

NSTISSI No. 3016
2 July 1991

NSTISS

NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR THE

GILLAROO PERSONAL COMPUTER

SECURITY DEVICE (PCSD)

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

2 July 1991


FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3016, "Operational Security Doctrine for the GILLAROO Personal Computer Security Device (PCSD)," provides the minimum standards for the operational use of the GILLAROO PCSD.

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. These officials may request additional copies from:

Executive Secretariat
National Security 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~~

OPERATIONAL SECURITY DOCTRINE FOR THE GILLAROO
PERSONAL COMPUTER SECURITY DEVICE (PCSD)

	SECTION
PURPOSE, SCOPE, AND RESTRICTIONS	I
EXCEPTIONS	II
REFERENCES	III
DEFINITIONS	IV
SYSTEM DESCRIPTION	V
KEYING INFORMATION	VI
CLASSIFICATION GUIDANCE	VII
TEMPEST REQUIREMENTS AND PROCEDURES	VIII
ACCOUNTABILITY	IX
PHYSICAL SECURITY	X
COMPUTER SECURITY	XI
MAINTENANCE AND REPAIR	XII
DESTRUCTION AND EMERGENCY PROTECTION . . .	XIII
REPORTABLE INCIDENTS	XIV

SECTION I - PURPOSE, SCOPE, AND RESTRICTIONS

1. This document provides the minimum safeguards and physical security requirements for the operational use of the GILLAROO PCSD. GILLAROO is a printed wiring assembly (PWA) which is installed in IBM personal computers (PCs) and IBM-compatible PCs to provide point-to-point and electronic mail (E-Mail) encryption and decryption capabilities.

2. This document applies 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 GILLAROO PCSD, system components, and associated COMSEC material. Promulgation may be made through the issuance of this document or through its incorporation into applicable Service, 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 GILLAROO equipment. Director of Central Intelligence (DCI) directives and other DCI guidance will take precedence over this instruction for use of GILLAROO equipment within a sensitive compartmented information facility (SCIF).

NSTISSI NO. 3016

4. Federal departments and agencies should be aware that since the GILLAROO PCSD is approved for classified communications, it may also be used for exclusively UNCLASSIFIED communications without the processing of a waiver to Federal Information Processing Standard (FIPS) 46-1, Data Encryption Standard (DES). This is in accordance with Section 17 of FIPS 46-1.

5. Before purchasing GILLAROO devices for exclusively UNCLASSIFIED operations, agencies should carefully consider their interoperability requirements with other UNCLASSIFIED organizations utilizing DES devices, as GILLAROO does not provide interoperability with DES devices.

6. Restrictions.

a. The GILLAROO PCSD is endorsed for traffic up to and including SECRET data communications when using appropriately classified operational key.

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

c. There will be no additional procurement of GILLAROO PCSDs after 31 December 1993.

d. The GILLAROO PCSD, when installed in a PC, 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 GILLAROO has been installed.

e. Approval must be obtained from the National Manager, NSTISS, (NSA, ATTN:) prior to allowing access to GILLAROO by citizens in countries hostile to U.S. interests.

.....
SECTION II - EXCEPTIONS
.....

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

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

NSTISSI NO. 3016

SECTION III - REFERENCES

8. The following list of references apply to U.S. Government users of GILLAROO PCSDs:
- 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. NTISSI No. 4003, Reporting COMSEC Insecurities, dated 3 November 1986.
 - 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 January 1988.
 - j. NTISSI No. 7000, TEMPEST Countermeasures for Facilities, dated 17 October 1988.
 - k. NTISSI No. 4006, Controlling Authorities for COMSEC Keying Material, dated 2 May 1989.
 - l. 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.

NSTISSI NO. 3016

9. The following list of references applies to U.S. Government contractors:

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

b. NSTISSAM TEMPEST/1-91 (Reference 8.m above).

