

NSTISSI No. 3018  
8 January 1992

**NSTISS**

NATIONAL  
SECURITY  
TELECOMMUNICATIONS  
AND  
INFORMATION  
SYSTEMS  
SECURITY

**OPERATIONAL SECURITY DOCTRINE**

**FOR THE**

**GUARDSMAN 100 AND 100T**

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

~~**FOR OFFICIAL USE ONLY**~~

**NSTISS**  
NATIONAL SECURITY  
TELECOMMUNICATIONS  
AND INFORMATION  
SYSTEMS SECURITY

**NATIONAL MANAGER**

8 January 1992

**FOREWORD**

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3018, "Operational Security Doctrine for the GUARDSMAN 100 and 100T," provides the minimum standards for secure operational use of the GUARDSMAN printed wiring assembly.


2. Extracts from this document may be made as necessary. Extracts must be marked FOR OFFICIAL USE ONLY, and cannot be given to the public without the specific approval of the National Manager, NSTISS.

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.

4. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from:

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

5. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

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

~~FOR OFFICIAL USE ONLY~~

OPERATIONAL SECURITY DOCTRINE FOR  
THE GUARDSMAN 100 AND 100T

	<u>SECTION</u>
PURPOSE AND SCOPE . . . . .	I
EXCEPTIONS . . . . .	II
REFERENCES . . . . .	III
DEFINITIONS . . . . .	IV
SYSTEM DESCRIPTION . . . . .	V
OPERATING RESTRICTIONS . . . . .	VI
KEYING INFORMATION . . . . .	VII
CLASSIFICATION GUIDANCE . . . . .	VIII
COMPUTER SECURITY . . . . .	IX
PHYSICAL SECURITY . . . . .	X
DESTRUCTION AND EMERGENCY PROTECTION. . . . .	XI
REPORTABLE INCIDENTS . . . . .	XII

SECTION I - PURPOSE AND SCOPE

1. This instruction provides the minimum security standards for the handling and control of the GUARDSMAN 100 and 100T.

2. The provisions of this instruction apply to all departments and agencies of the U.S. Government, their contractors, and other purchasers as authorized by the National Manager, NSTISS, who handle, distribute, account for, store, or use the GUARDSMAN, system components, and associated COMSEC material. Promulgation may be made through the issuance of this document or through its incorporation into applicable department or agency publications.

3. In cases of conflict between this instruction and other publications, this instruction will take precedence for COMSEC matters relating to the use of GUARDSMAN equipment. Director of Central Intelligence (DCI) directives and other DCI guidance will take precedence over this instruction for use of GUARDSMAN equipment within a sensitive compartmented information facility (SCIF).

NSTISSI NO. 3018

SECTION II - EXCEPTIONS

4. Requests for exceptions to any of the provisions of this NSTISSI must be submitted to the National Manager, NSTISS, National Security Agency (ATTN: ) , for approval prior to implementation. All requests for exceptions must be accompanied by complete operational justification.

SECTION III - REFERENCES

5. The following list of references apply to U.S. Government users of GUARDSMAN:

- a. NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.
- b. NACSIM No. 5203, Guidelines for Facility Design and RED/BLACK Installation, dated 30 June 1982.
- c. NCSC-9, National COMSEC Glossary, dated 1 September 1982.
- d. NTISSI No. 4001, Controlled Cryptographic Items, dated 25 March 1985.
- e. NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.
- f. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.
- g. NTISSAM COMPUSEC/1-87, Advisory Memorandum on Office Automation Security Guidelines, dated 16 January 1987.
- h. NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.
- i. FIPS PUB 46-1, Data Encryption Standard, dated 22 January 1988.
- j. NTISSI No. 7000, TEMPEST Countermeasures for Facilities, dated 17 October 1988.
- k. NSTISSI No. 4006, Controlling Authorities for COMSEC Material, dated 2 December 1991.

1. NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, dated 1 February 1991.

m. NSTISSAM TEMPEST/1-91, Compromising Emanations Laboratory Test Requirements, Electromagnetics, dated 21 March 1991.

