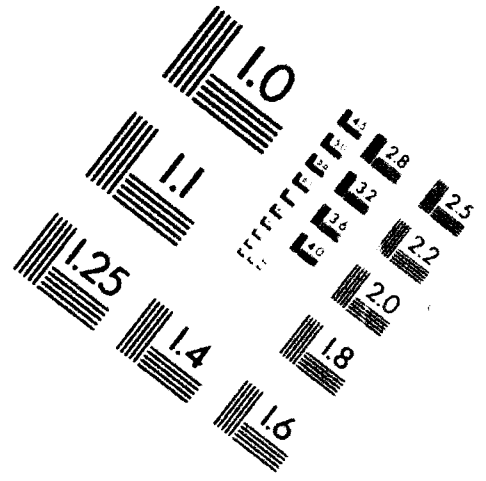
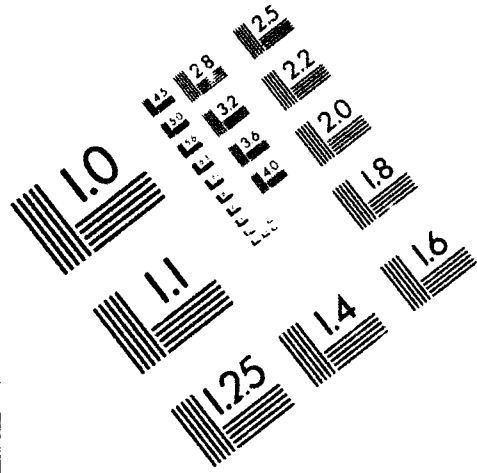




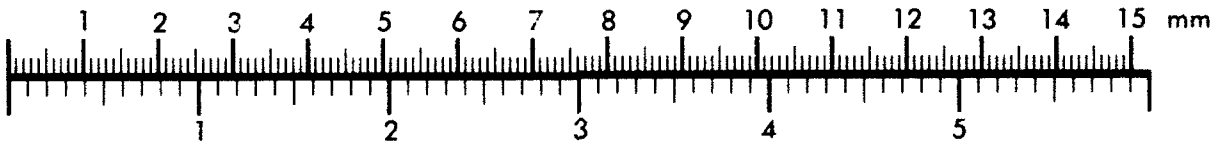
AIM

Association for Information and Image Management

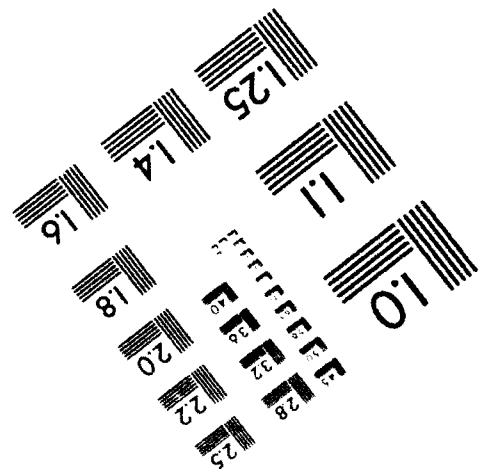
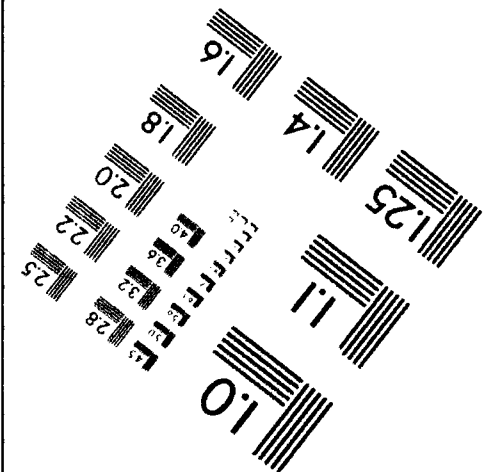
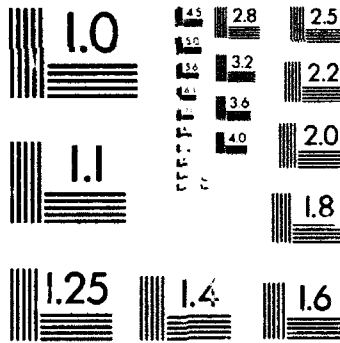
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202



Centimeter



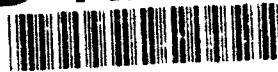
Inches



MANUFACTURED TO AIM STANDARDS
BY APPLIED IMAGE, INC.

2

AD-A270 027



5220.22-S

COMSEC SUPPLEMENT

TO

INDUSTRIAL SECURITY
MANUAL

FOR

SAFEGUARDING
CLASSIFIED
INFORMATION

S DTIC
ELECTE
OCT 04 1993
E D

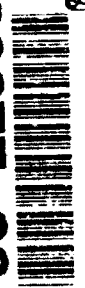


Approved for public release
Distribution unlimited

DEPARTMENT OF DEFENSE

MARCH 17, 1988

93-22968



151 pf

93 10 1 100



DEFENSE INVESTIGATIVE SERVICE
 1900 HALF ST. S.W.
 WASHINGTON, D.C. 20324-1700



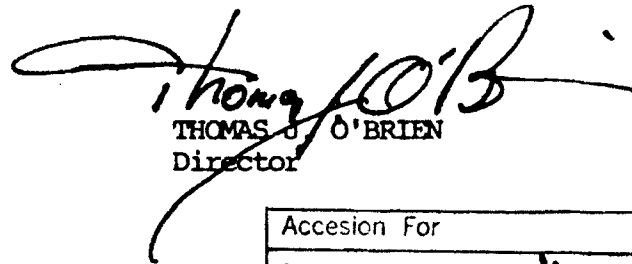
FOREWORD

This supplement to the Industrial Security Manual for Safeguarding Classified Information is issued under the authority of, and in accordance with, Department of Defense Directive 5220.22, "Department of Defense Industrial Security Program." It establishes uniform security practices within facilities used by prime and subcontractors having custody of classified or unclassified Communications Security (COMSEC) equipment/material of the Department of Defense and certain other Executive Departments and Agencies. Users of this publication are encouraged to submit recommended changes and comments to improve the publication to the Director, Defense Investigative Service.

In coordination with the National Security Agency (NSA), this Supplement includes detailed guidance in the areas of COMSEC accounting and control.

Included in this Supplement are provisions relative to Controlled Cryptographic Items (CCI's). These provisions delineate the minimum requirements for the acquisition and ownership, transportation, physical security and access control, key accounting, reporting of insecurities and disposition of CCI materials at contractor facilities.

This revision is issued pursuant to section 1A(i) of the Department of Defense Security Agreement (DD Form 441).


 THOMAS J. O'BRIEN
 Director

DTIC QUALITY INSPECTED 2

Accession For	
NTIS CRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

COMSEC SUPPLEMENT

Foreword

Section I - General.....1

- 1. Introduction
- 2. Purpose
- 3. Scope
- 4. Definitions
- 5. Subcontracting
- 6. TEMPEST Countermeasures
- 7. Foreign Bids and Proposals

Section II - Access Requirements.....17

- 8. Requirements for Access to Classified Information
- 9. Requirements for Access to Controlled Cryptographic Items (CCIs)
- 10. Briefing and Debriefing Requirements
- 11. Records of Briefings/Debriefings

Section III - Establishing a COMSEC Account/Subaccount.....21

- 12. Requirements for a Classified COMSEC Account
- 13. Requirements for an Unclassified COMSEC Account
- 14. Requirements for COMSEC Subaccounts
- 15. Conversion from a COMSEC Subaccount to a Primary COMSEC Account
- 16. Selection of COMSEC Custodian and Alternate COMSEC Custodian
- 17. Indoctrination and Guidance for the COMSEC Custodian
- 18. Duties of the COMSEC Custodian, Alternate COMSEC Custodian and Facility Security Officer
- 19. Temporary Absence of the COMSEC Custodian
- 20. Return of the COMSEC Custodian from Temporary Absence
- 21. Change of COMSEC Custodian
- 22. Change of Alternate COMSEC Custodian
- 23. Change of Facility Security Officer
- 24. Sudden, Indefinite, or Permanent Departure of the COMSEC Custodian
- 25. Sudden, Indefinite, or Permanent Departure of the Alternate COMSEC Custodian or Facility Security Officer
- 26. Requirements for Closing a Primary COMSEC Account
- 27. Requirements for Closing a COMSEC Subaccount

Section IV - COMSEC Material.....33

- 28. Identification
- 29. Accounting Legend Codes

Section V - Ownership and Acquisition of CCI.....35

- 30. General
- 31. Ownership Categories
- 32. Eligibility Criteria for CCI Equipment Ownership
- 33. Requirements and Procedures for Contractor Acquisition of CCI Equipment
- 34. Contractor Certification to the Authorized Vendor
- 35. Authorized Vendor Responsibilities

Section VI - The COMSEC Material Control System.....39

- 36. General
- 37. Responsibilities
- 38. COMSEC Material Control System Forms, Files, and Reports
- 39. Preparation of COMSEC Register File and COMSEC Accounting Reports
- 40. Hand Receipts
- 41. Possession Reports
- 42. Conversion of COMSEC Material
- 43. Inventory Report
- 44. Classification of COMSEC Accounting Reports and Files
- 45. Retention and Disposition of COMSEC Accounting Records
- 46. Accounting for and Entering Amendments to COMSEC Publications
- 47. Accounting for COMSEC Material Prior to Acceptance by the U.S. Government
- 48. Accounting for Government-Furnished Property and New Material
- 49. Residual Inventory and Master Disposition Record
- 50. Receipt of COMSEC Material
- 51. Procedures for Handling Keying Material
- 52. Transfer of COMSEC Material
- 53. NSA Central Office of Record and Military Department Accounting Headquarters
- 54. Packaging COMSEC Material for Shipments Outside the Facility
- 55. Authorized Modes of Transportation
- 56. CCI Equipment Distribution

Section VII - Handling and Control of Classified COMSEC Material During Development and Manufacture/Assembly65

- 57. General
- 58. Requirements
- 59. Reconciliation of In-Process Accounting Records
- 60. Auditing of In-Process Accounting Records

Section VIII - Handling and Control of Classified COMSEC Manuals During Development69

- 61. General
- 62. Entering Manuscripts into the COMSEC Material Control System

Section IX - Handling and Control of CCI During Development and Manufacture/Assembly.....71

- 63. Background and Scope
- 64. Requirements
- 65. Manufacture and Assembly in Production
- 66. Transition from Classified to CCI
- 67. Access
- 68. In-Process Controls
- 69. In-Process Procedures
- 70. Required Item Information
- 71. Breakage and Scrap
- 72. Loss of In-Process Controlled Material
- 73. Transition from In-Process Controls to Control Within the Formal COMSEC Accounting System
- 74. Destruction of CCI Materials
- 75. Subcontracting
- 76. Reconciliation of In-Process Accounting Records
- 77. Labeling of Components, Assemblies and Equipments
- 78. Auditing of In-Process Accounting Records

Section X - Keying Material Management.....79

- 79. General
- 80. Keying Material Source
- 81. Designation of Controlling Authorities
- 82. Responsibilities of a Controlling Authority
- 83. Considerations in Establishing a Cryptonet
- 84. Keying Material Support Plan (KMSP)
- 85. Contents of the Keying Material Support Plan
- 86. Annual Review of Keying Material