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

d. NTISSI No. 7000 (Reference 8.j above). Applicable to cleared contractors who have a TEMPEST requirement, as indicated in contractual documents and the 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

10. The definitions in NCSC-9 apply to this instruction with the exception that the term "COMSEC insecurity" is replaced by the term "COMSEC incident." The term "controlled COMSEC item" is replaced by the term "controlled cryptographic item," as defined below. For purposes of this document, the following definitions also apply:

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

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

NSTISSI NO. 3016

c. Message Indicator (MI). A sequence of bits transmitted for the purpose of synchronization.

d. Sensitive Unclassified U.S. Government Information. (This term is defined the same as sensitive information 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

11. The GILLAROO PCSD is a full-slot encryption board that provides embedded security for transmitting data between IBM and IBM-compatible PCs. GILLAROO may be used to encrypt and transmit both unclassified and classified information through the SECRET level. It provides secure point-to-point and electronic mail capabilities. The GILLAROO PCSD is a pluggable PWA, U.S. Government Serial Number Designator PES-B4-XXXXX, [REDACTED]

SECTION VI - KEYING INFORMATION

12. Format. Two types of canisters are supplied for the GILLAROO PCSD, 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.

NSTISSI NO. 3016

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.

13. Cryptoperiod and Key Logistics.

a. Operational.

(1) MI. The cryptoperiod for the MI is one year. The MI is not zeroized when the host computer is powered down. Even though 16 distinct MIs are contained in an MI canister, only one segment will normally be used. The remaining 15 MIs will only be used if internal tests on the PCSD fail or if the PCSD is reinserted after removal from the PC for shipment or maintenance.

(2) TEK. The cryptoperiod for the operational TEK is one month. The TEK is zeroized whenever the host computer is powered down. Therefore, 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 PCSDs that have prematurely depleted their key allocation. Additionally, the 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 in secure storage for one month in order to retrieve archival information.

b. Test.

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

(2) TEK. The cryptoperiod for the test TEK is one month. A new canister is used on the first day of each year. Test TEK is supplied in a canister with 16 different segments. 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. Reasonable care must be used to protect the test TEK, and the best possible overnight storage of both the canister and the test key segment must be used to preclude unauthorized access, theft, or loss.

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

NSTISSI NO. 3016

14. Insertion.

a. The KOI-18 key tape reader is used to load the MI and the TEK into the GILLAROO PCSD.

b.

(1)
(2)
(3)
(4)

c.

15. Key destruction. All key and MI 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.

16. Ordering key. Keying material, as well as MI, must be ordered from NSA at least 120 days prior to use. New users should 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.

17. Cryptonet size. The cryptonet size for GILLAROO is limited to 50 subscribers. Requests for larger cryptonets must be approved by NSA (ATTN:).

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

NSTISSI NO. 3016

SECTION VII - CLASSIFICATION GUIDANCE

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

19. 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."

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

21. Equipment.

a. When zeroized or not keyed, the GILLAROO PCSD, PES-B4-XXXX, is an unclassified controlled cryptographic item (CCI).

b. When a GILLAROO PCSD is installed in a PC, the label accompanying the GILLAROO that states, "Contains CCI PES-B4-XXXXX," must be affixed to the outside of the PC housing. This is to ensure that users will be made aware that the PC contains a controlled cryptographic item (CCI). When the PCSD is keyed, the PC assumes the classification of the key.

c. When a PC with a GILLAROO PCSD installed is powered off, both the PC and the PCSD revert to CCI status.

SECTION VIII -

22.

a.

[Redacted]

b.

[Redacted]

c.

[Redacted]

23.

[Redacted]

24. The following restrictions must be applied when using a GILLAROO PCSD:

a. [Redacted]

[Redacted]

b. [Redacted]

[Redacted]

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

NSTISSI NO. 3016

SECTION IX - ACCOUNTABILITY

25. PCSDs. As a CCI, the GILLAROO PCSDs, whether installed in PCs or uninstalled as spares, will be accounted for by serial number to a central point within each using organization. To facilitate serial number accounting of GILLAROO PCSDs, a separate stick-on label will be packaged with each GILLAROO PCSD. The stick-on label will be imprinted with the statement, "Contains Controlled Cryptographic Item PES-B4-XXXXX," and will bear the same serial number as the PCSD. When the PCSD is installed in the PC, the installer must affix the stick-on label to the outside of the PC. This will ensure that users will be aware that the PC contains a CCI. Additionally, each PCSD will also contain a label stating, "Controlled Cryptographic Item PES-B4-XXXXX," and will list the serial number which will be used for accounting and control purposes.

