Committee on National Security Systems

CNSS-057-06
19 April 2006

Secretariat Manager

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

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Changes for CNSS Instruction No. 3029 – ACTION MEMORANDUM

(U) The following changes have been made to CNSS Instruction No. 3029 to allow KG-175s to be transported pre-loaded with key. Please replace the current paragraph 32.a with:

a. (U//FOUO)

And, please delete Paragraph 42.c(6) (last item).

(b)(6)

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

CNSS-089-04
25 August 2004

Committee on National Security Systems

Secretariat Manager

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Changes for CNSS Instruction No. 3029 – ACTION MEMORANDUM

    1. (U) The following changes have been made to CNSS Instruction No. 3029 to clarify the instructions for retention of the audit log. Please replace the current paragraph 24 with:

    24. (U) Audit Log – It is up to the local SA to determine if auditing is required. Upon that determination, how often the log is to be reviewed is based on risk factors and local security policy. The audit log may be retained in physical form by use of the General Dynamics Encryption Manager (GEM) or GEM Lite (both are defined in ANNEX B, item g). It is recommended the log be retained (off-line from the TACLANE equipment) for a period of time that is adequate for use in troubleshooting problems and insecurities. The length of time to retain the audit log will be determined locally or by the parent department or agency. The information in the audit log is UNCLASSIFIED.

/s/

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

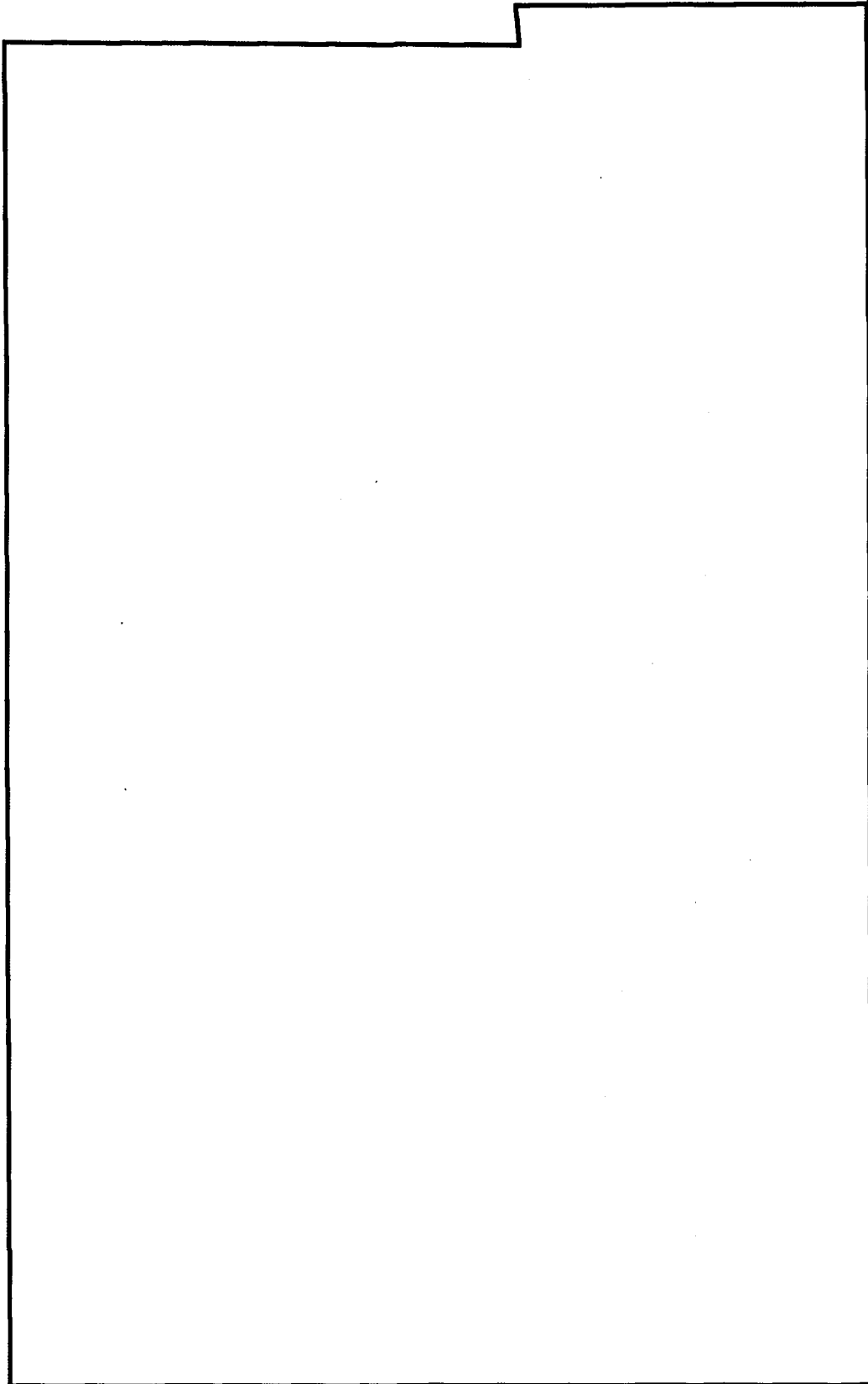(b)(3)-P.L. 86-36

DISTRIBUTION:

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CNSS Instruction No. 3029
May 2004

(U) OPERATIONAL SECURITY

DOCTRINE

FOR

TACLANE (KG-175)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Committee on National Security Systems

National Manager

FOREWORD

1.   (U) Committee on National Security Systems Instruction (CNSSI) No. 3029, "Operational Security Doctrine for the TACLANE (KG-175)," prescribes the minimum security standards for the protection and use of the KG-175 high-speed encryption device.