Section XI - Physical Security.....85

- 87. General
- 88. Closed Area Designation and Access Controls
- 89. CCI Access Controls
- 90. Storage Requirements
- 91. Record of Individuals Having Knowledge of the Combinations to Containers Storing Classified COMSEC Material

Section XII - Protection of Lock Combinations for Vaults and Containers Under the Control of the COMSEC Custodian/Alternate COMSEC Custodian.....91

- 92. General
- 93. Protective Packaging of Lock Combinations
- 94. Periodic Inspection and Superseded Combinations

Section XIII - Displays, Demonstrations and Marketing of CCI Equipment.....95

- 95. General
- 96. Requirements

Section XIV - Routine Destruction of COMSEC Material.....99

- 97. General
- 98. Training of Destruction Personnel
- 99. Procedures for Routine Destruction of COMSEC Material
- 100. Routine Destruction Methods
- 101. NSA-Approved Routine Destruction Devices
- 102. Reporting Destruction

Section XV - COMSEC Emergency Action Procedures.....103

- 103. Emergency Protection Planning
- 104. Preparedness Planning for Disasters
- 105. Preparedness Planning for Hostile Actions
- 106. Preparing the Emergency Plan
- 107. Emergency Destruction Priorities
- 108. Emergency Destruction Tools
- 109. Emergency Destruction Methods
- 110. Reporting Emergency Destruction
- 111. Review of Emergency Action Procedures

Section XVI - COMSEC Insecurity Requirements.....111

- 112. General
- 113. Types of COMSEC Insecurities
- 114. Reporting Insecurities
- 115. Types of Reports
- 116. Format and Content of Insecurity Letter Reports

Section XVII - Inspections/Audits of COMSEC Accounts.....119

- 117. Notification
- 118. Access
- 119. DIS Inspection Criteria
- 120. Report of Inspection
- 121. COR Audit Criteria
- 122. Primary COMSEC Account Audit
- 123. Report of COR Audit of Primary COMSEC Account
- 124. Report of COR Audit of COMSEC Subaccount
- 125. Report of Primary COMSEC Account Audit of its COMSEC Subaccount

APPENDIX I - Controlling Authority Insecurity Evaluation Guidance.....AI-1
APPENDIX II - COMSEC Briefing.....AII-1
APPENDIX III - CCI Control Agreement.....AIII-1
APPENDIX IV - Contracting Officer Authorization to Purchase CCI Equipment as
Contractor Acquired Property.....AIV-1
APPENDIX V - Figures.....AV-1

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION I. GENERAL

1. Introduction. The United States (U.S.) Communications Security (COMSEC) effort is controlled and managed under a separate set of security standards and procedures from those which apply to other classified information. The reasons for this are that COMSEC techniques and materials are targets continually sought by hostile intelligence services and because the loss of U.S. COMSEC information and materials can seriously damage the national interest. There is also a significant body of information indicating that TOP SECRET keying material is a high priority target for exploitation by hostile intelligence services and, therefore, it must be afforded special attention. The procedures relative to TOP SECRET keying material contained in this Supplement do not apply to Nuclear Command and Control COMSEC material which is controlled in accordance with JCS PUB 13, nor to key locally generated for immediate use, but they do apply to locally generated key which is held in physical or electronic form for future use. This Supplement establishes security requirements consistent with national policy established to protect U.S. communications as it applies to the private sector.

a. Department of Defense (DoD) COMSEC information is made available to contractors and their subcontractors under one or more of the following conditions:

(1) When electrical transmission of classified or sensitive unclassified national defense information among contractors, or between contractors and the Government, is required.

(2) When research, development, production or testing of COMSEC equipment or of communications equipment interfacing with COMSEC equipment is being undertaken on behalf of the Government.

(3) When the contractor is required to install, maintain or operate accountable COMSEC equipment in support of U.S. Government contracts.

b. The Deputy Director for Information Security, National Security Agency (NSA), his designated representative, or the Secretary or Head of the User Agency, or his designated representative, may establish additional physical safeguards for the protection of classified COMSEC information because of the nature of the item or the conditions under which it is to be produced or used. Such additional requirements shall be made applicable by incorporation in the contract or through appropriate notification from the contracting officer and shall be incorporated into the DoD Contract Security Classification Specification (DD Form 254).

c. Official instructions for the operation and installation of crypto-systems provided by the government or acquired by the contractor are not included in this supplement. They will be furnished separately to the contractor.

d. To help contractors and government personnel simplify their search for appropriate information systems security, the National Security Agency publishes The Information Systems Security Products and Services Catalogue quarterly. It is available by subscription from the U.S. Government Printing Office. This document contains separate lists of five different categories of NSA-endorsed or -evaluated information systems security products and services.

e. The contractor shall include procedures in or prepare a supplement to his Standard Practice Procedures (SPP), required by paragraph 5s, ISM, to cover COMSEC requirements.

2. PURPOSE. The purpose of this Supplement is to establish policies, procedures and responsibilities for the control of COMSEC material furnished to, generated or acquired by U.S. industry. This Supplement covers the safeguarding controls for classified and unclassified COMSEC material and equipment resident at cleared industrial facilities.

3. SCOPE. This Supplement serves as the single authoritative source for cleared industrial facilities engaged in the development, production, testing, or operational use of COMSEC material in support of U.S. Government contracts.

4. DEFINITIONS. For the purpose of this Supplement, the following definitions apply:

a. ACCESS: The ability and opportunity to obtain knowledge of classified or sensitive information, equipment, or other materials; or the ability and opportunity to have unrestricted use, handling, or physical control thereof. The particular requirements for access to different categories of COMSEC materials vary, and are detailed in this supplement and other official documents.

b. ACCOUNTING LEGEND CODE (AL): A numeric code used to indicate the minimum accounting controls required for COMSEC material. (May also be abbreviated ALC.)

c. ACCOUNTING NUMBER: A number assigned to an individual item of COMSEC material to facilitate its handling and accounting (may also be called register number or serial number).

d. ALC: See Accounting Legend Code.

e. ALTERNATE COMSEC CUSTODIAN: The individual designated by proper authority to perform the duties of the COMSEC Custodian during the temporary absence of the COMSEC Custodian.

f. APPROVED CCI COMMERCIAL CARRIER: A commercial carrier certified by the Military Traffic Management Command (MTMC) or the General Services Administration (GSA) as providing "Constant Surveillance Service (CSS)".

g. ATTENDED: Under continuous positive control of contractor personnel authorized for access or use.

h. AUTHENTICATION: A security measure designed to protect a communications system against acceptance of fraudulent transmissions or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

i. AUTHORIZED COMPANY COURIER: A duly authorized and trustworthy individual who has been officially designated to transport/carry COMSEC information and, if the material is classified, is cleared to the level of the material being transported.

j. AUTHORIZED VENDOR PROGRAM: A program in which a vendor producing secure telecommunications or COMSEC product under contract to NSA is authorized by NSA to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers under conditions set forth in a Memorandum of Understanding between NSA and the producing vendor.

NOTE: Eligible buyers are typically Government organizations or Government contractors. Products authorized for marketing and sale are placed on the Endorsed Cryptographic Products List.

k. AUTOMATED INFORMATION SYSTEM SECURITY: The totality of security safeguards used to provide a defined level of protection to an automated information system and data handled by it.

l. BINDING: The process of associating a specific communications terminal with a specific key.

m. CA: See Controlling Authority.

n. CALL KEY: See Per Call Key.

o. CANISTER: A type of protective packaging for key in punched or printed tape form.

p. CAP: See Contractor Acquired Property.

q. CCEP: See Commercial COMSEC Endorsement Program.

r. CCI: See Controlled Cryptographic Item.

s. CENTRAL OFFICE OF RECORD (COR): A central office which keeps records of all COMSEC material received by or generated within elements subject to its oversight.

NOTE: Usually within a Government department or agency, its duties include establishing and closing COMSEC accounts, maintaining records of COMSEC Custodian and Alternate COMSEC Custodian appointments, performing COMSEC inventories, and responding to queries concerning account management.

t. CERTIFICATION OF ACTION STATEMENT: A statement attached to the Report of a COMSEC audit by which a COMSEC Custodian certifies that all actions have been completed.

u. CERTIFIED INSTALLATION: An installation that has been determined by the government to meet minimum applicable physical and technical security requirements for the installation of COMSEC equipment.

v. CIK: See Crypto-Ignition Key.

w. CLEARED COURIER: A duly authorized, cleared (to the level of the information being transported), and trustworthy person who has been officially designated to transport classified information.

x. CO: See Contracting Officer

y. COGNIZANT SECURITY OFFICE: The Defense Investigative Service Director of Industrial Security having industrial security jurisdiction over the geographical area in which a facility is located.

z. COMMERCIAL COMSEC ENDORSEMENT PROGRAM (CCEP): A program in which cryptographic subsystems and telecommunications equipment using embedded cryptography are developed, produced, and marketed in accordance with formal agreements between individual commercial vendors and the National Security Agency.

NOTE: Formal agreements are in the form of Memoranda of Understanding (MOU) and more comprehensive Memoranda of Agreement (MOA) between NS. and the commercial vendors. Products proposed for the CCEP must satisfy a number of requirements. The product must be of direct and obvious benefit in meeting national security objectives. The company must not be foreign owned, controlled or influenced, as evidenced by completion and satisfactory evaluation of Certificate Pertaining to Foreign Interest (DD Form 441S). It must obtain a facility clearance and be able to meet NSA product assurance survey requirements. After the product is satisfactorily evaluated, it is endorsed by NSA, placed on the Endorsed Cryptographic Products List, and becomes available for direct marketing and sale to eligible buyers.

aa. COMMON FILL DEVICE (CFD): Any one of a family of devices developed to read in, transfer, or store key (e.g., KOI-18, KYK-13).

ab. COMMUNICATIONS SECURITY (COMSEC): Measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications.

NOTE: COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information. See also Telecommunications and Automated Information Systems Security.

ac. COMPROMISE: a. (General) The disclosure of classified data to persons not authorized to receive that data.

b. (Automated Information Systems) A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information may have occurred.

ad. COMPUTER SECURITY (COMFUSEC): See Automated Information System Security.

ae. COMSEC: The abbreviation for Communications Security.

af. COMSEC ACCOUNT: An administrative entity identified by an account number, responsible for maintaining custody and control of COMSEC material. (See also Primary Account and Subaccount.)

ag. COMSEC ACCOUNT AUDIT: The periodic examination, announced or unannounced, of COMSEC accounts by the appropriate COR.

ah. COMSEC ACCOUNTING: Procedures which document the control of COMSEC material from its origin through destruction or other final disposition.

ai. COMSEC AIDS: All COMSEC material, other than equipments or devices, which assists in securing telecommunications and is required in the production, operation, and maintenance of COMSEC systems and their components. Some examples are: COMSEC keying material and supporting documentation, such as operating and maintenance manuals.

aj. COMSEC CONTRACTOR: A contractor authorized by contract with the U.S. government to produce COMSEC material.

ak. COMSEC CUSTODIAN: The individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. This applies to both primary accounts and subaccounts.

al. COMSEC EQUIPMENT: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor, and by reconverting such information to its original form for authorized recipients, and equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, and authentication equipment.

am. COMSEC FACILITY: A facility which contains classified COMSEC material.

an. COMSEC INSECURITY: Any occurrence which jeopardizes the security of COMSEC material or the secure electrical transmission of classified or sensitive government information.

ao. COMSEC INVENTORY RECONCILIATION REPORT: A certificate issued by the COR that compares the semiannual inventory of a COMSEC account with the COR's records and identifies any discrepancies noted.

ap. COMSEC MATERIAL: COMSEC aids and hardware which have the purpose to secure telecommunications or to ensure authenticity of such communications.