26. Keys. Classified keying material, as well as MI, will be accounted for by short title and serial number at the Central Office of Record in accordance with NACSI No. 4005 (Accounting Legend Code 1). Local accounting of unclassified key is established by local regulations.

SECTION X - PHYSICAL SECURITY

27. Uninstalled equipment. Uninstalled GILLAROO PCSDs and unkeyed PCs containing GILLAROO must be safeguarded and stored in accordance with NTISSI No. 4001.

28. Key. NTISSI No. 4006 provides guidance on controlling authority responsibilities associated with key. Requirements for safeguarding and storage of classified and unclassified key are provided in NACSI No. 4005.

29. Access to key. Access to GILLAROO key and keyed PCs 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. This includes military and civilian employees of foreign governments or international organizations to which the equipment has been formally approved for foreign release.

30. 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. After the PC is keyed and the used tape segment is destroyed, the canister shall be returned immediately to secure storage. All canisters except

NSTISSI NO. 3016

the current month's canister shall be kept in secure storage by the COMSEC custodian. 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 to be responsible for keying, storing, and destroying the GILLAROO keying material according to this doctrine.

31. Shipment.

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

b. Equipment.

(1) PCs containing the GILLAROO PCSDs must be shipped only to facilities which employ individuals who are authorized access. If this is not possible, the PCSD and the outer CCI label must be removed prior to shipment, as in the case of shipment for repair.

(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 that 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. USPS registered mail and APO/FPO are the only services offered by the USPS which are authorized for shipping CCI equipment. Overseas shipments by U.S. registered mail must be sent only to APO/FPO addresses.

(c) Commercial carriers (only within the U.S., 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 manually or electronically prepared tally record as evidence that this service was provided.

NSTISSI NO. 3016

(d) U.S. military or military-contract air service (e.g., MAC, LOGAIR, or QUICKTRANS) provided that 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. Government or a U.S. Government contractor may transport GILLAROO PCSDs, only if there is a signature record that provides evidence of continuous accountability and custody of the shipment from pick-up to ultimate destination, and either of the following:

1. There is a continuous U.S. presence (e.g., a U.S. citizen accompanies a foreign driver) while the material is in transit; or

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

SECTION XI - COMPUTER SECURITY

32. If any classified or sensitive unclassified U.S. Government information will be handled by, or is resident in, any PCs containing GILLAROO PCSDs, the computer security requirements applicable to that particular government agency or department must be followed. Use of the GILLAROO PCSD shall in no way bypass or negate any of the computer security requirements. The following guidance is provided to cover those areas where doctrine is not established but where local security measures need to be implemented. Many of these security measures are presently required by other regulations and are included here as a reminder. Additional guidance is available in NTISSAM COMPUSEC/1-87, Advisory Memorandum on Office Automation Security Guidelines.

a. Users should be cautioned that the GILLAROO PCSD secures only the data transferred out of the PC by the user purposely engaging that function. There is no security provided to 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 assurances that no remote access to files is enabled without GILLAROO being engaged (i.e., no auto-answer in bypass mode).

NSTISSI NO. 3016

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

c. Removable hard disks and floppy disks which contain classified information must be removed and the PC, as well as any non-removable disks, must be sanitized using an approved sanitization program before unclassified information can be transmitted to an uncleared user or classified information transmitted to an individual with a lower clearance.

d. Prior to entering the bypass mode for transmission of unclassified traffic or using the PC for unclassified (non-GILLAROO) applications, users must remove removable hard disks and floppy disks which contain classified information and execute approved sanitization procedures 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. PCs containing the GILLAROO PCSD and having removable hard disks and floppy disks which contain classified information must have those disks removed at close of daily operations and stored in an appropriate security container.

SECTION XII - MAINTENANCE AND REPAIR

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

a.

b.

34. Inoperative GILLAROO PCSDs. Under no circumstances is the user or any maintenance personnel allowed to disassemble the protective metal sheathing surrounding the GILLAROO PCSD.