6. The following list of references apply to U.S. Government contractors:

a. NSTISSAM TEMPEST/1-91 (Reference 5.m. above).

b. U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual, dated 2 February 1986 (for U.S. Government contractors who are not participants in the Defense Industrial Security Program).

c. DoD 5220.22-S, COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information (CSISM), dated 17 March 1988 (for U.S. Government contractors who are participants in the Defense Industrial Security Program).

d. NTISSI No. 7000 (Reference 5.j. above, applicable to cleared contractors who have a TEMPEST requirement, as indicated in contractual documents and DD form 254). Copies may be requested from the appropriate Defense Investigative Service field office.

e. Cleared U.S. Government contractors and federally sponsored non-government entities who are not participants in the Defense Industrial Security Program will use implementers of the governmental references provided by their U.S. Government sponsors.

#### SECTION IV - DEFINITIONS

7. The definitions in NCSC-9 apply to this instruction with the exception that the term "COMSEC insecurity" is replaced by the term "COMSEC incident"; and "controlled COMSEC item" is replaced by "controlled cryptographic item," as defined in NTISSI No. 4001. For purposes of this document, the following definitions also apply:

- a. Traffic Encryption Key (TEK). Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.
- b. Message Indicator (MI). A sequence of bits transmitted for the purpose of synchronization.
- c. Sensitive Unclassified U.S. Government Information. (This term is defined the same as the term sensitive information is defined in Public Law 100-235.) Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

#### SECTION V - SYSTEM DESCRIPTION

8. GUARDSMAN is a stand-alone data encryption device that contains the NSA-endorsed GILLAROO printed wiring assembly (PWA) as its cryptographic logic. (All GUARDSMAN units will contain the GILLAROO PWA except in instances where it has been removed for repair.) It allows secure file transfers over phone lines and electronic mail networks. GUARDSMAN allows stand-alone GILLAROO connectivity via RS-232 interface to the personal computer (PC) serial port. It has performance features identical to those of GILLAROO and is interoperable with the GILLAROO in a net environment. Unlike GILLAROO, GUARDSMAN can be connected to both IBM and non-IBM compatible PCs, as well as mainframe computers. It operates at user selectable data rates ranging from 110 to 9600 bits per second. GUARDSMAN is produced in both TEMPEST approved (model 100T) and non-TEMPEST approved versions (model 100).

#### SECTION VI - OPERATING RESTRICTIONS

9. The GUARDSMAN 100T is NSA-approved for protecting classified information up to and including SECRET as well as sensitive unclassified U.S. Government information in accordance with FIPS PUB 46-1. The GUARDSMAN 100T may be used both within and outside the U.S. The GUARDSMAN 100 is NSA-approved for both classified and unclassified uses within the

NSTISSI NO. 3018

U.S. [Redacted]

10. When test key is used, all data communications must be UNCLASSIFIED.

11. When connected to a PC, GUARDSMAN is the only communications port that may be used for external communications. However, boards that have been installed in the same PC for accessing a serial printer, "mouse," or similar item may remain in the PC even though the GUARDSMAN has been connected.

12. Data should be transmitted through file transfers. Real-time keyboard transfers and use of the bypass mode should be kept to a minimum.

13. There will be no procurement of the GUARDSMAN 100 or 100T after 31 December 1993. However, previously fielded units may still be used after this date and NSA will continue to provide key for previously fielded units.

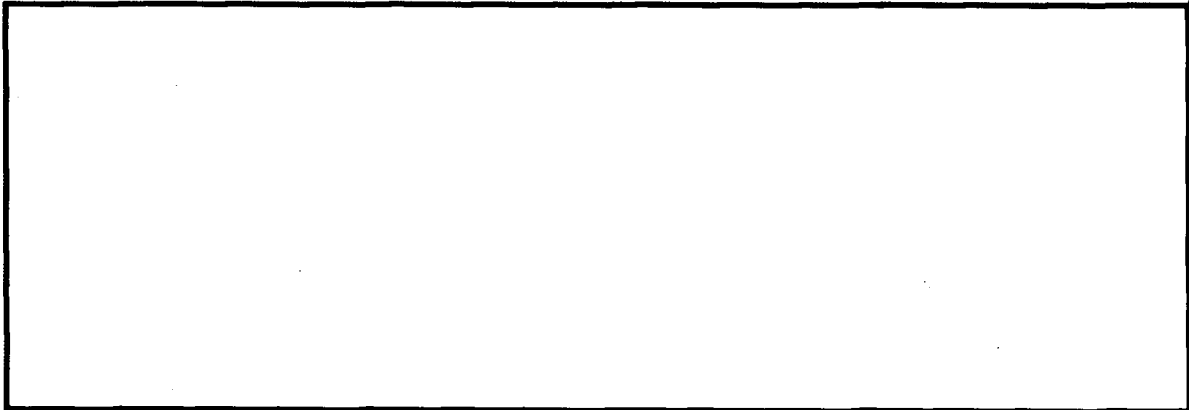
14. [Redacted]