NOTE: COMSEC material includes, but is not limited to, COMSEC key, CCI, items which embody or describe COMSEC logic, and other items which perform COMSEC functions.

aq. COMSEC MATERIAL CONTROL SYSTEM (CMCS): A logistics system through which COMSEC material marked "CRYPTO" and other COMSEC material is distributed, controlled, and safeguarded.

NOTE: The CMCS consists of all COMSEC Central Offices of Record (CORs), cryptologic depots, and COMSEC accounts and sub-accounts.

ar. COMSEC MEASURES: All COMSEC techniques used to secure telecommunications or COMSEC material.

as. COMSEC REGISTER FILE: An accounting file containing a record of each COMSEC item accountable by a contractor.

at. COMSEC SUPPORT SERVICES: See Contractor COMSEC Support Services.

au. COMSEC SUPPORT SYSTEM: The documentation, doctrine, keying material, protection, equipment engineering, production, distribution, modification and maintenance of COMSEC material.

av. COMSEC SYSTEM: The combination of all measures intended to provide communications security for specific telecommunications systems, including associated cryptographic, transmission, emission, computer and physical security measures, as well as the COMSEC support system.

aw. COMSEC VENDOR: A contractor authorized to produce and sell COMSEC equipment.

ax. CONFIGURATION CONTROL: The requirement for proper authority to be granted before a modification can be made to system's hardware, firmware, software, or documentation, so that the system is protected against the introduction of improper modification prior to, during, and after systems implementation.

ay. CONTINGENCY KEY: Keying material held for use on a cryptonet under specific operational conditions or in support of specific contingency plans.

az. CONTRACTING OFFICER (CO): Any government official who in accordance with departmental or agency procedures is currently designated as a contracting officer with the authority to enter into and administer contracts and make determinations and findings with respect thereto or any part of such authority.

ba. CONTRACTOR-ACQUIRED PROPERTY (CAP): Property acquired by or otherwise provided to a contractor for performance under a contract and to which the Government has title.

bb. CONTRACTOR COMSEC SUPPORT SERVICES: Services provided at the contractor level including installation, maintenance, keying, etc.

bc. CONTRACTOR-OWNED EQUIPMENT: See Plant Equipment.

bd. CONTROLLED CRYPTOGRAPHIC ITEM (CCI): A secure telecommunications or information handling equipment, or associated cryptographic component or ancillary device which is unclassified when unkeyed (or when keyed with unclassified key) but controlled. Equipments and components so designated shall bear the designator "Controlled Cryptographic Item" or "CCI".

NOTE: Certain non-cryptographic hardware items which perform critical COMSEC functions are also designated "CCI." CCIs may be procured only by government entities and government contractors.

be. CONTROLLED SPACE: An area to which access is physically controlled.

bf. CONTROLLING AUTHORITY (CA): The designated official responsible for directing the operation of a cryptonet.

bg. COR: See Central Office of Record

bh. CRYPTO: A marking or designator identifying all COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive but unclassified government or government-derived information, the loss of which could adversely affect the national security interest.

bi. CRYPTO-ANCILLARY EQUIPMENT: Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not itself perform cryptographic functions.

bj. CRYPTO-EQUIPMENT: Equipment which embodies a cryptographic logic.

bk. CRYPTOGRAPHIC COMPONENT: The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or automated information processing system. A cryptographic component may be a modular assembly, a printed wiring assembly (PWA), a microcircuit, or a combination of these items.

bl. CRYPTOGRAPHY: The principles, means, and methods for rendering plain information unintelligible to the uninitiated and for restoring encrypted information to intelligible form.

bm. CRYPTO-IGNITION KEY (CIK): A key storage device that must be plugged into a COMSEC equipment to enable secure communications.

bn. CRYPTOMATERIAL: All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.

bo. CRYPTONET: The stations holding a specific short title of operational or contingency key who can communicate with one another.

bp. CRYPTONET COMPARTMENTATION: Limiting cryptonet size as a means of controlling the volume of traffic protected by that key or limiting the distribution of key to specific user communities.

bq. CRYPTOPERIOD: The time span during which each key setting for a cryptoperiod remains in effect.

br. CRYPTOSEcurity: The security or protection resulting from the proper use of technically sound cryptosystems.

bs. CRYPTOSYSTEM: The associated items of COMSEC material used as a unit to provide a single means of encryption or decryption.

bt. CSO: See Cognizant Security Office.

bu. DCS: See Defense Courier Service.

bv. DCS FORM 1: The receipt for material shipped via DCS.

bw. DCS FORM 10: The Defense Courier Authorization Record which authorizes contractor personnel to receipt for DCS shipped material.

NOTE: ARFCOS Forms 1 and 10 may be used until exhausted.

bx. DD250: Material Inspection and Receiving Report.

by. DECRYPTION: A generic term encompassing decoding and deciphering.

bz. DEFENSE COURIER SERVICE (DCS): Formerly ARMED FORCES COURIER SERVICE. The Defense Courier Service was established by Department of Defense Directive 5200.33, dated September 30, 1987. The DCS is a joint military courier organization under the cognizance of the Commander in Chief, Military Airlift Command (CINCMAC). The DCS is authorized to transport all types and classifications of Government materials, including classified cryptographic equipment, and keying materials designated CRYPTO.

ca. DEPOT MAINTENANCE: See Full Maintenance

cb. DESTRUCTION REPORT: Documentation on an SF153 of the physical or electronic destruction of COMSEC material by NSA-authorized means.

cc. DIRECT SHIPMENT: Shipment of COMSEC material directly from NSA to using COMSEC accounts.

cd. DIRNSA: The Director, National Security Agency. Often used as a generalized address for official correspondence with the National Security Agency.

ce. DIS: Defense Investigative Service.

cf. DROP ACCOUNTABILITY: A procedure under which a COMSEC account initially receipts for COMSEC material, and then provides no further accounting for it to its Central Office of Record (COR). AL-4 items are drop accountable.

cg. ELEMENT: A subdivision of COMSEC equipment, or an assembly or sub-assembly which normally consists of a single piece or group of replaceable parts. An element is a removable item necessary to the operation of an equipment, but does not necessarily perform a complete function in itself.

ch. EMBEDDED CRYPTOGRAPHY: Cryptography incorporated within an equipment or system whose basic function is not cryptographic.

ci. EMISSION SECURITY: The protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems and telecommunications systems.

cj. FAR: Federal Acquisition Regulation.

ck. FILL DEVICE: See Common Fill Device.

cl. FORMAL TRAINING: Classroom and laboratory instruction conducted by qualified instructors using an approved course of instruction and employing a method for determining whether the student meets established performance requirements for satisfactory completion. "On-the-job" training does not meet the intent of this definition.

cm. FORTUITOUS CONDUCTOR: Continuous metallic objects (e.g., water pipes, heating/cooling ducts, ceiling grids, structural steel, etc.) capable of serving as a conduction path for compromising emanations through the controlled space boundary.

cn. FULL MAINTENANCE: Complete diagnostic repair, modification, and overhaul of COMSEC equipment including repair of defective assemblies by piece part replacement.

co. GOVERNMENT CONTRACTOR TELECOMMUNICATIONS: Telecommunications between or among government departments or agencies and their contractors, and telecommunications of, between or among government contractors and their subcontractors, which relate to Government business or performance of a Government contract.

cp. GOVERNMENT FURNISHED PROPERTY (GFP): Property in the possession of, or directly acquired by the Government, and subsequently made available to a contractor but to which the Government retains ownership. Government Furnished Equipment (GFE) is included in this definition.

cq. HAND RECEIPT: A document used to record local or temporary transfer of COMSEC material from a COMSEC Custodian to a user and acceptance by the user of the responsibility for the COMSEC material.

cr. HARD-COPY KEY: Physical keying material such as printed key cards/lists, punched key tapes, or programmable, read-only memories (PROMs).

cs. HARD-WIRED KEY: Key which is permanently installed in a COMSEC equipment.

ct. IMITATIVE (COMMUNICATIONS) DECEPTION: Introduction of deceptive messages or signals into an adversary's telecommunications signals.

cu. INDUSTRIAL TEMPEST PROGRAM: A program established to support U.S. manufacturers who wish to produce TEMPEST-suppressed equipment to sell to the U.S. Government. Qualified participants in the program are supplied classified TEMPEST information. Resulting equipment, if accredited, will be listed in the U.S. Government Preferred Products List.

cv. INFORMATION SYSTEMS SECURITY PRODUCTS AND SERVICES CATALOGUE: Published quarterly by the NSA Information Systems Security Organization and available by subscription from the U.S. Government Printing Office (GPO), this document contains five lists which were previously published separately: The Endorsed Cryptographic Products List (ECPL), NSA Endorsed Data Encryption Standard (DES) Products List, Protected Services List, Evaluated Products List, and Preferred Products List.

cw. INSECURITY: See Cryptographic Insecurity, Personnel Insecurity, and Physical Insecurity.

cx. INVENTORY: (a) The physical verification of the presence of each item of COMSEC material charged to a COMSEC account. (b) A listing of each item of material charged to a COMSEC account.

cy. INVENTORY REPORT: A report of items of material that were physically sighted in accordance with inventory procedure.

cz. IRREGULARLY SUPERSEDED KEYING MATERIAL: Keying material used on an "as-needed" basis, rather than during a specified period of time.

da. ITP: See Industrial TEMPEST Program.

db. KDC: See Key Distribution Center

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

dd. KEY DISTRIBUTION CENTER (KDC): A COMSEC facility that generates and distributes key in electrical form.

de. KEY ENCRYPTION KEY: A key that is used in the encryption and decryption of other keys, for transmission (rekeying) or storage.

df. KEY LIST: A printed series of key settings for a specific cryptonet.

dg. KEY MANAGEMENT: The process by which key is generated, stored, protected, transferred, loaded, and destroyed.

dh. KEYED: The condition of containing key. In applications employing a CIK, the crypto-equipment is considered unkeyed when the CIK is removed.

di. KEYING: All keying-related changes to the crypto-equipment, such as inserting the Crypto-Ignition Key, loading electronic key, and updating or zeroizing key.

dj. KEYING MATERIAL: A type of COMSEC aid which supplies encoding means for manual and automanual cryptosystems or key for machine cryptosystems.

dk. KEYING MATERIAL SUPPORT PLAN: A detailed description of the operational needs of a proposed cryptonet including the structure, keying material specifications, and distribution plan.

dl. KMSP: See Key Management Support Plan.

dm. L6061: COMSEC Material Record Form which documents facility possession, location, and current user of a specific equipment or device.

dn. LIMITED MAINTENANCE: COMSEC maintenance performed by personnel who are not authorized to know the details of the cryptoalgorithm. Limited maintenance of a crypto-equipment normally involves disassembly, trouble isolation, and replacing faulty subassemblies (without soldering).

do. LONG TITLE: The descriptive title of an item of COMSEC material (e.g., General Purpose Encryption Device).

dp. MAINTENANCE KEY: Key intended only for off-the-air, in-shop, use. Maintenance key may not be used to protect classified or sensitive but unclassified government information.

dq. MASTER DISPOSITION RECORD: An account maintained by the contractor/vendor which itemizes serial numbers of equipments or components and shipping information where applicable.

dr. MODIFICATION: Any change to the electrical, mechanical, or software characteristics of a COMSEC equipment, assembly, or device.

ds. MANDATORY MODIFICATION: A change to a COMSEC end item which NSA requires to be completed and reported by a specified time compliance date.

dt. NEGATIVE INVENTORY: An annual pre-printed inventory sent to a COMSEC account which does not currently hold COMSEC material.

du. NET MODE: A mode of operation in which all net members have the same key.

dv. NET KEY: A key held in common by all members of a given cryptonet.

dw. NET VARIABLE: See Net Key.

dx. NO-LONE ZONE: An area, room, or space to which no person may have unaccompanied access and which, when manned, must be occupied by two or more appropriately cleared individuals.

dy. OPERATIONAL KEY: Key intended for use on-the-air for protection of operational information or for the production of secure electrical transmission of key streams.

dz. PAGE CHECK: Verification of the presence of each required page in a publication.