2.   (U) CNSSI No. 3029 is effective upon receipt. It replaces the NSTISSI No. 3029 Systems Security Doctrine for the TACLANE (KG-175), dated 8 February 2002, which should be destroyed. This revision incorporates upgrades to the equipment.

3.   (U) Representatives of the Committee on National Security Systems may obtain additional copies of this CNSSI at the address listed below.

4.   (U) U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

5.   (U//~~FOUO~~) Comments and suggestions regarding this CNSSI may be sent directly to the National Security Agency,

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

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

CNSS Secretariat [   ] . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CNSSI No. 3029

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE
FOR TACLANE (KG-175)

SECTION I – (U) PURPOSE AND SCOPE

1.   (U) This doctrine contains minimum security standards for the protection and use of TACLANE (KG-175) equipment, its associated components and Communications Security (COMSEC) material. This doctrine applies to TACLANE Classic and TACLANE-E100 units.

2.   (U) The provisions of this doctrine apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, or use the TACLANE and its associated COMSEC material.

3.   (U) Any conflicts between the requirements contained in this doctrine and any other national-level publication shall be identified and submitted for resolution to the Director, National Security Agency (DIRNSA)._____ However, this does not preclude any department or agency of the U.S. Government from applying more stringent security measures to their equipment than this doctrine requires.

SECTION II – (U) REFERENCES   (b)(3)-P.L. 86-36

4.   (U) This doctrine makes reference to a number of other national-level documents. A listing of these documents is contained in ANNEX A.
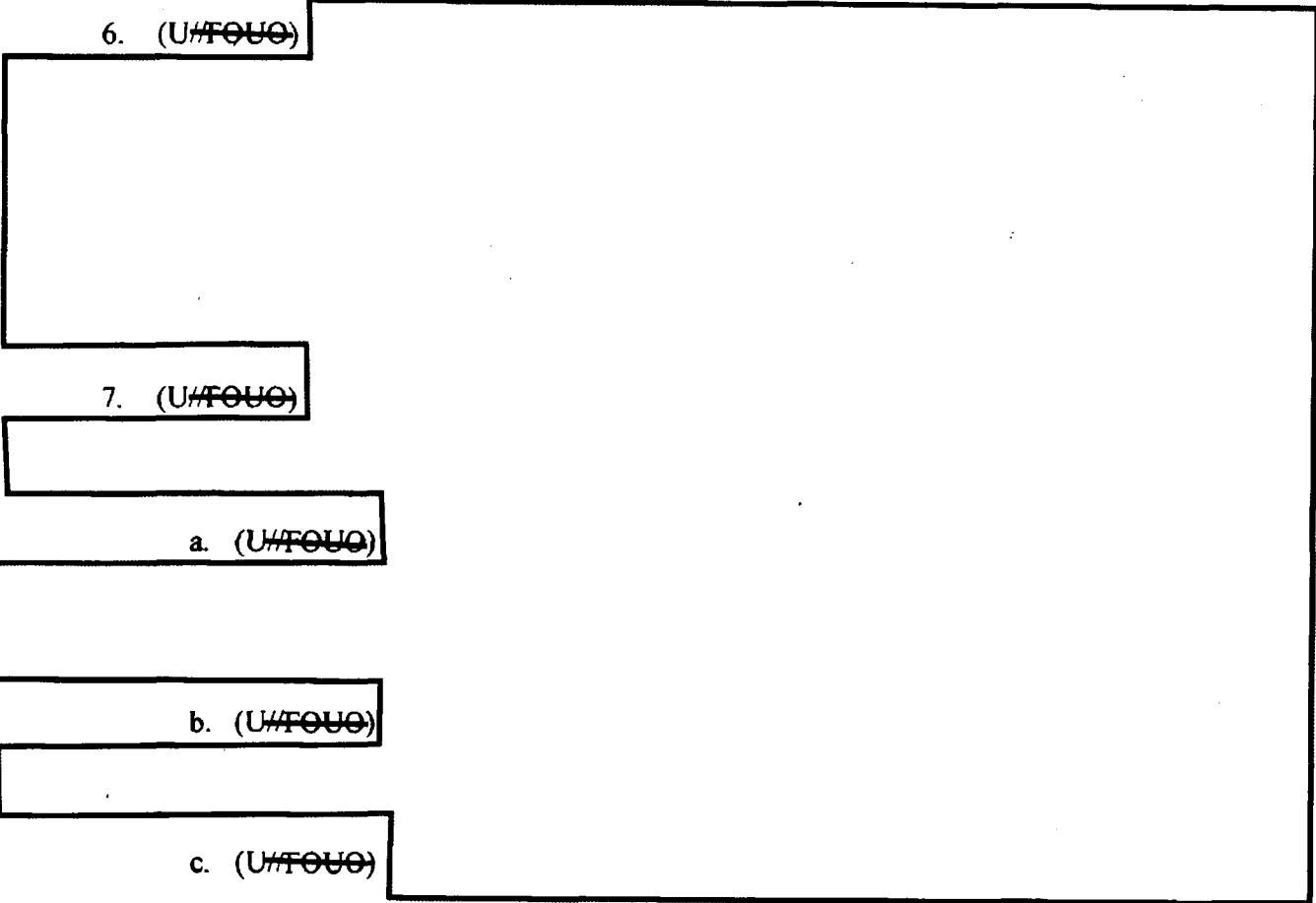
SECTION III – (U) DEFINITIONS

5. (U) Definitions and acronyms contained in reference a apply to this doctrine. Additional definitions of specialized terms that are unique to this doctrine are contained in ANNEX B.