15. [Redacted]



a. [Redacted]

b. [Redacted]

NSTISSI NO. 3018



16. The following procedures must be followed when using GUARDSMAN equipment:

- a. 
- b. 

SECTION VII - KEYING INFORMATION

17. Format. Two canisters are supplied for GUARDSMAN, one containing the MI and the other containing TEK. Although the MI is not key, it is included within this section because of its close association with the TEK. Both are supplied by NSA as standard, hole-punched tape in protective canisters. MI and TEK are being supplied for operational and test use. Each canister is identified by a unique short title.

a. MI. Both operational and test MIs are supplied in canisters with 16 different segments. MI canisters, test and operational, are superseded yearly. Each user within a network must use an MI with a unique short title; thus, the number of short titles necessary is equal to the number of members within a network.



b. TEK. The operational TEK canisters contain 31 identical segments while the test TEK canisters contain 16 different segments. Operational TEK is superseded monthly and test TEK is superseded yearly. All users within a network will use a TEK with the same short title; thus, multiple copies of the same short title will be necessary for a network.

18. Cryptoperiod and Key Logistics.

a. Operational.

(1) MI. The effective period for each canister of MI tape is one year. Although 16 distinct MIs are contained in an MI canister, only one segment will normally be used with the remaining 15 being used only if the GILLAROO PWA within the GUARDSMAN fails or any other circumstances requiring loading of MI as described in SECTION VII, paragraph 19.b.

(2) TEK. The effective period for each canister of operational TEK is one month. A new canister is used on the first day of each month. TEK is provided in a canister that contains 31 identical segments of the same key with a monthly cryptoperiod. A new segment is pulled daily, or as needed, and must be destroyed after use with the exception of the last segment. The last segment of the key (the 31st) may be kept in secure storage in the terminal area until the end of the month to rekey those devices that have prematurely depleted their key allocation. This last segment may be retained in the terminal area for an additional week to decrypt back traffic. The COMSEC custodian is authorized to retain the superseded key for one month in order to retrieve archival information after this period.

b. Test.

(1) MI. Test MI must be used for the duration of a testing period, and must be replaced with operational MI when the system goes to operational status.

(2) TEK. Test TEK is supplied in a canister with 16 different segments. A new canister is used on the first day of each year. The cryptoperiod for each segment of test TEK is one month. Each segment is to be used for as many test sessions as required within a single monthly cryptoperiod and must be destroyed at the end of the month. The segment shall be destroyed as soon as possible after supersession and may not be held for longer than 12 hours following supersession. Reasonable care must be used to protect the test TEK, and the

NSTISSI NO. 3018

best possible overnight storage of both the canister and the test key segment must be used to preclude unauthorized access, theft, or loss.

19. Insertion.

a. The KOI-18 key tape reader is used to load the MI and the TEK into the GUARDSMAN unit via the key-fill cable.

b.

[Redacted]

(1)

(2)

(3)

[Redacted]

c.

[Redacted]

20. Key Destruction. All TEK and MI segments should be destroyed by the user, with a witness present. The destruction should be documented by the witness and the user on the disposition record of the key tape handling instructions. The destruction shall be done using one of the approved methods specified in NTISSI No. 4004.

21. Ordering Key. Keying material, as well as MI, must be ordered from NSA at least 120 days prior to use. New users must inform NSA when they initiate operations so that follow-up key can be shipped automatically. Military users should order their key through their Cryptologic Support Element.

22. Cryptonet Size. The cryptonet size for GUARDSMAN is limited to 50 subscribers. Requests for larger cryptonets must be approved by NSA (ATTN: [Redacted]).