- ea. PDS: See Protected Distributed System.
- eb. PER CALL KEY: A key which is generated on demand and distributed electrically to secure an individual time period of communication between or among users authorized that key. Per call key is a type of Traffic Encryption Key (TEK).
- ec. PERSONNEL INSECURITY: The capture, unauthorized absence, defection or control by a hostile intelligence entity of an individual having knowledge of, or access to, classified or sensitive COMSEC information or material.
- ed. PERSONNEL SECURITY: The procedure established to ensure that all personnel who have access to sensitive or classified information have the required authority as well as appropriate clearance.
- ee. PHYSICAL SECURITY: The application of physical barriers and control procedures to prevent unauthorized access to resources, information, or material.
- ef. PLANT EQUIPMENT: Contractor property of a capital nature (including equipment, machine tools, test equipment, telecommunications security and protection equipment, furniture, vehicles, and accessory and auxiliary items).
- eg. PPL: See Preferred Products List.
- eh. PREFERRED PRODUCTS LIST: A list of commercially produced equipment which meets TEMPEST and other requirements prescribed by the National Security Agency. This list is contained in the Information Systems Security Products and Services Catalogue.
- ei. PROTECTED DISTRIBUTION SYSTEM (PDS): A wireline or fiber-optics system which includes adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of classified information.
- ej. PROTECTIVE PACKAGING: Packaging techniques for keying material which discourage penetration and/or which reveal that a penetration has occurred, or which inhibit viewing or copying of keying material prior to the time it is exposed for use.
- ek. REGULARLY SUPERSEDED KEYING MATERIAL: Keying material which is superseded on a regular established schedule.
- el. REINSTALLATION: The connection of previously installed equipment which has been moved to a new location at a facility.
- em. REMOTE REKEYING: Secure electrical distribution of a key by radio or wire/fiber optic line.
- en. RESERVE KEYING MATERIAL: Key held to satisfy unplanned needs.

eo. SELF-AUTHENTICATION: Implicit authentication of all transmissions on a secure system (such as PDS) or cryptonet to a predetermined level.

ep. SENSITIVE BUT UNCLASSIFIED INFORMATION: Information, the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests.

NOTE: National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens. The heads of Federal Government departments and agencies are responsible for determining what information is sensitive, but unclassified, and for providing systems protection for such information when transmitted, processed or stored in or on telecommunications and automated information systems.

eq. SUPERSESSON: Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

er. SYSTEM CERTIFICATION: The determination that physical and technical security (especially TEMPEST) requirements have been met.

es. TAMPERING: An unauthorized modification which alters the proper functioning of a cryptographic or automated information processing equipment or system in a manner which degrades the security it provides.

et. TEST KEY: Key intended for "on-the-air" testing of COMSEC equipment or systems.

eu. TRAFFIC ENCRYPTION KEY: Key used to encrypt plain text or superencrypt previously encrypted text and/or to decrypt cipher text.

ev. TRAINING KEY: Cryptographic key intended for use for on-the-air or off-the-air training.

ew. TRANSFER OF ACCOUNTABILITY: The process of transferring accountability for COMSEC material from the COMSEC account of the shipping organization to the COMSEC account of the receiving organization.

ex. TWO-PERSON INTEGRITY: A system of storage and handling designed to prohibit access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. NOTE: The concept of "Two-Person Integrity" (TPI) procedures differs from "No-Lone Zone" procedures in that under TPI controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction). No-Lone Zone controls are less restrictive in that the two authorized persons need only to be physically present in the common area where the material is located. Two Person Control refers to Nuclear Command and Control COMSEC material while Two-Person Integrity refers only to COMSEC keying material.

ey. UNIQUE KEY: See Key Encryption Key.

ez. UNIQUE VARIABLE: See Key Encryption Key.

fa. UNKEYED: Containing no key or containing key which has been protected from unauthorized use by removing the CIK.

fb. UPDATE: A cryptographic process which is performed to irreversibly modify the key to protect back traffic.

fc. USER: An individual who is required to use COMSEC material in the performance of his official duties and who is responsible for safeguarding that COMSEC material.

fd. VENDOR: See COMSEC Vendor.

fe. VULNERABILITY: A weakness in a telecommunications system, automated information system, or cryptographic system, or system security procedures, hardware design, internal controls, etc., which could be exploited to gain unauthorized access to classified or sensitive information.

ff. WITNESS: An appropriately cleared (if applicable) and designated individual, other than the COMSEC Custodian, who witnesses the inventory or destruction of COMSEC material.

fg. ZEROIZE: To remove or eliminate the key from a crypto-equipment or fill device.

5. Subcontracting:

a. Classified or sensitive unclassified COMSEC information shall not be disclosed to a potential subcontractor nor shall the contractor negotiate or award a subcontract requiring the disclosure of such COMSEC information without the prior written approval of the government contracting officer.

b. When awarding subcontracts which will involve the fabrication of classified or CCI COMSEC material, prime contractors shall require that subcontractors develop in-process accounting procedures and submit them to the NSA COR through the prime contractor for approval. These procedures shall be developed in accordance with the in-process accounting procedures contained in this supplement and shall be submitted to NSA for review a minimum of 90 days prior to the start of fabrication of classified or CCI material. Prime contractors shall require that subcontractors do not commence fabrication of classified or CCI materials until the applicable in-process accounting procedure has been reviewed and approved by the NSA COR. For classified subcontracts, prime contractors shall ensure that the requirements for in-process accounting are specified in the subcontractor's Contract Security Classification Specification (DD Form 254). If the subcontract involves fabrication of an item after it has transitioned to CCI and no classified information is provided to, or no classified test results are generated by the subcontractor, then the in-process requirements will be included in the appropriate contractual document.

6. TEMPEST Countermeasures.

TEMPEST countermeasures are not addressed in this supplement.

7. Foreign Bids and Proposals.

A contractor who is, or who has been, engaged in a COMSEC contract involving information on behalf of a User Agency or contractor facility shall not enter into discussion nor negotiate on matters involving COMSEC information with representatives of other nations or with representatives of foreign commercial firms, without prior written approval from the User Agency or the Deputy Director for Information Security, NSA.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION II. ACCESS REQUIREMENTS

8. Requirements for Access to Classified COMSEC Information.

a. Access to classified COMSEC information may be afforded U.S. citizens who have been granted a final security clearance by the Government and have a need-to-know as defined in paragraph 3bg, ISM. (Contractor-granted CONFIDENTIAL clearances are not valid for access to classified COMSEC information.) An interim TOP SECRET clearance, however, is valid for COMSEC but only at the SECRET level and below. Non-U.S. citizens, including immigrant aliens, are not eligible for access to classified COMSEC information.

b. When a contractor requires access to COMSEC material accountable within a CMCS, it may not be necessary to establish a COMSEC account if an existing COMSEC account is available to support the requirement. However, if it is necessary to request the establishment of a COMSEC account, the procedures in Section III of this supplement must be followed.

c. The security clearances of personnel occupying the positions of Facility Security Officer, COMSEC Custodian, and Alternate COMSEC Custodian of COMSEC accounts must be based on a Background investigation (BI) current within five years. The following procedures shall be followed for COMSEC account personnel:

(1) The contractor shall request, in writing to their Cognizant Security Office (CSO), the basis for the current personnel security clearance to include the date of the BI or latest periodic reinvestigation. The letter will identify the individuals by name, social security number and position occupied; that is, Facility Security Officer, COMSEC Custodian and Alternate COMSEC Custodian. The letter response by the CSO to this request will be retained as part of the employee's clearance record.

(2) If the individual was not the subject of a BI current within five years, a completed Personnel Security Questionnaire (Industrial) (DD Form 49) and a completed Applicant Fingerprint Card (FD Form 258) will be forwarded to the CSO for these individuals. The employee's COMSEC job title will be shown in the "to be completed by employer", block C of the DD Form 49.

d. Other employees who require access to COMSEC information which is classified SECRET or below do not require a security clearance based on a BI; however, the provisions of paragraph 8a, above, apply.

9. Requirements for Access to Controlled Cryptographic Items (CCIs). Access to CCIs will be limited to U.S. citizens whose duties require such access. Non-U.S. citizens, including immigrant aliens, may be authorized access to CCIs and other unclassified COMSEC information and material only with the prior written approval of NSA. However, within the United States, this prohibition does not apply to non-U.S. citizens who perform building maintenance or custodial duties in contractor spaces containing installed CCI equipment, provided the equipment is not keyed. When CCI equipment is keyed, persons who require access must possess a security clearance at least equal to the classification level of any key contained in the equipment.

10. Briefing and Debriefing Requirements.

a. Briefings.

(1) The contractor will ensure that all employees who have a need for access to classified COMSEC information will receive the COMSEC Briefing contained in Appendix II of this Supplement. Additionally, employees who require access to unclassified COMSEC keying material, or access to CCI equipment that involves accounting, installing, troubleshooting, maintaining, or keying operations will also receive the COMSEC briefing. Keying operations include all keying-related changes to the equipment, such as inserting Crypto Ignition Keys (CIKs), loading electronic key, and updating or zeroizing existing keys.

(2) The Facility Security Officer, the COMSEC Custodian and Alternate COMSEC Custodian will be briefed by a representative of the Government. Other employees will be briefed by the Facility Security Officer, the COMSEC Custodian, Alternate COMSEC Custodian or other appropriate individual specifically designated in writing by the Facility Security Officer.

(3) The briefing must include the pertinent parts of the contractor's Standard Practice Procedures covering local procedures for implementing the control requirements of this Supplement.

(4) Personnel who have a continuing need for access to classified COMSEC information must be given periodic rebriefings, at least annually. In addition to reminding personnel of their continuing responsibility for safeguarding COMSEC information, the rebriefing must emphasize any specific security deficiencies noted in the interval since the last briefing. The rebriefings will be conducted by those individuals designated for initial briefings.