NSTISSI NO. 3016

Failed or inoperative GILLAROO PCSDs must be returned to the vendor for replacement. Military users should follow the directives of their parent organization in this regard.

35. Treatment of hard disks in PCs containing the GILLAROO PCSD.

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 U.S. citizens and cleared to the highest classification level of the data processed by the PC unless the permanent hard disks have been zeroized 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.

36. Labeling. Maintenance employees must be made aware that THEY SHALL NOT REPLACE PCSDs WITHOUT REMOVING THE OLD STICK-ON LABEL FROM THE PC AND THEN ATTACHING THE NEW LABEL INDICATING THE SERIAL NUMBER OF THE NEWLY INSTALLED PCSD. Accounting reporting must be complied with when the change is made.

SECTION XIII - DESTRUCTION AND EMERGENCY PROTECTION

37. GILLAROO users must employ the routine and emergency destruction procedures of NTISSI No. 4004.

SECTION XIV - REPORTABLE INCIDENTS

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

a. Suspected tampering with the PCSD;

b. Unexpected anomalies in the operation of the GILLAROO PCSD;

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

NSTISSI NO. 3016

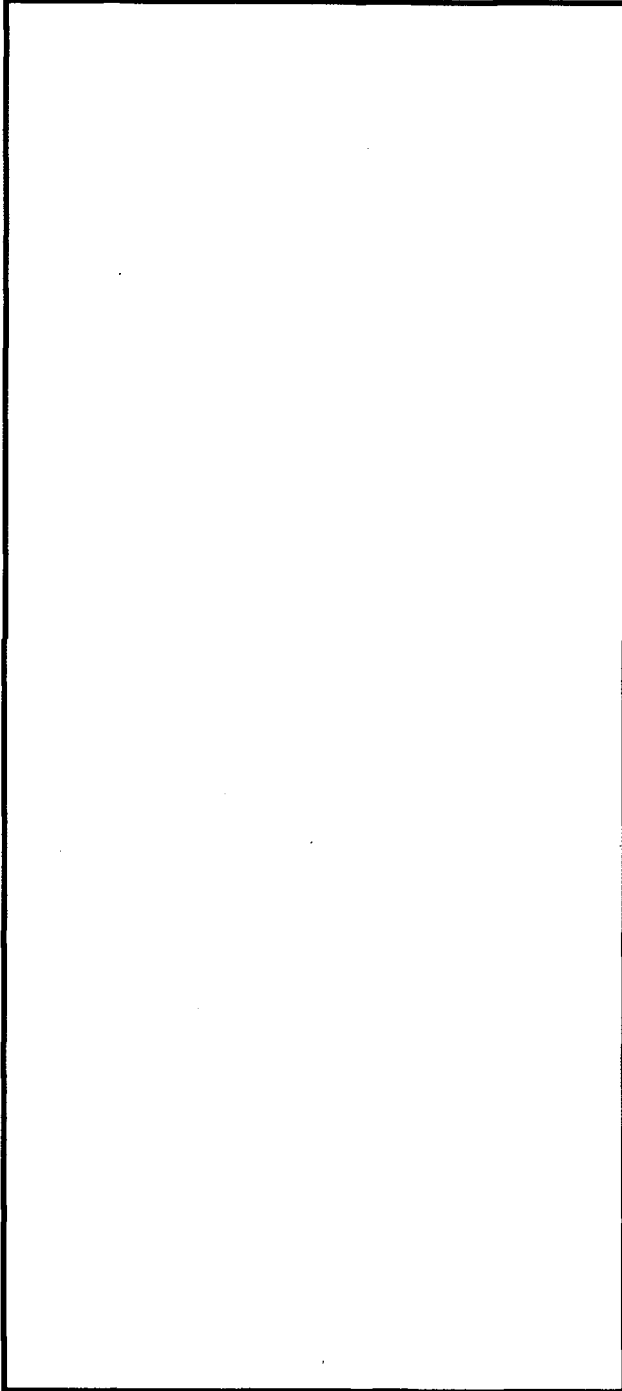
c. Torn or disarrayed shrink wrapping around the GILLAROO PCSD when received; and

d. Disassembly of the PC by unauthorized personnel.