SECTION IV – (U) EQUIPMENT/SYSTEM DESCRIPTION/LEVEL OF USE

6. (U//~~FOUO~~)

7. (U//~~FOUO~~)

   a. (U//~~FOUO~~)

   b. (U//~~FOUO~~)

   c. (U//~~FOUO~~)

8. (U) <u>Throughput</u> - The maximum throughput of the TACLANE Classic equipment will be 44.736 Mbps for ATM and 7 Mbps for IP. The TACLANE-E100 provides a maximum aggregate throughput of 165 Mbps full-duplex, or 100 Mbps half-duplex. The development of the TACLANE equipment is being performed in several releases providing initial and final capabilities.

9. (U) <u>TACLANE System Components</u> - The TACLANE system is comprised of a KG-175 equipment, a Crypto-Ignition Key (CIK), and an Ancillary Kit (optional). The Ancillary Kit includes one transit case, two extra CIKs, two AUI Cables, four DS-3 Cables, and two 10Base-T cables.

2

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

CNSS Instruction
No. 3029

10. (U//~~FOUO~~)

<p style="border:1px solid; height:100px;"></p>

    a. (U) Reference b sets forth minimum security standards for safeguarding, controlling, and using the LMD/KP.

    b. (U) Reference c sets forth minimum security standards for the protection and use of the DTD.

11. (U//~~FOUO~~)

SECTION V – (U) PERSONNEL RESPONSIBILITIES

12. (U) <u>Local Authority</u> - The Local Authority (LA) is responsible for the network and security configuration of all TACLANE equipment within the LA's domain. Specifically, the LA is responsible for the following functions:

    a. (U) Net planning; and

    b. (U) Requesting generation of FIREFLY credentials.

13. (U) <u>Security Administrator</u> - The Security Administrator (SA) (For the purpose of this doctrine the acronym SA will mean Security Administrator) is responsible for maintaining, monitoring, and controlling all functions performed by the TACLANE equipment. The SA also interfaces with both the COMSEC Custodian/Manager and the LA for management of keying material. The SA (or the designated Alternate SA) is the only individual who may fill TACLANE key and initialize CIKs. Since the SA or the alternate configures the security functions of the TACLANE, this individual must be knowledgeable of all TACLANE security functions. The SA is responsible for the following:

    a. (U) Performing initialization and distribution of CIKs to operators;

    b. (U) Receipting for all TACLANE key from the COMSEC custodian/manager;

    c. (U) Physical keying/rekeying of TACLANE equipment, including ensuring that each key is filled into the appropriate/approved TACLANE equipment;

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

3

d. (U) Ensuring that only approved procedures are followed for the storage, protection, and local accounting of TACLANE key and the SECRET Field Tamper Recovery (FTR) CIK for Release 2.0/2.0E or later versions of TACLANE;

e. (U) Notifying the COMSEC Custodian/Manager of incidents/insecurities affecting TACLANE material and ensuring recovery actions are taken, when appropriate;

f. (U) Performing zeroization of TACLANE equipment and/or disposal of CIKs. (In tactical environments, an operator may perform zeroization in an emergency situation); and

g. (U//FOUO)

14. (U) COMSEC Custodian/Manager - The COMSEC Custodian/Manager is responsible for the normal duties of a COMSEC Custodian, as well as providing the interface, through the appropriate channels, to the National Security Agency (NSA) for FIREFLY key and the key generation element for preplaced (traditional) key; ordering key, etc. Depending upon local conditions, the functions of LA and SA may be combined and vested in one individual or group of individuals. The role of COMSEC Custodian/Manager may also be combined with one or both of these roles.

15. (U//FOUO)

SECTION VI – (U) KEYING INFORMATION

16. (U) Controlling Authority - Reference d establishes the responsibilities of organizations that serve as controlling authorities for COMSEC keying material, and provides guidance for fulfilling those responsibilities.

17. (U) Key Distribution - All keying material will be distributed through means of the EKMS. Use of an EKMS key loader, (DTD, (SDS Secure DTD2000 System), and Simple Key Loader) will be means of loading key into the TACLANE equipment. The ordering, generation, and distribution of TACLANE key will follow established EKMS and COMSEC Material Control System (CMCS) doctrine.

18. (U) Types of Key

4

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

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

19. (U) <u>Cryptoperiods</u>

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

NOTE: (U) The cryptoperiod shall always expire on the last day of the same month one year following its generation. Thus, key that is generated by the Central Facility on June 5, 1998, shall expire on June 30, 1999.

d. (U//~~FOUO~~)

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

20. (U//~~FOUO~~)

NOTE: (U) The Changeover Preplaced TEK is a Preplaced TEK that is loaded into the TACLANE in anticipation of the expiration of the current Preplaced TEK. When a Changeover Preplaced TEK is loaded into the equipment, it shall automatically become effective on a predetermined date set by the SA. Once this occurs, the current Preplaced TEK shall automatically be deleted

21. (U) <u>Alarms</u> - TACLANE equipment does not contain an audible alarm feature. The operator must watch for the Alarm Light Emitting Diode (LED) indicator to light. An alarm message can be seen in the audit log.

SECTION VII - (U) CLASSIFICATION/MARKING

22. (U) Reference e provides general classification guidance for COMSEC information. The following additional guidance also applies:

a. (U) The TACLANE equipment is an UNCLASSIFIED/Controlled Cryptographic Item (CCI) when unkeyed.

b. (U) When keyed, the TACLANE is classified at the highest classification level of the key it contains, but never less than UNCLASSIFIED/CCI, and must be protected accordingly.

NOTE: (U) For the purpose of this document, a keyed TACLANE is a TACLANE with key loaded and a CIK inserted. If key is loaded but the CIK is removed and properly stored, the TACLANE is considered to be unkeyed.