(5) Personnel whose access is strictly limited to unclassified COMSEC keying material and/or CCI equipment as described in paragraph (1), above, only require an initial briefing.

b. Debriefings. When personnel who have been briefed terminate employment (begin a layoff or leave of absence for an indefinite period, or for a period in excess of 120 days), no longer require, or no longer meet the requirements for access as set forth in this Section, they will be given

an oral debriefing. In the case of termination of employment, the debriefing shall be accomplished prior to the employee's departure from the facility. The debriefing will, at a minimum, include the specific points set forth in paragraph 5g, ISM.

(1) The Facility Security Officer, COMSEC Custodian and Alternate COMSEC Custodian must be debriefed by a representative of the Government. When these individuals remain employed and have been debriefed, the CSO will submit a report to DISCO. The report will include the individual's name and social security number and will inform DISCO that the individual no longer occupies the position of COMSEC Custodian, Alternate COMSEC Custodian, or Facility Security Officer. An Employee Change of Status Report (DISCO Form 562) will be submitted to the CSO by the contractor.

(2) Other personnel will be debriefed by the Facility Security Officer, COMSEC Custodian, Alternate COMSEC Custodian or other appropriate individual specifically designated in writing by the Facility Security Officer.

11. Records of Briefings/Debriefings. The contractor will maintain a record of all personnel who have been briefed and debriefed. The record will indicate the name of the employee briefed, the name of the person who conducted the briefing, and the date of briefing(s) and debriefing.

a. For classified COMSEC Accounts, the employee's Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government) (SF-189A) will be used.

b. For unclassified COMSEC Accounts, the record of briefing/debriefing will be maintained for a minimum of five years from the debriefing date.

THIS PAGE INTENTIONALLY LEFT BLANK

Section III. Establishing a COMSEC Account/Subaccount

12. Requirements for a Classified COMSEC Account. In order to establish a COMSEC Account at a contractor facility, the following procedures will be adhered to:

a. Nominate individuals to fill the positions of COMSEC Custodian, and Alternate COMSEC Custodian, each of whom shall be a U.S. citizen possessing the required security clearance based on a background investigation (BI) current within five years. The number of Alternate COMSEC Custodians will be kept to an absolute minimum. No more than two Alternate COMSEC Custodians will be nominated per COMSEC account unless operational requirements necessitate otherwise. The nomination of more than two Alternates will be justified in the letter of request for appointment. The individuals nominated will meet the criteria specified in paragraph 16, below.

b. Furnish in writing to the CSO, with a copy to the COR, the name of the Facility Security Officer and the names of the individuals nominated as COMSEC Custodian and Alternate COMSEC Custodian. Their dates and levels of security clearance, their Social Security Numbers and their dates and places of birth shall also be indicated. In addition, the letter must identify the contracts to be supported by the account and copies of the appropriate DD Forms 254 "Contract Security Classification Specification" must be attached to the letter, as well as the copy furnished to the COR. Arrangements will be made with the CSO to brief the Facility Security Officer, COMSEC Custodian, and Alternate COMSEC Custodian. The letter must include the following information:

(1) Purpose of the account (i.e., Contract, MOU, MOA number) and general description of effort (i.e., production (list short titles); study (provide brief description); R&D (list short titles or part numbers, if known); support secure/protected communications (list equipment by short title, if known); other (identify).

(2) Location where the COMSEC material will be used.

(3) Verification that actual users of the material are appropriately cleared and are U.S. citizens.

(4) A list of COMSEC material to be held by the account.

c. Safeguarding capabilities for the level of classified COMSEC material to be issued to the account must be established. The CSO will assist the contractor in the establishment of safeguarding capability and advise the COR when this is accomplished.

d. The COR will confirm to the contractor, with a copy furnished to the CSO, the establishment of the account, assignment of an account number, appointment of the COMSEC Custodian and Alternate COMSEC Custodian(s) and acknowledge for the record the name of the Facility Security Officer. The account number assigned will thereafter be referred to in all correspondence or transactions relating to the COMSEC account.

e. A minimum of 90 to 120 days should be allowed to establish an account or to confirm an appointment.

f. DCS Services. DCS services for material qualified for such courier service may be obtained under two different situations. The following paragraphs provide the proper procedures under each condition.

(1) Contractual Requirement.

a. When a Government activity is negotiating a contract, the Contracting Officer (CO) must take into consideration the possible need for DCS services by the contractor. When it has been determined that DCS services will be required and the company to which the contract will be awarded has been selected, the Government CO will submit a letter, Subject: Request for DCS Services, to:

Commander
Defense Courier Service
ATTN: Operations Division
Fort George G. Meade, MD 20755-5370

The letter will contain the following information: the name and location of the contractor requiring the DCS service; name, address, and telephone number of the contractor's Government contracting official; contract number and expiration date of the contract; identification of the type of material to be received and dispatched; the size and weight of the material; the quantity of material involved; production schedules; frequency of shipment; and any special considerations.

b. Upon receipt of the aforementioned letter, HQ DCS will review the request and submit to the Government CO, a letter of approval or disapproval of the requested services. Where the request is approved, the response will indicate the condition of approval, e.g., the servicing DCS Station; whether the service will be door-to-door or at a designated point, etc.

c. The Government CO will then issue a copy of the letter of approval to the contractor with instructions to contact the assigned DCS Servicing Station to obtain the procedures for establishing a DCS account.

d. Upon completion by the contractor of all the requirements, including the proper preparation of the required DCS Forms 10, the DCS Servicing Station will then establish the contractor's DCS account.

(2) Non-contractual Requirement. In those cases where a contractor has purchased COMSEC equipment as plant equipment and will require DCS services for the movement of the associated key and other qualified material (i.e., maintenance/operating manuals, etc.), the contractor will need to solicit the assistance of one of its Government COs to initiate the letter for DCS services on his/her behalf. The contractor must provide the consenting Government CO with the appropriate information for inclusion in the letter requesting the DCS services (refer to paragraph 12f(1)(a) above). The Government CO will then follow the same procedures as outlined in paragraph 12f(1) above.

13. Requirements for an Unclassified COMSEC Account. An unclassified COMSEC account may be established to support sensitive but unclassified national security programs. The procedures for establishing an unclassified COMSEC account are as follows:

a. Nominate individuals to be the COMSEC Custodian and Alternate COMSEC Custodian. These individuals need not possess a clearance, but must be U.S. citizens and should be designated based on their trustworthiness following the selection criteria specified in paragraph 16 below.

b. Furnish in writing to the appropriate COR, the names and SSNs of the individuals nominated as COMSEC Custodian and Alternate COMSEC Custodian. The letter will also contain the facility's name, complete address and where the account will be located. The written notice must state whether access is required to unclassified operational keying material or the installation, maintenance, and operation of CCI equipment. A statement will also be included in the letter that minimum physical security standards prescribed in this Supplement for safeguarding the unclassified keying material can be met. The COR will make arrangements for the nominated individuals to receive a COMSEC briefing, and will confirm to the contractor, the establishment of the account, assignment of an account number, and appointment of the COMSEC Custodian and Alternate COMSEC Custodian. The account number assigned will thereafter be referred to in all correspondence or transactions relating to the COMSEC account.

14. Requirements for COMSEC Subaccounts. COMSEC subaccounts may be established at those contractor facilities which are divisions or subsidiaries of the primary COMSEC account. The subaccount procedure is only applicable to those facilities which require the use of CCI equipment and its associated key. Facilities requiring the use of classified COMSEC equipment must request the establishment of a primary account.

a. Use of Hand Receipts. The use of hand receipts is encouraged within limits to reduce the burden of accounting. However, the objective is security and, therefore, prudence and good judgment must be employed. In general, corporate facility users located in buildings external to that of the COMSEC account may be supported by the COMSEC Custodian through the use of hand receipts. However, the Custodian must exercise proper judgment when deciding if the users can be best supported through the establishment of a COMSEC subaccount. Some factors to be considered when deciding on the best method of support are the geographical location of the user, the quantity of equipment and associated material required, and the number of such users within any one building.

b. Classified COMSEC Subaccount. When it is determined that a classified COMSEC subaccount is required, the following procedures will be followed:

(1) The contractor establishing the COMSEC subaccount will furnish in writing to the primary COMSEC account, the name of the FSO and the names of the individuals nominated as subaccount COMSEC Custodian and Alternate(s). Their level of security clearance, the dates on which the clearances were granted, their SSNs, and dates and places of birth will also be provided. As with primary accounts, these individuals must have their clearances based on a BI current within 5 years and must be selected

following the criteria specified in paragraph 16, below. The letter will also specify the facility's CAGE code, the classified mailing and courier addresses, and the address of the DIS Cognizant Security Office (CSO) supporting that facility. The letter will also indicate whether the installation, maintenance, and operation of CCI equipment and access to classified operational keying material will be necessary. NOTE: A subaccount may not hold material to which the prime account Custodian cannot have access. Where the FSO and/or the individuals nominated as COMSEC Subaccount Custodian and Alternate(s) require an update to bring their BIs current within five years, the primary COMSEC account will initiate such a request to the DIS CSO. The primary COMSEC account shall also make arrangements for the responsible Government Agency or Department to provide a COMSEC Briefing to the COMSEC Subaccount's FSO, Custodian and Alternate(s).

(2) The primary COMSEC account will confirm to the Subaccount, with a copy furnished to the DIS CSO, the establishment of the COMSEC subaccount, the assignment of an account number, and selection of the subaccount FSO and the appointment of the Custodian and Alternate(s). The COMSEC subaccount number assigned will thereafter be referred to in all correspondence and transactions relating to the subaccount. Subaccount numbers will be derived from the primary COMSEC account number, followed by a dash and numerical designator (e.g., if the primary COMSEC account number is 870415, the first subaccount number will be 870415-1; the second 870415-2, etc.).

c. When establishing an unclassified COMSEC subaccount, the contractor shall provide the primary COMSEC account with the same information as that described in paragraph 13b, above. The individuals nominated to fill the positions of subaccount COMSEC Custodian and Alternate COMSEC Custodian(s) need not possess a clearance, but should be designated based on their trustworthiness following the selection criteria specified for primary account personnel. The FSO of the primary account or his designated representative shall arrange to provide the subaccount COMSEC Custodian and Alternate with a COMSEC Briefing. The primary account will confirm in writing to the subaccount applicant, the establishment of the subaccount, the assignment of the subaccount number, and appointment of the subaccount COMSEC Custodian and Alternate. The COMSEC subaccount number assigned will thereafter be referred to in correspondence and transactions relating to the subaccount. Unclassified subaccount numbers will be derived in the same manner as that specified in paragraph 14b(2), above.

d. Duties of the FSO (if any), COMSEC Custodian and Alternate COMSEC Custodian of COMSEC Subaccounts: Where pertinent, the duties outlined in paragraph 18, below, are applicable to subaccount personnel as well.

15. Conversion from a COMSEC Subaccount to a Primary COMSEC Account. The primary COMSEC account may submit a request for the conversion of its subaccount to a primary account only when the primary COMSEC account can no longer provide the required support on a regular basis.

a. Conversion of a Classified COMSEC Subaccount:

(1) The primary account will submit a letter of justification requesting the conversion of a subaccount to a primary account to the DIS

CSO, with a copy furnished to the COR, and the COMSEC subaccount. The letter will nominate the individuals presently performing the COMSEC subaccount custodial duties to fill the positions of the COMSEC Custodian, Alternate COMSEC Custodian(s), and identify the present COMSEC subaccount FSO. In addition, the letter will provide all the information required of a contractor when initially requesting the establishment of a primary COMSEC account (refer to paragraph 12, above).