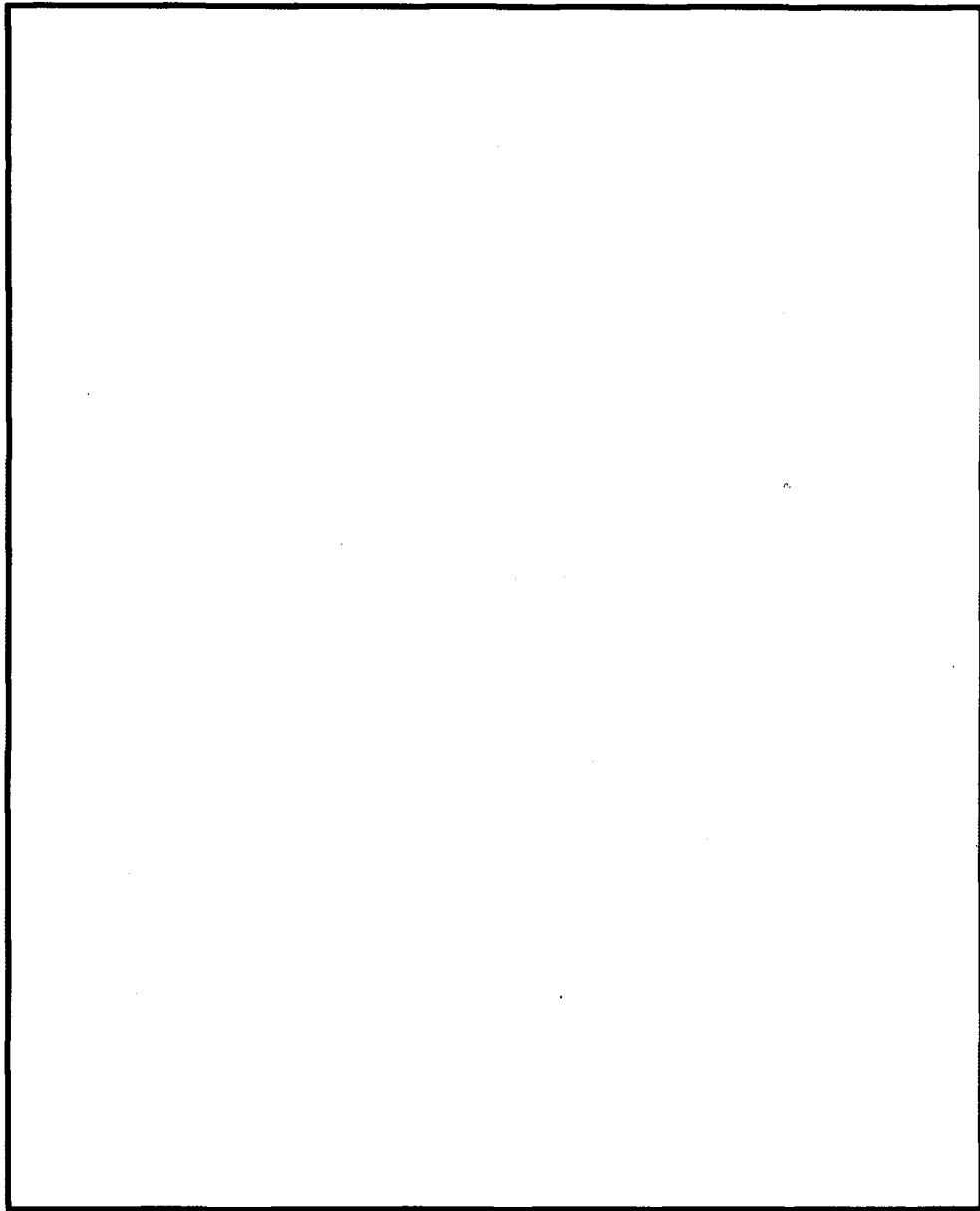
(b) (3) - P.L. 86-36

·NSTISSI No. 3016

DISTRIBUTION:
NSA



NSTISSI No. 3016



NSTISSI No. 3016