23. (U) ANNEX C contains a summary of the classification and handling of TACLANE keying material and equipment.

SECTION VIII - (U) SECURITY AUDIT LOG

24. (U) <u>Audit Log</u> - The audit log may be retained in physical form by use of the General Dynamics Encryption Manager (GEM) or GEM Lite (both are defined in ANNEX B, item g). It is up to the local SA to determine how often the log is to be reviewed based on risk factors and local security policy. It is recommended the log be retained (off-line from the TACLANE equipment) for a period of time that is adequate for use in troubleshooting problems and insecurities. The length of time to retain

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

the audit log will be determined locally or by the parent department or agency. The information in the audit log is UNCLASSIFIED.

SECTION IX – (U) CONTROL REQUIREMENTS

25. (U) Control Requirements - Since the TACLANE equipment is UNCLASSIFIED/CCI when unkeyed, it must be handled as specified in paragraph 26 below. NSTISSI No. 4005 (reference f) prescribes the minimum national standards for safeguarding and control of classified COMSEC equipment and COMSEC keying material. Individuals requiring access to TACLANE equipment must possess an appropriate U.S. Government security clearance and must have a need-to-know for the equipment. Reference f also prescribes the minimum national standards for safeguarding COMSEC facilities operated by the U.S. Government or by contractors in connection with U.S. Government contracts.

26. (U) NSTISSI No. 4001 (reference g) prescribes the minimum national standards for handling and control of unkeyed CCI equipment and components.

27. (U//FOUO)

28. (U//FOUO)

    a. (U) The Operational CIK can be stored in the same room as the equipment; however, the CIK must be protected to the same classification level as the TACLANE. The CIK may be stored in a separate room from the TACLANE in a secure container that will afford adequate protection (e.g., a locked cabinet or desk will be sufficient).

    b. (U) Operational CIKs created for use during normal operations must be protected against unauthorized access and use. Prescribed controls are not needed for CIKs created for equipment testing using test TEKs.

    c. (U//FOUO)

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

CNSS Instruction
No. 3029

29. (U//FOUO)

a. (U) The EM workstation must be a stand-alone workstation or reside on a network dedicated to encryptor management. The EM workstation may not be used for general purpose computing or reside on a general purpose network.

b. (U) When using TACLANE in a low-to-high tunneling mode (i.e., CT side of TACLANE contains a higher classification than PT side), the following shall apply:

(1) (U) The EM workstation must be a stand-alone workstation and must be the only device connected to the PT side of the Fronting TACLANE;

(2) (U) With the exception of the Fronting TACLANE, TACLANEs may not be managed from the PT side;

(3) (U) The Fronting TACLANE and Managed TACLANE must physically reside within the protected boundary of the high-side network;

(4) (U) The operators of the EM must be cleared to the level of the high-side network; and

(5) (U) If the low-side network has connectivity to the unclassified Internet, SNMP management on both the PT and the CT sides must be disabled.

c. (U) Password protection on the EM Workstation is required when the workstation is in full configuration mode and is recommended when in limited configuration or monitor-only modes.

30. (U) Accountability

a. (U) The TACLANE equipment must be accounted for by its serial number and assigned Accounting Legend Code (ALC) 1. Detailed accounting requirements for CCI equipment are contained in reference g.

b. (U) Accountability Requirements for TACLANE Keying Material

(1) (U) All keying material distributed as set forth in paragraph 18, above, is assigned ALC-6 and shall be accounted for in accordance with requirements contained in reference f.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(2) (U) All keying material is accountable by registration number until actually loaded into the TACLANE equipment. The operational key is marked CRYPTO and may range from UNCLASSIFIED to TOP SECRET.

(3) (U) Keying material used in classroom training only shall be UNCLASSIFIED and used indefinitely. It is accounted for locally.

(4) (U) The FTRCIK is assigned ALC 4 and is accounted for within the COMSEC Material Control System (CMCS).

c. (U) CIKs must be accounted for locally. Local accounting is done by the SA. With respect to the CIKs, the local accounting procedures must include a record of all CIKs created along with the names and organizations/locations of the persons to whom they are issued. In addition, a responsible person must inventory the CIKs semi-annually or upon appointment of a new SA.

31. (U//~~FOUO~~)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

32. (U) <u>Transportation & Shipping</u>

a. (U//~~FOUO~~)

b. (U) Operator CIKs must be transported on the person of an authorized operator. When they must be shipped, they shall be handled through U.S.-controlled postal systems, preferably by U.S. Registered Mail. Operator CIKs must always be shipped separately from their associated equipment, except when the equipment has been zeroized as noted in paragraph 41 below.
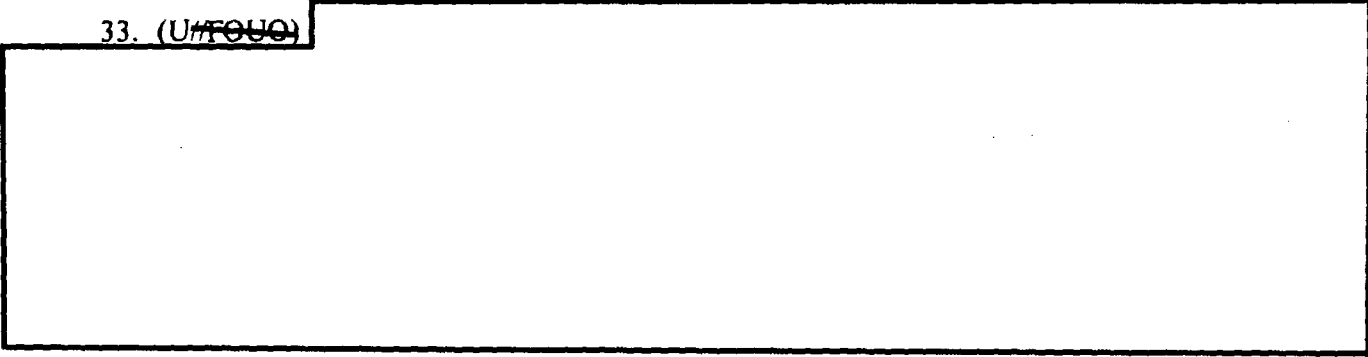
c. (U//~~FOUO~~)