(2) If the conversion is approved, the COR will confirm to the contractor, with a copy furnished to the CSO and the contractor's former primary account, the establishment of the primary COMSEC account, assignment of an account number, appointment of the COMSEC Custodian, Alternate COMSEC Custodian(s) and acknowledge for the record the name of the FSO. The account number assigned will thereafter be referred to in all correspondence and transactions relating to the COMSEC account.

b. Conversion of an Unclassified COMSEC Subaccount:

(1) The primary account must submit a letter of justification requesting the conversion of its subaccount to a primary account to the COR, with a copy furnished to the COMSEC subaccount. The letter will nominate the individuals presently performing as COMSEC Custodian and Alternate COMSEC Custodian(s). In addition, the letter will provide all the information required of a contractor when initially requesting the establishment of an unclassified primary COMSEC account (refer to paragraph 13, above).

(2) If the conversion is approved, the COR will confirm to the contractor, with a copy furnished to its former primary account, the establishment of the primary COMSEC account, assignment of an account number, and appointment of the COMSEC Custodian and Alternate COMSEC Custodians(s). The account number assigned will thereafter be referred to in all correspondence and transactions relating to the COMSEC account.

c. Transfer of COMSEC Material to the newly Established Primary COMSEC Account. Upon approval of the conversion and establishment of the new primary COMSEC account, the contractor's former primary COMSEC Account Custodian will prepare a "paperwork" transfer of all COMSEC material charged to his account but actually held by his former subaccount. An original and one copy of the SF-153 will be provided to the new primary COMSEC account with an advance copy to the COR. Upon receipt of the SF-153, the "receiving" custodian will sign the transfer report, assign it an incoming transaction number (using his new account number sequence), and provide a copy to his former primary COMSEC account and to the COR, retaining one for his files. All accounting files relating to the former subaccount must be retained by both custodians for a period of three years.

16. Selection of COMSEC Custodian and Alternate Custodian. Because of the sensitivity of COMSEC material and the rigid controls required, the COMSEC Custodian and Alternate Custodian must possess exemplary qualities of loyalty, reliability and honesty. This criteria must be followed when selecting COMSEC subaccount personnel as well. Each contractor is, therefore, obligated to carefully screen personnel to ensure that the individuals selected:

a. Are responsible individuals qualified to assume the duties and responsibilities of a COMSEC Custodian.

b. Are in a position or level of authority which will permit them to exercise proper jurisdiction in fulfilling their responsibilities and, in cleared facilities, be accountable to the Facility Security Officer regarding their COMSEC duties.

c. Have not been previously relieved of COMSEC Custodian duties for reasons of negligence or non-performance of duties.

d. Are in a position which will permit maximum tenure as a COMSEC Custodian in order to reduce the possibility of frequent replacement.

e. Will not be assigned duties which will interfere with their duties as COMSEC Custodian and Alternate Custodian.

f. Are actually performing the custodial functions on a day-to-day basis. The COMSEC Custodian position will not be assumed solely for the purpose of maintaining administrative or management control of the account functions.

17. Indoctrination and Guidance for COMSEC Custodians. Upon appointment of each new Custodian and Alternate, the sponsoring organization must ensure that adequate training is provided. Formal training courses are, however, required for custodial appointees of NSA-contractor COMSEC accounts. Requests for training will be directed to the following address:

Director
National Security Agency
Operation, Building No. 3
ATTN: Y13
Fort George G. Meade, MD 20755-6000

Indoctrination and guidance for COMSEC subaccount custodial appointees will be the responsibility of the primary COMSEC account.

18. Duties of the COMSEC Custodian, Alternate COMSEC Custodian and Facility Security Officer.

a. The COMSEC Custodian. The COMSEC Custodian will be responsible for the receipt, custody, issue, safeguarding, accounting and, when necessary, destruction of COMSEC material. The COMSEC Custodian is further responsible for the maintenance of up-to-date records and the submission of all required accounting reports. The COMSEC Custodian will be thoroughly familiar with the procedures for handling COMSEC material outlined in this Supplement. In fulfilling his/her responsibilities, the COMSEC Custodian will perform the following duties:

(1) Protect COMSEC material charged to the account and limit access to such material to individuals who have a valid need-to-know and, if the material is classified, are properly cleared. Prior to having access to COMSEC material charged to the account, contractor personnel must be given the COMSEC briefing in accordance with requirements of the Section II.

(2) Keep informed of any proposals or any new contracts to be serviced by the COMSEC account and modifications to any existing contracts in matters pertaining to accountable COMSEC material.

(3) Where applicable, retain a copy of the DD Form 254, "Contract Security Classification Specification" as part of the custodial records and ensure compliance with the specification.

(4) Receive, receipt for, and ensure the safeguarding and accounting for all COMSEC material issued to the COMSEC account, or produced within the facility.

(5) Maintain COMSEC accounting and related records as outlined in Section VI.

(6) Conduct an inventory semiannually, and upon appointment of a new COMSEC Custodian, by physically sighting all COMSEC material charged to the account, and reconcile this inventory with the COR.

(7) Perform a reconciliation of in-process accounting records, when applicable, upon appointment of a new COMSEC Custodian; and when directed by the COR, Contracting Officer, or Facility Security Officer.

(8) Perform routine destruction of COMSEC material when required, or effect other disposition of material as directed by the COR or Contracting Officer.

(9) Submit transfer, inventory, destruction, and possession reports when required.

(10) Ensure the prompt, accurate entry of all amendments to COMSEC publications held by the account.

(11) Ensure that required page checks are accomplished on all keying material (as specified in paragraph 51) and on all publications when they are received, returned from hand receipt, transferred, destroyed, when a change of Custodian occurs, and when posting amendments which include replacement pages to ensure completeness of each publication. At an activity where the size of the COMSEC account is so large as to prevent the COMSEC Custodian from personally checking security packages and markings, performing required page checks and posting amendments, such actions may be performed by other individuals cleared and authorized, provided these individuals are properly instructed by the COMSEC Custodian.

(12) Be aware at all times of the location of every item of accountable COMSEC material held by the account and the general purpose for which it is being used.

(13) Establish procedures to ensure strict control of each item of keying material whenever the material is turned over from one shift to another or from one individual to another.

(14) Ensure that appropriate COMSEC material is readily available to authorized individuals whose duties require its use. If the material is classified, verify that the individuals are cleared to the level of the material. Issue material to users by means of a hand receipt as provided for in Section II and advise recipients of their responsibility for safeguarding the material until it is returned to the Custodian.

(15) Ensure that all COMSEC material shipped outside the contractor facility is packaged and shipped in compliance with the provisions of Section VI.

(16) When applicable, make the necessary shipping arrangements with the Defense Courier Service (DCS).

(17) Report immediately to the Facility Security Officer any known or suspected incidents of a COMSEC insecurity. This report will be submitted in accordance with the procedures outlined in Section XVI.

(18) Prepare for the safeguarding of COMSEC material during emergency situations in accordance with the provisions of Section XV.

(19) Ensure that the COR is provided up-to-date copies of all DD Forms 254 on contracts which involve COMSEC account material.

(20) Verify the identification, clearance, and need-to-know of any individual requesting access to the records and/or material associated with the COMSEC account.

b. The Alternate COMSEC Custodian. The purpose of an Alternate COMSEC Custodian is to assist the COMSEC Custodian and provide continuity of operations in his/her absence. The Alternate COMSEC Custodian is responsible for:

(1) Keeping aware of the day-to-day activity of the COMSEC account in order that he/she may assume the duties of the COMSEC Custodian, whenever necessary, without undue interruption of operations.

(2) Performing those duties outlined in paragraph 18a, above, during the temporary absence of the COMSEC Custodian.

(3) Ensuring that semiannual inventories are only signed by the Alternate COMSEC Custodian in the absence of the COMSEC Custodian.

(4) In the event of the sudden permanent departure or unauthorized absence of the COMSEC Custodian, performing those duties listed in paragraph 18a, above, until the appointment of a new COMSEC Custodian.

c. Facility Security Officer. The Facility Security Officer is responsible for:

(1) Preparing a supplement to the facility SPP to cover COMSEC procedures and ensuring implementation of procedures prescribed for safeguarding and control of COMSEC material and information, including in-process accounting procedures.

(2) Providing, as a minimum, staff supervision and guidance to the COMSEC Custodian and Alternate COMSEC Custodian.

(3) Being aware of new contracts which may require the application of in-process COMSEC accounting procedures to material being produced and ensuring that the COMSEC Custodian is provided copies of all DD Forms 254 related to COMSEC contracts.

(4) Maintaining a record of safe combinations, limiting access to those individuals who are appropriately cleared and have the need-to-know, and ensuring that the combination changes are accomplished as prescribed in this Supplement.

(5) Establishing procedures to limit access to operational keying material to persons who are appropriately cleared and have the need-to-know.

(6) Notifying the CSO and the COR of any change in the COMSEC Custodian, Alternate, or Facility Security Officer.

(7) Making the COR, Contracting Officer, CSO and all known suppliers of accountable COMSEC material aware of any abnormal situation at the contractor facility (e.g., strikes, riots, facility shutdown, etc.) which may adversely affect the normal procedures for receiving, storing, shipping or other aspects of the security of COMSEC material.

(8) Reporting immediately to the COR and the CSO any incident that may have subjected to compromise any COMSEC material furnished by the government; or generated or acquired by the contractor.

(9) Where applicable, ensuring that in-process accounting procedures are prepared and are being followed.

(10) Where applicable, forwarding copies of the annual clearance certifications received from the COR to the COMSEC subaccount(s) FSO(s).

19. Temporary Absence of the COMSEC Custodian. When the COMSEC Custodian is to be absent for a period not to exceed 60 days, the Alternate COMSEC Custodian will assume the responsibilities and duties of the COMSEC Custodian. An absence in excess of 60 days will be treated as a permanent absence, and a new COMSEC Custodian must be nominated.

20. Return of the COMSEC Custodian from Temporary Absence. Upon return of a COMSEC Custodian from a temporary absence, he or she will be informed of all changes made to the COMSEC account during his or her absence. If COMSEC material was receipted for on a transfer report by the Alternate COMSEC Custodian during the absence, the COMSEC Custodian will inventory the COMSEC material and will sign and date the front side of the COMSEC account's copy of the report, accompanied by the remark "received from Alternate COMSEC Custodian" thus relieving the Alternate COMSEC Custodian of accountability for the material.

21. Change of COMSEC Custodian. When it becomes necessary to terminate the COMSEC Custodian's appointment, the contractor must select, nominate, and forward for confirmation to the Cognizant Security Office (with a copy furnished to the COR), the name of the new COMSEC Custodian as specified by the procedures in paragraph 12 of this Supplement.

a. Upon receipt of the confirmation letter from the COR, the newly appointed COMSEC Custodian and predecessor will:

(1) Conduct a physical (sight) inventory of all COMSEC material held by the COMSEC account and perform a reconciliation of in-process accounting records, if applicable. (The change of COMSEC Custodian will be effective the date the inventory is signed).

