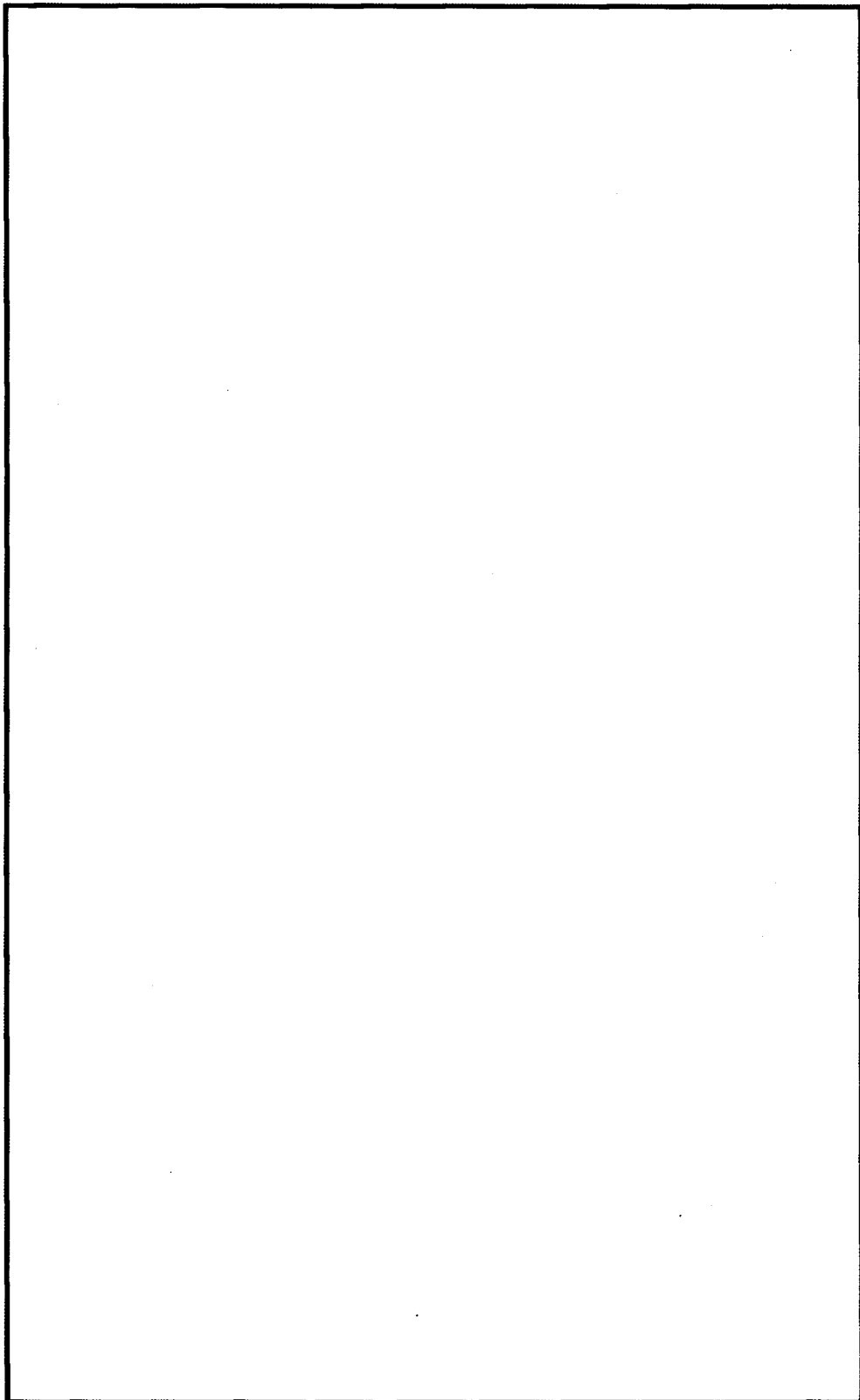
ANNEX BSUMMARY OF ACCESS REQUIREMENTS

SYSTEM COMPONENT	ACCESS REQUIREMENTS							
	A	B	C	D	E	F	G	H
Classified U.S. key tape and KY-57/58/67, KYV-2/2A, KYK-13, KYX-15 containing classified U.S. key	X	X				X		
Classified allied or NATO key tape & KY-57/58/67, KYV-2/2A, KYK-13, KYX-15 containing classified allied or NATO key	X	X				X	X	
KY-57/58/67, KYV-2/2A, KYK-13, KYX-15 which are unkeyed or contain only unclassified key & KOI-18	X			X		X	X	X
Classified KY-57/58, KY-67, KYV-2/2A supporting documentation	X		X			X	X	
Ky-57/58/67 & KYV-2/2A handsets and KYV-57/58 data terminals	X				X	X	X	

- A. Operational need for access.
 B. Clearance at level of highest classified key.
 C. CONFIDENTIAL or SECRET clearance.
 D. No clearance required.
 E. Uncleared U.S. or foreign persons under supervision of cleared U.S. persons.
 F. U.S. Government military or civilian employee who is a U.S. citizen or resident alien & employee of U.S. Government contractor who is U.S. citizen.
 G. Military or civilian employee of NATO or allied government to which crypto-equipment has been released.
 H. The local tampering risk and nationality of the affected personnel must be considered, when access by foreign nationals is involved.