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

33. (U//~~FOUO~~)

SECTION X – (U) MAINTENANCE

34. (U//~~FOUO~~)
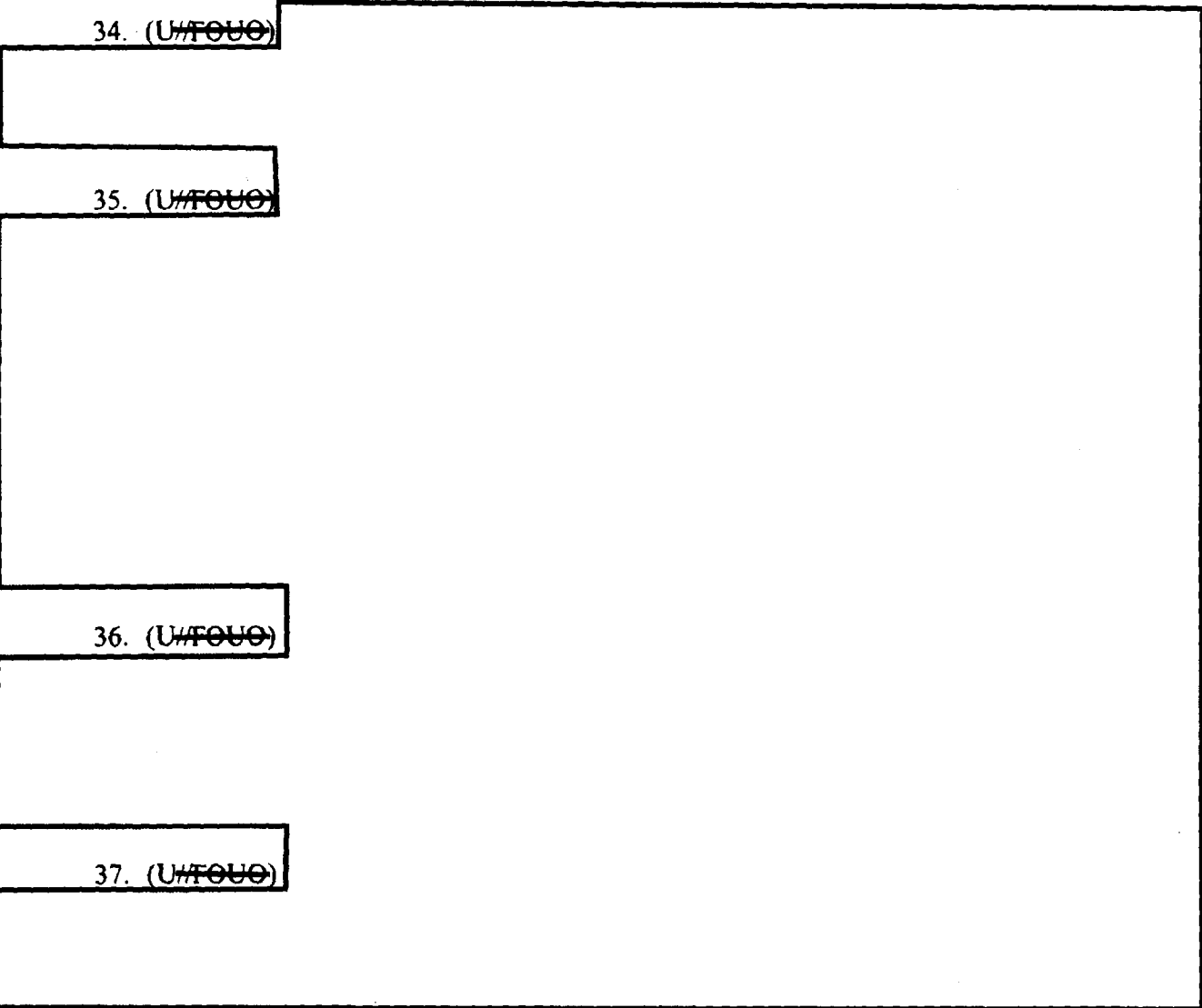
35. (U//~~FOUO~~)

36. (U//~~FOUO~~)

37. (U//~~FOUO~~)