### SECTION VIII - CLASSIFICATION GUIDANCE

23. For general COMSEC classification guidance, see NTISSI No. 4002.

24. Traffic Encryption Keys (TEKs). Operational TEKs for classified applications are classified at the maximum level of the traffic that they protect, up to and including SECRET. Test TEKs are UNCLASSIFIED. All TEKs, both operational and test, are marked "CRYPTO."

25. Message Indicator (MI). All MIs, both test and operational, are UNCLASSIFIED and marked "CRYPTO."

26. Equipment. As long as a GILLAROO PWA resides within a GUARDSMAN unit, the unit must be controlled as if controlling the GILLAROO PWA itself.

a. When keyed, a GUARDSMAN equipment assumes the classification of the key.

b. When a GUARDSMAN equipment is powered off the key is zeroized and it reverts to CCI status.

### SECTION IX - COMPUTER SECURITY

27. If any classified or sensitive unclassified U.S. Government information is to be processed by, or is resident in, any PCs connected to GUARDSMAN equipment, the computer security requirements applicable to that particular government agency or department must be followed. Use of GUARDSMAN equipment shall in no way bypass or negate any of the computer security requirements. For additional guidance consult NTISSAM COMPUSEC/1-87. The following specific rules apply to PCs connected to GUARDSMAN:

a. Users should be cautioned that GUARDSMAN secures only the data transferred out of the PC by the user. There is no security provided for the internal processing or storage of information. Stored files must be controlled and secured by other means, such as local physical procedures for restricting access to disk files, etc., and must include assurances that no remote access to files is possible without GUARDSMAN being engaged (i.e., no auto-answer in bypass mode).

b. A PC with a non-removable disk and a GUARDSMAN attachment must not be used for classified processing unless all users, even those connected via the GUARDSMAN, have a clearance and a need-to-know for all classified information resident in the connected PCs.

c. Removable hard disks and floppy disks that contain classified information must be removed and the PC, as well as any non-removable disks, must be purged either by degaussing or overwriting before transmitting unclassified information. (A listing of approved degaussers is contained in the Information Security Products and Services Catalogue published by NSA.) This procedure also applies when transmitting classified information to an individual with a lower clearance than the highest classification level of data on the system.

d. Prior to entering the bypass mode for transmitting unclassified traffic or using the PC for unclassified (non-GUARDSMAN) applications, users must remove removable hard disks and floppy disks that contain classified information. Approved sanitization procedures (i.e., degaussing or overwriting with ones, then zeros, and then random data) must be executed on both the PC and any non-removable disks. When the need exists to use plain text headers and trailers in conjunction with encrypted transmissions, the bypass mode may be used in the transmission of the headers and trailers without removal of classified disks or use of sanitization procedures.

e. Removable hard disks and floppy disks that contain classified information must be removed at the close of daily operations and stored in an appropriate security container.

#### SECTION X - PHYSICAL SECURITY

##### 28. Accountability.

a. The GUARDSMAN unit serves as a host for the CCI GILLAROO PWA. The GILLAROO PWA requires continuous serial number accountability to a central point. The presence of a GILLAROO PWA in a GUARDSMAN unit is indicated by the label "Contains Controlled Cryptographic Item PES-B4-XXXXX," which bears the same serial number as the embedded GILLAROO PWA. If the GILLAROO PWA is replaced in a GUARDSMAN unit, a new label bearing the new GILLAROO PWA serial number must be affixed to

the exterior of the GUARDSMAN unit. GUARDSMAN units should not normally be opened for the sole purpose of verifying the serial number of the embedded GILLAROO PWA.

b. Classified keying material, as well as MI which is unclassified and marked "CRYPTO," will be accounted for by short title as accounting legend code (ALC-1), and accountable by serial number to the central office of record, according to NACSI No. 4005. After reporting initial receipt, unclassified key may be accounted for, in accordance with service or agency directives (ALC-4).

29. Access to GUARDSMAN Equipment. Uninstalled GUARDSMAN equipment must be stored in accordance with NTISSI No. 4001. Access to keyed GUARDSMAN equipment is restricted to those authorized individuals who have a clearance equal to the classification of the key in use and who require such access in the performance of their duties.