(2) Prepare an SF-153 listing all COMSEC material to be transferred. If classified operational key is included in the transfer, the SF-153 will be stamped "CONFIDENTIAL." Identify the report as a "change of COMSEC Custodian" and check both "received" and "inventoried" in block 14. The report will be addressed from the contractor (block 2) to the COR (block 3). The new COMSEC Custodian will sign block 15 and the departing Custodian will sign as the witness in block 17. The signed original copy will be forwarded to the COR and a signed duplicate copy will be retained in the COMSEC account's file. In the case of an account holding over 50 line items, a COMSEC Custodian may request a preprinted inventory from the COR, and this request should be included in the letter of nomination.

b. Under normal circumstances, the new COMSEC Custodian will have received his or her letter of confirmation before action is initiated to transfer the COMSEC account. However, if the confirmation is delayed and the departure of his or her predecessor is imminent, the transfer will be accomplished prior to the receipt of the confirmation letter.

c. After receipting for COMSEC material charged to the COMSEC account, the new COMSEC Custodian will assume full responsibility for administering the account.

d. The former COMSEC Custodian will be relieved of responsibility for only that COMSEC material included in the transfer/inventory report. He or she is not relieved of responsibility for COMSEC material which is involved in any unresolved discrepancy until a clear COMSEC Inventory Reconciliation Report has been received from the COR.

e. A change in COMSEC Custodian should normally be scheduled at least 40 days in advance of the departure of the COMSEC Custodian to allow for the receipt of a clear COMSEC Inventory Reconciliation Report before the former COMSEC Custodian departs. However, the former COMSEC Custodian may depart prior to the return of the COMSEC Inventory Reconciliation Report provided no discrepancies or irregularities were evident at the time the inventory and transfer were made. Responsibility for resolving discrepancies discovered after a COMSEC Custodian has departed rests with the contractor.

22. Change of Alternate COMSEC Custodian. When a change in Alternate COMSEC Custodian is necessary, the contractor will select, nominate, and forward for confirmation to the CSO (with a copy furnished to the COR), the name of the new Alternate as specified by the procedures in paragraph 12. A Change of Alternate COMSEC Custodian should be made prior to the departure of the present Alternate COMSEC Custodian, if possible.

23. Change of Facility Security Officer. When it is necessary to make a change in the Facility Security Officer, notification will be sent to the CSO, with a copy provided to the COR. The same information specified in paragraph 12, above, is required.

24. Sudden, Indefinite, or Permanent Departure of the COMSEC Custodian.

a. Under emergency circumstances such as the sudden, indefinite, or permanent departure of the COMSEC Custodian, the contractor will nominate a new COMSEC Custodian (preferably the Alternate COMSEC Custodian) in compliance with the provisions of paragraph 12. The new COMSEC Custodian and an appropriately cleared witness will immediately conduct a complete physical inventory of all COMSEC material held by the COMSEC account and perform a reconciliation of in-process accounting records, if applicable. In the case of unauthorized absence of the COMSEC Custodian, the contractor will immediately report the circumstances to the COR and if the COMSEC account is classified, the CSO.

b. Upon the completion of the inventory, an SF-153 will be prepared and identified as a "possession report." The possession report will be annotated with the remark "Sudden, indefinite, or permanent departure of the COMSEC Custodian" or "Unauthorized absence of the COMSEC Custodian," as appropriate. The new COMSEC Custodian will sign block 15 and the witness will sign block 17. The signed original copy of the report will be forwarded to the COR and a signed duplicate copy will be retained in the COMSEC account's file.

25. Sudden, Indefinite, or Permanent Departure of the Alternate COMSEC Custodian or Facility Security Officer. The COR and CSO should be notified as soon as possible in the event that an Alternate COMSEC Custodian or Facility Security Officer must be replaced due to a sudden, indefinite, or permanent departure. The unauthorized absence of either must be immediately reported to the COR and the CSO.

26. Requirements for Closing a Primary COMSEC Account. The COMSEC account will be closed when all COMSEC material has been properly disposed of, no discrepancies exist, and the COR has determined that the COMSEC account is no longer required. Upon determination that a COMSEC account should be closed, the contractor must submit to the CSO, with a copy furnished to the COR, a formal written request for the disestablishment of the COMSEC account. If the COMSEC account was unclassified, the contractor will submit this information directly to the COR. The COR will notify the contractor in writing that the COMSEC account has been closed and the appointments of the COMSEC Custodian and Alternate(s) have been terminated. For classified COMSEC accounts, the COR will provide a copy of the letter closing the COMSEC account to the CSO. COMSEC accounting records and files will be disposed of in accordance with paragraph 45.

27. Requirements for Closing COMSEC Subaccounts. If a primary account determines there is no longer a requirement for a COMSEC subaccount and all COMSEC material has been properly disposed of and no discrepancies exist, the primary COMSEC account will notify the subaccount in writing that the COMSEC Custodian and Alternate(s) are relieved of their duties. The primary COMSEC account will provide the DIS CSO (if the account contained classified material) a copy of the letter closing the subaccount.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION IV. COMSEC MATERIAL

28. Identification.

a. Short Titles. For accounting purposes, COMSEC material may be identified by short titles derived from the Telecommunications Security Nomenclature Systems (TSEC); or bear designators derived from the Joint Electronics Type Designation System (JETDS); or a federal part number; or by short titles assigned by a Military Department. In many cases, the new CCI category may not be assigned any short title, but may instead bear the manufacturer's commercial designator. These equipments will, however, be marked "Controlled Cryptographic Item" or "CCI" and will bear a Government Serial Number (GSN) label. The GSN has been developed for accounting purposes and will be the designator by which the COMSEC Custodian will identify and control the CCI. The GSN is composed of three fields; for example, the label may read "GSN: PES-B4 192." The first field "PES" identifies the manufacturer; the second field "B4" identifies the type of product; and the third field "192" identifies the serial number of the unit. For purposes of the SF-153 (as per the above example), the designator "PES-B4" will be listed in the short title block and the "192" in the accounting number block. (NOTE: The GSN for STU-III Low Cost Terminals will vary from the above format.)

b. Accounting Numbers. Most COMSEC material is assigned an accounting (register) number at the point of its origin to facilitate accounting. However, COMSEC material may be received which does not bear an accounting number or for which accounting for by number is impractical and therefore not required. (An example of this type of material is a TSEC-nomenclatured printed circuit board which may bear a manufacturer's serial number, but which is only accounted for by quantity and will be listed on accounting reports as an "N/N" (no number) item in the "numbers column" of the COMSEC accounting reports.)

c. Edition. In addition to being identified by short title or designator and accounting number, if applicable, COMSEC material may be identified by alphabetic or numeric edition. COMSEC material is superseded when new COMSEC material becomes effective (effective edition). Note: The current effective edition of classified operational keying material is considered CONFIDENTIAL. This information should not be disclosed over an unsecure mode of communication, e.g. unsecure telephone, teletype, facsimile, etc.

d. CRYPTO Marking. COMSEC keying material which is used to protect or authenticate telecommunications carrying national security and government sensitive information is identified by the bold marking CRYPTO. The purpose of this marking is to make this material readily identifiable from other material so that its dissemination can be restricted to personnel whose duties require access and, if the material is classified, who have been granted a final security clearance equal to or higher than the classification of the keying material involved. Specific instructions on the handling of keying material are contained in this Supplement and the DD Forms 254 for applicable contract.

e. Subdivisions of Equipment. Operational COMSEC equipments are identified and accounted for by one short title rather than by individual components and/or subassemblies. Classified subassemblies, elements, and microcircuits when not incorporated in an equipment will, however, be accounted for by type and quantity.

29. Accounting Legend Codes.

a. For the purpose of accounting, all COMSEC material is identified by one of the following accounting legend codes:

(1) ALC-1. Continuous accountability by accounting number within the COMSEC Material Control System.

(2) ALC-2. Continuous accountability by quantity within the COMSEC Material Control System.

(3) ALC-3. Initial receipt required; locally accountable by accounting number thereafter. Local accounting records must be maintained for a minimum of 90 days after supersession.

(4) ALC-4. Initial receipt required; may subsequently be controlled in accordance with service or agency directives.

b. The accounting legend code will be assigned by the originating Government department or agency and will represent the minimum accounting standard to be applied. For NSA contracts, the accounting legend code for the material produced will be stipulated in the contract.

c. The accounting legend code will appear on all accounting reports but not necessarily on the material. No holder will apply accounting procedures less restrictive than those specified by the accounting legend code assigned unless specifically authorized by the COR.

d. Material such as correspondence, logs, reports, etc., are excluded from the COMSEC Material Control System.

SECTION V - OWNERSHIP AND ACQUISITION OF CCI

30. General. This section describes the criteria for CCI ownership and the requirement and procedures for acquiring CCI equipment directly from NSA authorized vendors in support of U.S. Government contractor's secure communications requirements. It's recognized that there may be a distinction between the owner and the actual user of the CCI equipment. The Information Systems Security Products and Services Catalogue contains a list of CCI equipment available for direct acquisition.

31. Ownership Categories. The currently available Government-Furnished Equipment (GFE) mechanism does not alone provide flexibility to satisfy the requirement to provide secure communications for U.S. Government contractors as directed in the provisions of NACSI 6002. This necessitated that new options become available for acquiring and owning CCI equipment. The ownership categories are described below:

a. Government-owned:

(1) CCI equipment purchased by a U.S. Department or Agency and furnished to a contractor as GFE as defined in Federal Acquisition Regulation (FAR) 45.101(a).

(2) CCI equipment purchased by a contractor upon authorization from a Government Contracting Officer and charged to a contract(s) which requires the securing of classified information and/or securing or protecting unclassified but sensitive Government information. This equipment is designated as Contractor-Acquired Property (CAP), as defined in FAR 45.101(a).

b. Contractor-owned: CCI equipment purchased by a contractor as plant equipment, as defined in FAR 45.101(a).

32. Criteria for CCI Equipment Ownership Eligibility. Authorization to acquire CCI equipment and associated materials as plant equipment is an administrative determination by NSA/DDI that the contractor is eligible, from a security viewpoint, to own CCI equipment. CCI equipment ownership is limited, as follows:

a. Any U.S. Government Department or Agency may purchase and own CCI equipment.

b. U.S. Government contractors may purchase and own CCI equipment, as follows:

(1) Authorization to acquire CCI equipment as plant equipment will not be granted to contractor activities located outside the U.S., Puerto Rico, or a U.S. possession or trust territory. Eligible U.S. Government contractors may purchase CCI equipment and associated materials within the United States for use by divisions or operations centers located outside of the U.S. only in accordance with applicable U.S. export regulations.

(2) Authorization to acquire CCI equipment as plant equipment may be granted only to contractors organized and existing under the laws of the U.S. or Puerto Rico. Contractors organized and existing under the laws of a U.S. possession or trust territory may not be authorized to acquire CCI equipment as plant equipment, except with the prior approval of the NSA/DDI based on a case-by-case review in accordance with applicable guidelines.

(3) Contractors which are determined to be under foreign ownership, control or influence (FOCI) are not authorized to acquire CCI equipment as plant equipment except when there has been a specific determination by the Director, NSA, that authorization of the contractor to purchase CCI equipment as a capital asset will serve the national interests of the U.S.