10

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36
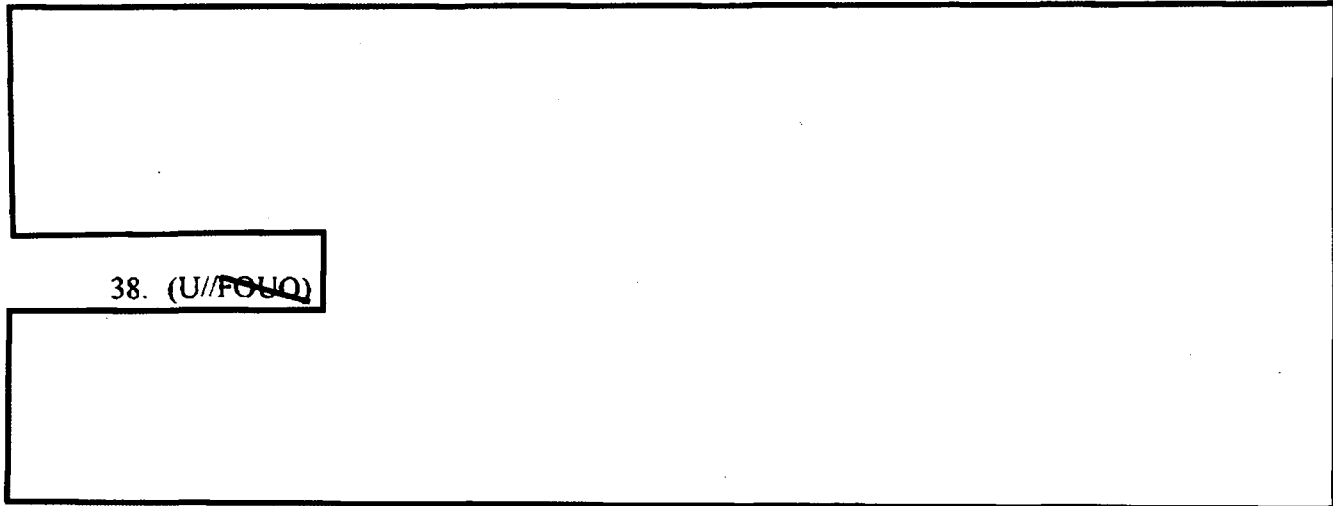
38. (U//FOUO)

SECTION XI – (U) DISPOSITION/DESTRUCTION

39. (U//FOUO)

40. (U) <u>Emergency Destruction</u> - In the event that emergency destruction is necessary, the device must be powered off by unplugging the AC line cord and by removing the battery from the battery compartment located on the front panel of the equipment. The battery cover is held on by two thumbscrews that can usually be removed by hand but may require a flat-blade screwdriver. Alternatively, a U.S. currency dime will also fit into the thumbscrew slot. Once all power has been removed for three seconds, all classified information, operating software, configuration data, and the key is deleted from the TACLANE device.

41. (U) <u>Zeroization</u>

    a. (U) Active (panic) zeroization of all key in the TACLANE equipment is accomplished from the equipment's front panel by simultaneously pressing both zeroization buttons. It may also be accomplished by operator command through the HMI. Any attempt to tamper with the equipment also results in complete zeroization.

    b. (U//FOUO)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36
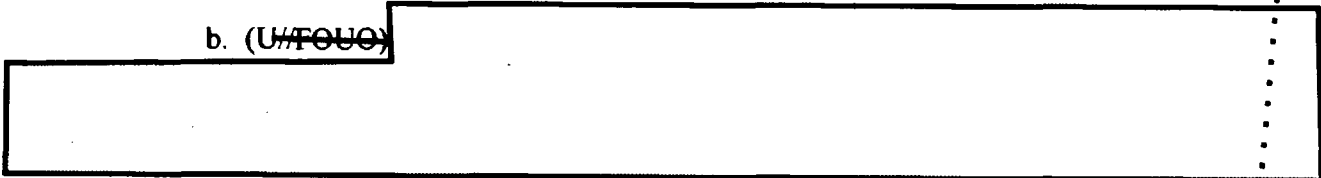
SECTION XII – (U) COMSEC INCIDENTS/ADMINISTRATIVE INCIDENTS

42. (U) Reference k contains a general listing of reportable COMSEC incidents and the standards for reporting them. Additional reportable COMSEC incidents specific to TACLANE follow:

a. (U//FOUO)

     (1) (U)

     (2) (U)

     (3) (U)

b. (U//FOUO)

c. (U) In addition, a COMSEC Incident Report must be submitted to DIRNSA, [   ] in accordance with requirements set forth in reference g using the standard reporting channels established within each Department or Agency for any of the following incidents:

     (1) (U) Loss of both an Operational CIK and its associated, keyed and unkeyed TACLANE equipment.

     (2) (U) Loss of an FTR CIK.

     (3) (U) Any suspected tampering, including that due to:

          (a) (U//FOUO) [   ]

          (b) (U) Opening the TACLANE unit.

     (4) (U) Unauthorized access to the equipment.

     (5) (U) Known or suspected theft of a keyed or unkeyed equipment.

     (6) (U) Shipment of a keyed equipment without having obtained prior authorization from the appropriate central authority for that equipment.

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

12

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

43. (U) <u>Administrative Incidents</u> - The following occurrences are administrative incidents which need not be reported to NSA unless there is an indication of espionage or sabotage. Such occurrences should, however, be monitored and evaluated within each using organization for possible follow-up action.

   a. (U//~~FOUO~~)
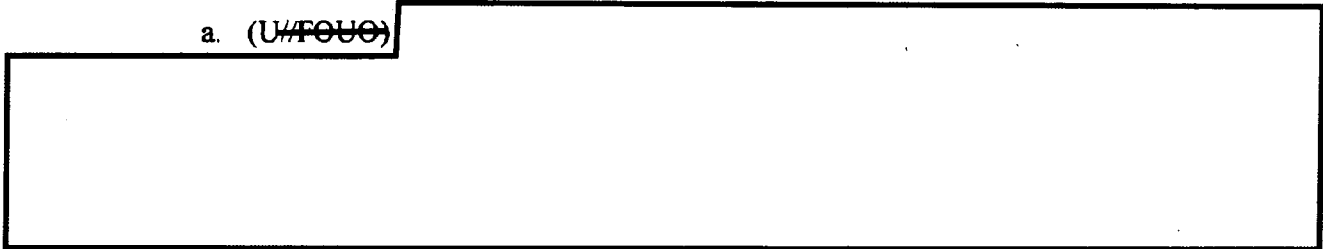
   b. (U) <u>Loss of any CIK</u> - Loss of a CIK must be promptly reported to the SA, who will immediately ensure deletion of that CIK from the specific TACLANE equipment with which it was associated. (Currently, the initial primary CIK cannot be deleted.) In addition, an "Insecure Practice" Report must be submitted through department or agency channels for appropriate action.