30. Key. NSTISSI No. 4006 provides guidance on controlling authority responsibilities associated with key. Requirements for the safeguarding and storage of classified and unclassified key are provided in NACSI No. 4005. Unclassified key marked "CRYPTO" must be safeguarded, stored, and handled in a controlled manner to preclude unauthorized access, theft, or loss.

31. Access to Key. Access to GUARDSMAN key is restricted to those authorized individuals who have a clearance equal to the classification of the key and who require such access in order to perform their duties.

32. Personnel Authorized to Key Equipment. In order to restrict access to the key, certain individuals at each terminal shall be appointed to key the terminal daily. The canister shall be returned to secure storage immediately after the keying of the PC. The designated individual should be responsible for the immediate destruction of used tape segments in accordance with paragraph 20 above. With COMSEC custodian approval, the current month's TEK canister may be stored in an approved security container by the user in the terminal area. In this case, the COMSEC custodian shall designate one person in the user area who shall be responsible for keying, storing, and destroying the GUARDSMAN keying material in accordance with this doctrine.

**33. Transportation.**

a. Key. The procedures in NACSI No. 4005 apply to the shipment of unclassified and classified key.

b. Equipment.

(1) GUARDSMAN equipment bearing the label "contains CCI ..." must be shipped only to facilities that employ individuals who are authorized access.

(2) CCIs may be transported by any means that provide continuous accountability and protection against losses while in transit. These criteria are satisfied by any of the following means:

(a) A courier who meets the access requirements of NTISSI No. 4001, and has been formally authorized by a department, Service, or agency of the U.S. Government or by a U.S. Government contractor/company.

(b) U.S. Postal Service (USPS) registered mail, provided it does not at any time pass out of U.S. control and does not pass through any foreign postal system or any foreign inspection. To ensure that U.S. registered mail destined for overseas addresses stays within U.S. channels, it should only be addressed to an APO or FPO. USPS registered mail is the only service offered by the USPS that is authorized for shipping CCI equipment.

(c) Commercial carriers (only within the U.S., and its territories and possessions) that utilize a system that accurately reflects a continuous chain of accountability and custody for the material while in transit. The system must have the capability of providing a manual or electronic tally record as evidence that this service was provided.

(d) U.S. military or military-contract air service (e.g., MAC, LOGAIR, or QUICKTRANS), provided the requirements for constant surveillance service are observed.

(e) U.S. Diplomatic Courier Service.

(f) In foreign countries where there is a significant U.S. military presence (i.e., a country with two or more military bases where U.S. military personnel are stationed), foreign nationals who are employed by the U.S.

NSTISSI NO. 3018

Government may transport GUARDSMAN equipment, provided there is a signature record that provides continuous accountability and custody of the shipment from pick-up to ultimate destination, and either of the following:

1. A continuous U.S. presence (e.g., a U.S. person accompanying a foreign driver) while the material is in transit; or

2. Transportation of the material in a locked container (e.g., CONEX, DROMEDARY) that also has a shipping seal affixed to it as a means of preventing undetected access to the enclosed material.

34. Maintenance. Users must follow the requirements of NSTISSI No. 4000 and department and agency implementing directives regarding maintenance.

a. [Redacted]  
b. [Redacted]

35. Inoperative GUARDSMAN Equipment. When a failed or inoperable equipment is recognized, an immediate attempt must be made to zeroize this equipment. Failed or inoperative GUARDSMAN units must be returned to the vendor for replacement. Military users should follow the directives of their parent organization in this regard.

36. Treatment of Hard Disks in PCs Connected to GUARDSMAN.

a. A PC with a removable hard disk that has processed classified data must have the hard disk removed prior to the PC undergoing regular maintenance by unclassified personnel.

b. Personnel performing maintenance on a PC with a non-removable hard disk must be a U.S. citizen cleared to the highest classification level of the data processed by the PC unless the permanent hard disks have been purged prior to maintenance, i.e., overwritten with ones, then zeros, and then random data.

c. A defective hard disk must be disposed of or repaired as classified material. If it cannot be degaussed or erased, it cannot be declassified and, therefore, must be repaired only by cleared personnel. (A listing of approved degaussers is contained in the Information Security Products and Services Catalog produced by NSA.)