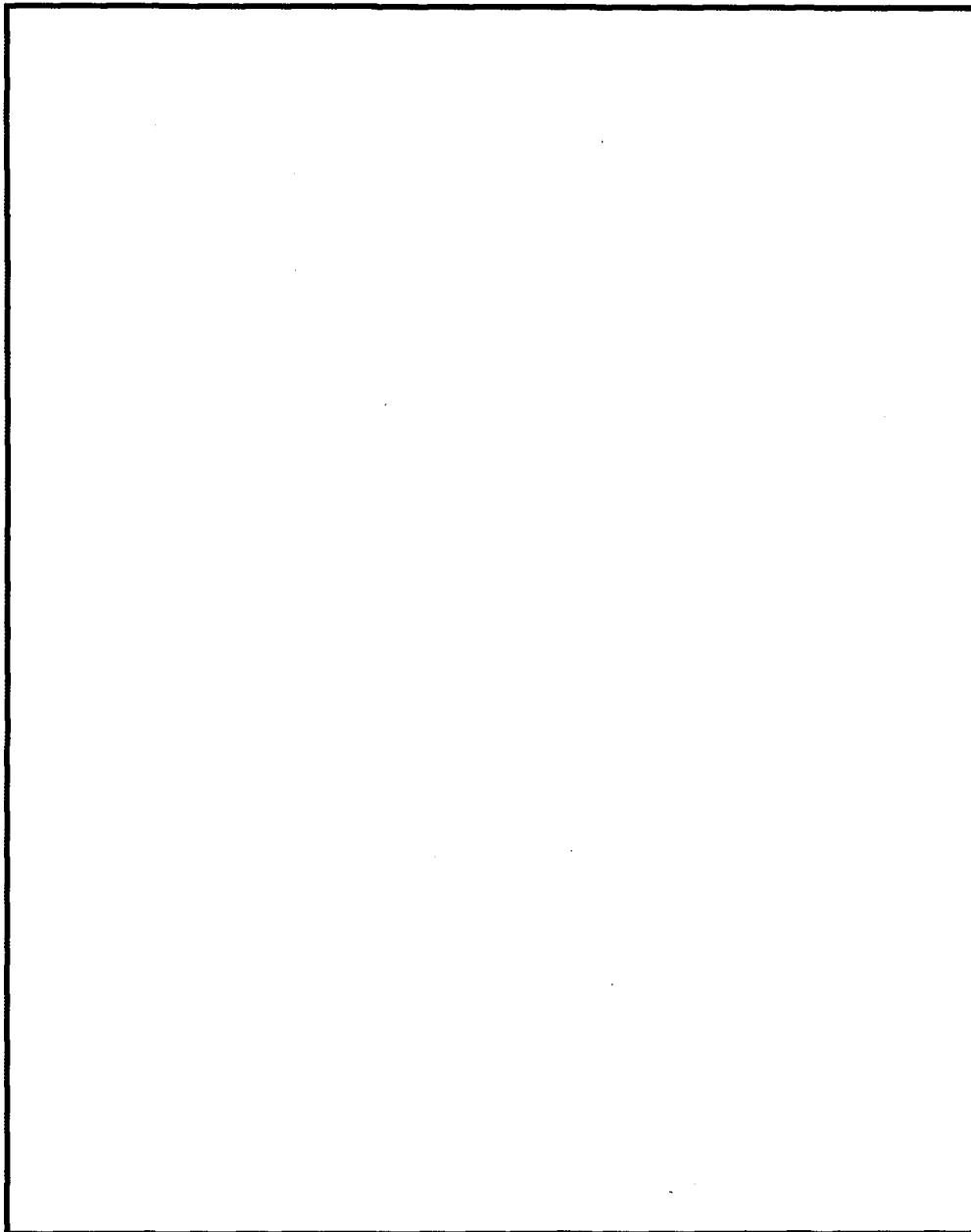
~~FOR OFFICIAL USE ONLY~~ANNEX B to
NTISSI No. 3011

NTISSI No. 3011



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

NTISSI No. 3011



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

~~FOR OFFICIAL USE ONLY~~

NTISSI No. 3011

~~FOR OFFICIAL USE ONLY~~