SECTION XIII - (U) EXCEPTIONS

44. (U) <u>Exceptions</u> - Requests for exceptions to any of the provisions of this doctrine must be approved, on a case-by-case basis, prior to implementation. Each request shall include a complete operational justification and shall be submitted through appropriate department or agency channels to DIRNSA, IA Policy, Procedures and Insecurities Division (I01P), for review.

3 Encls:
  1. ANNEX A - References
  2. ANNEX B - Definitions of Specialized Terms
  3. ANNEX C - TABLE, Classification and Handling of TACLANE (KG-175)
         Keying Material and Equipment

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

13

ANNEX A

<u>REFERENCES</u>

The information contained in this ANNEX is unclassified in its entirety.

The following national-level documents are referenced in this interim operational systems security doctrine:

      a. **NSTISSI No. 4009**, National Information Assurance (IA) Glossary, dated May 2003.

      b. **NAG No. 71**, Interim Operational Systems Security Doctrine for the Local Management Device/Key Processor (LMD/KP) (KOK-22), dated April 1997.

      c. **CNSSI No. 3021**, Operational Security Doctrine for the AN/CYZ-10/ 10A Data Transfer Device (DTD), dated September 2002.

      d. **NSTISSI No. 4006**, Controlling Authorities for COMSEC Material, dated 2 December 1991.

      e. **NTISSI No. 4002**, Classification Guide for COMSEC Information, dated 5 June 1986.

      f. **NSTISSI No. 4005**, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated August 1997.

      g. **NSTISSI No. 4001**, Controlled Cryptographic Items, dated July 1996.

      h. **NSTISSI No. 7000**, Tempest Countermeasures for Facilities (U), dated 29 November 1993.

      i. **NSTISSI No. 4000**, Communications Security Equipment Maintenance and Maintenance Training, dated January 1998.

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

      k. **NSTISSI No. 4003**, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.

ANNEX B

DEFINITIONS OF SPECIALIZED TERMS

a. (U) **Asynchronous Transfer Mode (ATM)** - ATM is a networking technology (data communications technology that is based on transmission of small, fixed-length data units called cells) that supports voice, video, imagery, and data applications over a single high-speed network.

b. (U//~~FOUO~~)

c. (U) **Human Machine Interface (HMI)** - The HMI is the front panel of the TACLANE equipment. The power switch, fill port, LCD window, zeroization buttons, and status LEDs are displayed on this panel. The CIK is also used at this location.

d. (U) **Local Authority [LA]** - The individual who is responsible for the network and security configuration of all TACLANE equipment within his/her domain.

e. (U) **Point To Point Key** - Key held by only two communication nodes versus a net of 3 or more where anyone can talk to anyone. This configuration is typical of trunk encryptors to limit the amount of data being protected by a single key.

f. (U) **Security Administrator [SA]** - The individual who is responsible for maintaining, monitoring, and controlling functions performed by the TACLANE equipment.
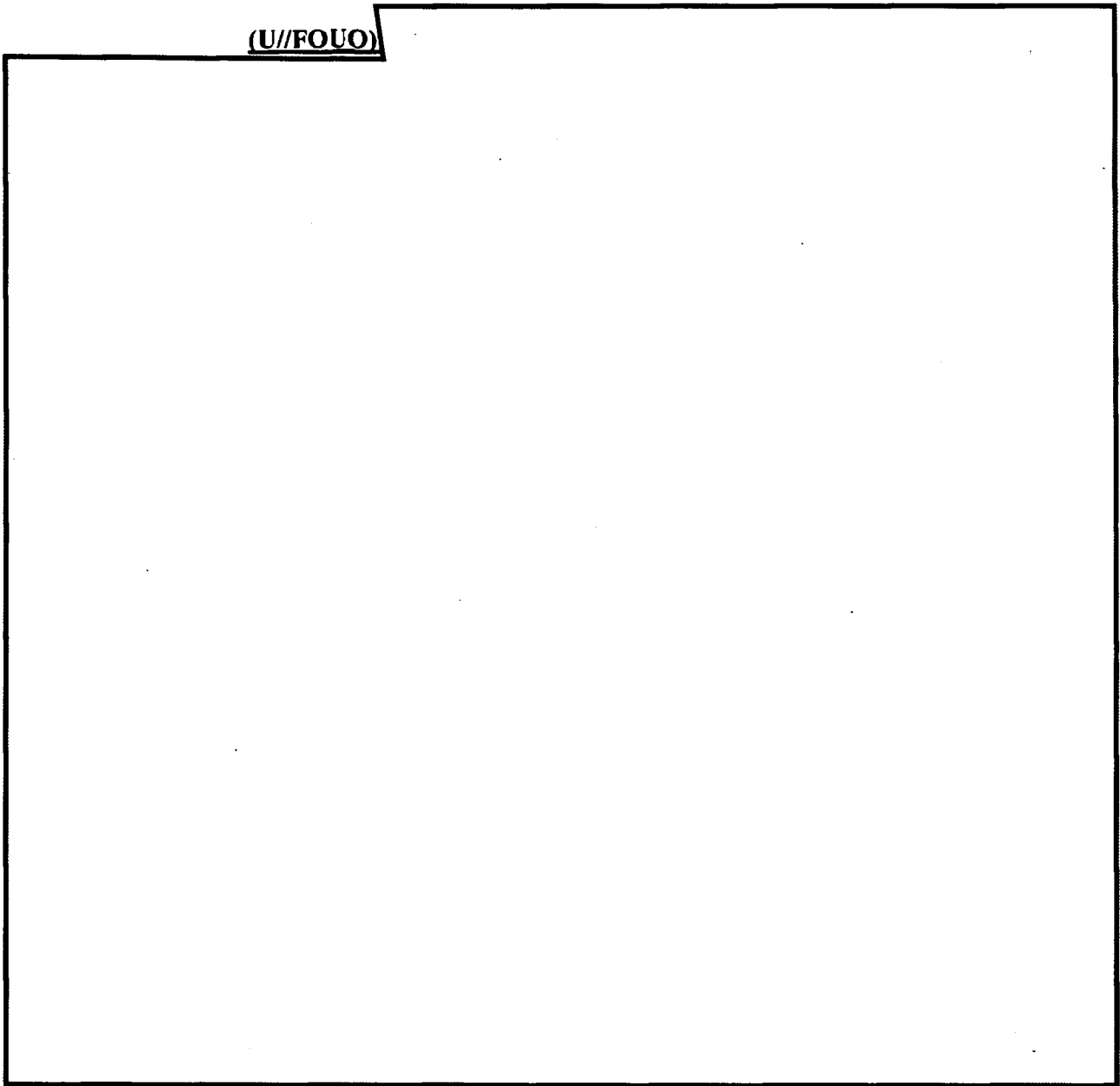
g. (U) **General Dynamics Encryptor Manager (GEM)** and GEM Lite are network management software packages for the TACLANE equipment. Services of the security manager include, but are not limited to: Audit data upload, remote on-line/off-line/restart control, compromise key list, and PVC (Permanent Virtual Circuit) configuration.