37. Tamper Checks. Trusted maintenance personnel should check for signs of tampering whenever the PC is opened or GUARDSMAN is installed/removed.

SECTION XI - DESTRUCTION AND EMERGENCY PROTECTION

38. GUARDSMAN users must employ the routine and emergency destruction procedures of NTISSI No. 4004.

SECTION XII - REPORTABLE INCIDENTS

39. The incident reporting requirements of NSTISSI No. 4003 apply to GUARDSMAN equipment and key. In addition, the following specific incidents are reportable to NSA (ATTN: ):

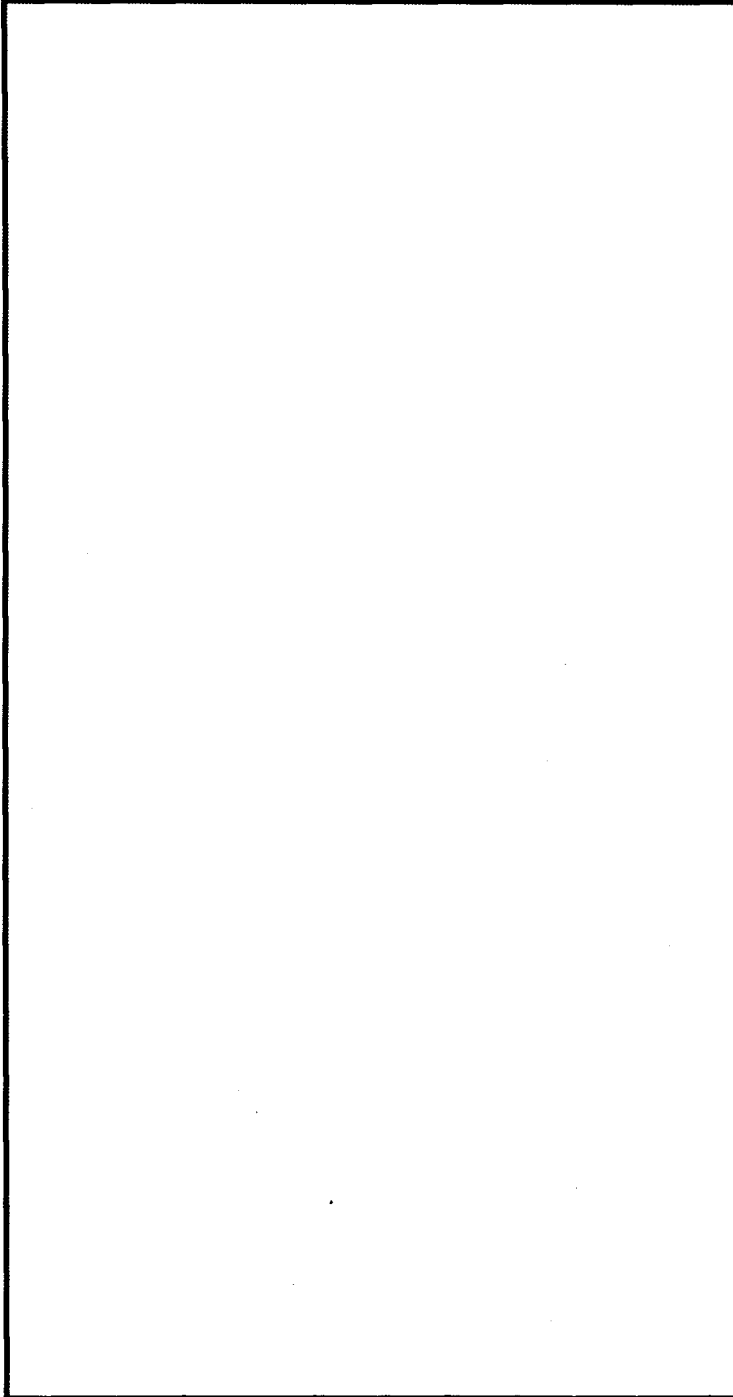
(b) (3)-P.L. 86-36

- a. Suspected tampering with the GUARDSMAN equipment;
- b. Unexpected anomalies in the operation of the GUARDSMAN equipment;
- c. Torn or disarrayed shrink wrapping around the GUARDSMAN equipment when received;
- d. Disassembly of the GUARDSMAN by unauthorized personnel; and
- e. Receipt of a broken or modified canister, or one which is not completely intact. This applies to both TEK and MI canisters.



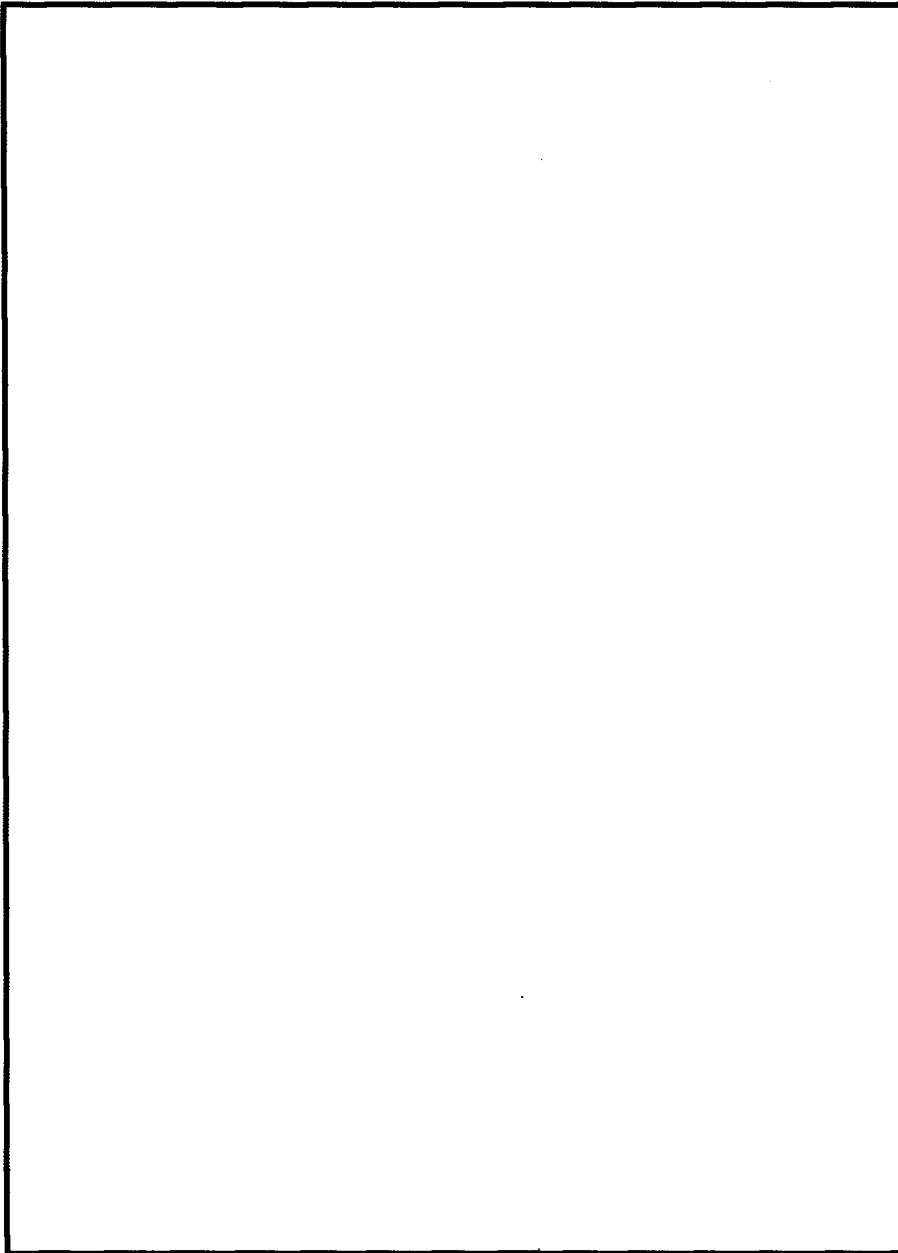
NSTISSI No. 3018

DISTRIBUTION:  
NSA



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

NTISSI No. 3018



~~FOR OFFICIAL USE ONLY~~

NSTISSI No. 3018

~~FOR OFFICIAL USE ONLY~~

---