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

ANNEX C

(U//FOUO)

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

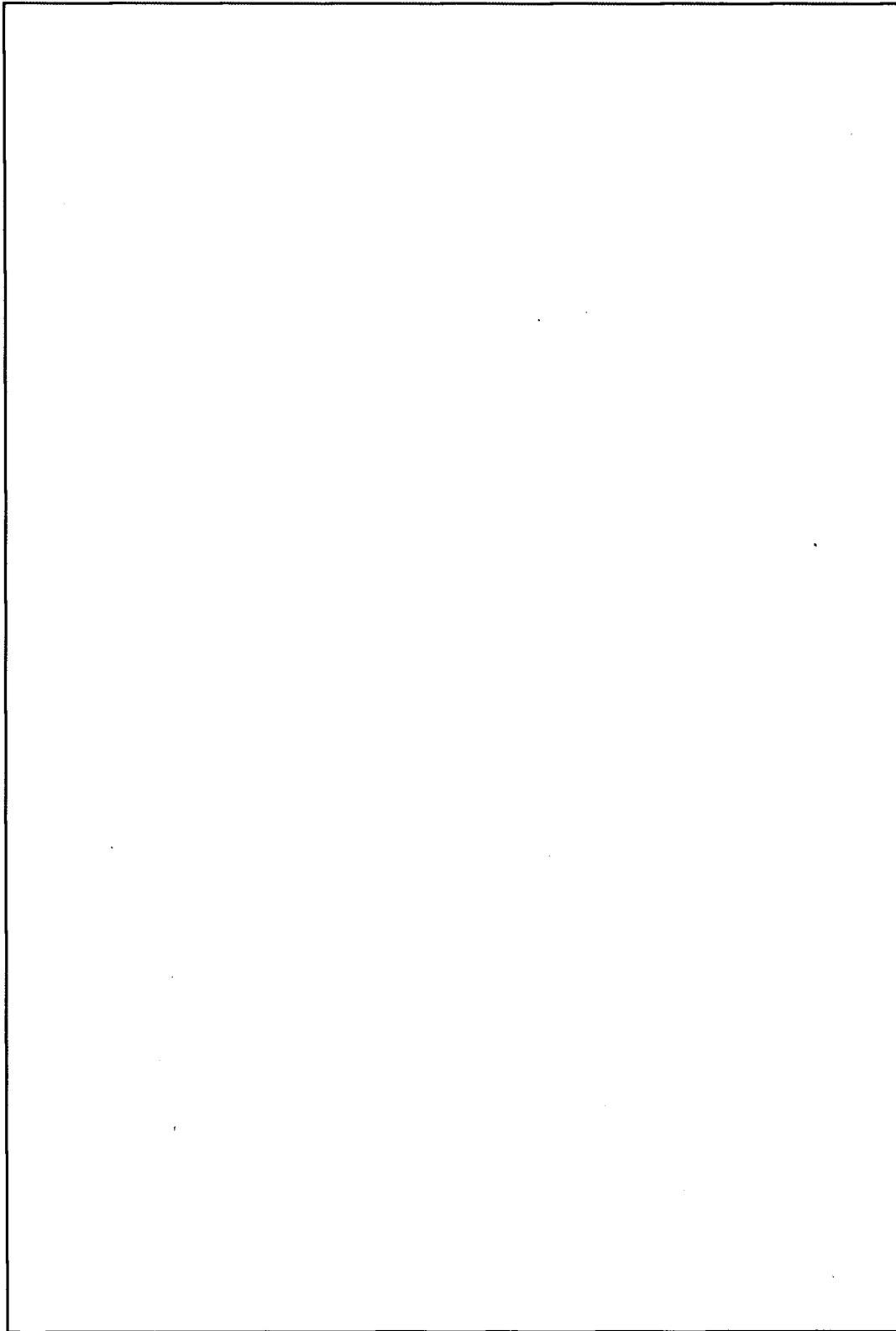UNCLASSIFIED//FOR OFFICIAL USE ONLY

DISTRIBUTION:

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