33. Requirements and Procedures for Contractor Acquisition of CCI Equipment.

a. When the CCI equipment is to be purchased as Contractor-Acquired Property, the following requirements and procedures will be followed:

(1) Each existing contract or future contract which requires the transmission of classified or sensitive Government information must contain a specific statement of any requirement for securing or protecting telecommunications.

(2) The contractor and the appropriate CO(s) shall negotiate agreements applicable to the treatment of the costs under existing or new contract(s) requiring the securing or protection of telecommunications. If it is determined that the costs will not be directly charged to the contract, then the procedures for Contractor-Owned Property apply (see subparagraph b, below).

(3) The contractor will initiate a letter to NSA, ATTN: Y131, requesting eligibility to directly procure the desired CCI equipment. The letter will indicate the contract(s) to which the equipment will be charged, the type of equipment, and the location(s) where the equipment will be installed. If the requesting contractor is cleared, the letter will contain the requesting facility's CAGE code and the full name, address, and CAGE code of its corporate headquarters or parent company, if any. If a COMSEC account is in place at the facility, or if an existing COMSEC account is available to support the requirement, the letter will include that information. If not, a statement must be made that the facility will initiate a request for the establishment of a COMSEC account (see Section III for the proper procedures). The contractor will arrange for and submit along with the letter to NSA, a properly completed Contracting Officers Authorization to Purchase form (see Appendix IV to this Supplement).

(4) Upon receipt of the aforementioned letter, NSA will determine the requester's eligibility to procure the CCI equipment and will notify the contractor in writing. The contractor will also be required to furnish to NSA a properly executed CCI Control Agreement, a copy of which is contained in Appendix III of this Supplement.

b. When the CCI equipment is to be purchased as plant equipment/Contractor-Owned Property, the following requirements and procedures must be followed:

(1) The contractor will initiate a letter to NSA, ATTN: Y131, requesting eligibility to procure as plant equipment the desired CCI equipment. The letter must confirm that the facility desiring to own the CCI equipment is performing or will be performing under a U.S. Government contract at the time of the CCI equipment delivery. ^{1/} The letter must indicate the type of equipment and the locations where the equipment(s) will be installed. The letter will also contain the requesting facility's CAGE code, if any, and, when applicable, the full name, address, and CAGE code of its corporate headquarters or parent company. If a COMSEC account is in place at the facility, or if an existing COMSEC account is available to support the requirement, the letter will include that information. If not, a statement must be made that the facility will initiate a request for the establishment of a COMSEC account (see Section III for proper procedures).

(2) Upon receipt of the aforementioned letter, NSA will determine the requester's eligibility to procure the CCI equipment and will notify the contractor in writing. The contractor will also be requested to furnish to NSA a properly executed CCI Control Agreement, a copy of which is contained in Appendix III to this supplement.

34. Contractor Certification to the Authorized Vendor. After the contractor's eligibility has been determined by NSA and the requirements outlined above have been fulfilled, the contractor will certify his eligibility to the Vendor and provide the Vendor with his COMSEC account number, shipping address, and the address of the appropriate COR.

35. Authorized Vendor Responsibilities. Prior to shipment, the Vendor must confirm with NSA the eligibility of the contractor to receive CCI equipment, and verify the COMSEC account number with the appropriate COR. If shipment is direct to a subaccount, the account number and shipping address must be verified with the primary COMSEC account. If the shipment is to a Military Logistics System account, verification must be obtained from the cognizant Military Accounting Headquarters. This step must be completed for each and every sale.

^{1/} In many instances, there is no current contract between a corporate headquarters office and the U.S. Government; however, it is often necessary for the corporate office to be in secure communication with its subordinate offices which are performing under a U.S. Government contract in order to discuss the program under contract. The Government, therefore, encourages corporate offices to own CCI equipment for the purpose of securely communicating with their subordinate offices, whether to discuss sensitive government programs or company proprietary information, providing that: the corporation is not under FOCI; there is a current U.S. Government contract in place at one of the subordinate offices; and, if the keying material to be employed is classified, that the corporate headquarters has been granted a facility clearance commensurate with the level of the key.

THIS PAGE INTENTIONALLY LEFT BLANK

Section VI. THE COMSEC MATERIAL CONTROL SYSTEM

36. General. COMSEC material control within the U.S. Government and industrial facilities is based on a system of centralized accounting and decentralized custody and protection. Computer applications are employed to minimize manual bookkeeping and to provide timely and accurate data essential to continuous and effective control of COMSEC material entrusted to or produced by U.S. industry for the government.

37. Responsibilities. This section encompasses responsibilities performed by the DIS, the CORs, contractor COMSEC Custodians, and users of COMSEC material. The responsibilities listed below are representative of the respective roles of DIS, the COR, and the U.S. Government contractor in support of the COMSEC Material Control System.

a. The Defense Investigative Service has been directed by DoD to inspect contractor procedures, methods, and facilities associated with COMSEC material control. DIS responsibilities include the following:

(1) Establishing the facility security clearance required for classified COMSEC accounts.

(2) Ensuring the proper investigatory basis and clearance exist for the Facility Security Officer, COMSEC Custodian and Alternate COMSEC Custodian.

(3) Providing to the COR, on a timely basis, verification of the facility's clearance, its document and hardware storage capability, appropriate physical location and classified mailing address, and, when requested, where the COMSEC account will receive classified key, verification that adequate supplemental controls are in place.

(4) Providing COMSEC briefings/debriefings where required.

(5) Ensuring that document and equipment marking requirements are followed.

(6) Approving and periodically inspecting area controls, storage and destruction processes and procedures.

(7) Ensuring proper transportation procedures are followed.

(8) Reviewing and ensuring reporting requirements are followed.

(9) Ensuring the provisions of NACSI 6002 are properly applied by the User Agency.

(10) Verifying that CCI equipment, assemblies, and components within cleared contractor facilities are being properly controlled in accordance with the CSISM.

b. COR responsibilities include the following:

- (1) Establishing and closing COMSEC accounts.
- (2) Maintaining a record of all COMSEC accounts, to include clearance verification, when applicable, of all COMSEC Custodians, Alternate COMSEC Custodians, and Facility Security Officers.
- (3) Formally appointing the COMSEC Custodian and Alternate COMSEC Custodian, and maintaining a record of the Facility Security Officer designated by each contractor.
- (4) Maintaining master records of all COMSEC material held by contractors under its auspices.
- (5) Verifying COMSEC account holdings.
- (6) Auditing COMSEC accounts, in-process accounting procedures, and, where applicable, inspecting secure telecommunication facilities.
- (7) Providing COMSEC training and guidance, when required.
- (8) Approving in-process accounting systems for prime and subcontractors to ensure compliance with procedures prescribed herein.

c. Contractors.

- (1) Including procedures in, or preparing a supplement to, the Standard Practice Procedures (SPP), required by paragraph 5s, ISM, to cover COMSEC requirements.
- (2) Providing proper facilities for the storage and safeguarding of COMSEC material.
- (3) Nominating a COMSEC Custodian and Alternate COMSEC Custodian, and designating the Facility Security Officer.
- (4) Ensuring that all new COMSEC Custodians and Alternate COMSEC Custodian receive adequate training.
- (5) Ensuring that the COMSEC Custodian, Alternate COMSEC Custodian, Facility Security Officer and other persons involved in the handling and control of COMSEC material safeguard the material in accordance with this Supplement and applicable contract or Memorandum of Agreement requirements.

38. COMSEC Material Control System Forms, Files and Reports.

a. Forms. The forms used in the COMSEC Material Control System are limited to the multipurpose Standard Form 153 (COMSEC Material Report); Form A1721 (COMSEC Material Hand Receipt); and the L6061, (COMSEC Material Record Card). Where NSA is the COR, these forms may be ordered from DIRNSA, ATTN: L1112 (contact the NSA COR on (301) 688-8110 for a copy of the format to be utilized when ordering the forms from L1112).

b. Accounting Records. Accounting reports are prepared on an SF-153 and are used to record the transfer, possession, inventory, and destruction of accountable COMSEC material. Accounting reports may be prepared either

manually or by data processing equipment. The required copies and distribution of accounting reports are covered in the appropriate paragraphs which outline the detailed preparation of particular reports. The various reports and a brief description of their use are as follows:

(1) Transfer Report: Used to record COMSEC material transferred from one COMSEC account to another. (See figures 2 and 3.)

(2) Destruction Report: Used to report the physical destruction or other authorized expenditure of COMSEC material. (See figure 4.)

(3) Inventory Report: Used to report the physical (sight) inventory of COMSEC material. (See figures 5 and 6.)

(4) Possession Report: Used to report the possession of COMSEC material. Specific circumstances requiring the accomplishment of possession reports are prescribed in paragraph 41. (See figure 7.)

c. Hand Receipt. A hand receipt is used to record the acceptance of and responsibility for COMSEC material issued to a user by a COMSEC Custodian. (See figures 9, 10 and 11.)

d. Files. Each COMSEC Custodian will establish and maintain COMSEC accounting and related files as indicated in (1) and (2) below.

(1) Accounting Files:

(a) Incoming transfer reports, possession reports, and change-of-custodian transfer reports.

(b) Destruction and outgoing transfer reports.

(c) Inventory reports.

(d) Hand receipts.

(e) COMSEC Register File (L6061) or a comparable system approved by the COR.

(f) In-process accounting records (if applicable).

(g) Master Disposition Record of COMSEC Material (if applicable).

(2) Related Files:

(a) Courier, mail, and package receipts.

(b) Correspondence to include such records as COMSEC Custodian and Alternate COMSEC Custodian appointment confirmation letters, messages, and other documentation related to COMSEC accounting.

39. Preparation of COMSEC Register File and COMSEC Accounting Reports.

a. COMSEC Register. All COMSEC material held by an account will be controlled internally, using a COMSEC Register File. This register will consist of an active section and an inactive section, both of which shall be maintained in alphanumeric order. Normally, this file will consist of L6061s; however, where the COMSEC account holdings are very large, consideration to maintaining this information on a personal mini-computer controlled by the COMSEC Custodian may be warranted and is acceptable, subject to prior COR approval. However, care must be taken to control the data base as much as possible since unauthorized persons could alter/erase information without the immediate knowledge of the COMSEC Custodian. Automated Register Files containing information on classified operational keying material must be approved by the CSO prior to use.

(1) The active Register File will contain a record for each accountable item currently held in the account and will contain the following information:

- (a) Short title, edition, quantity and accounting number (if any).
- (b) Classification and Accounting Legend Code (ALC).
- (c) Date of receipt, the COMSEC account from which it was received, and incoming transaction number.
- (d) The applicable Contract or MOU/MOA Number.
- (e) Hand receipt information (reverse side).

(2) The inactive section of the register file will contain a record for each item which has been removed from the account and will contain the specific disposition date for the item, as follows:

- (a) The type of disposition (transfer, destruction, etc.) and the date of the action.
- (b) The outgoing transaction number.
- (c) If transferred, the receiving COMSEC account number.

(3) Special attention should be given to maintaining this Register File in a current and accurate status as it is a convenient reference and important tool for maintaining strict control over all COMSEC material in the account.

b. Preparation of COMSEC Accounting Reports. Proper preparation, accuracy, and timely submission of COMSEC accounting reports are essential for the effective control of COMSEC material.

(1) Each report must include the official titles and address of the activity involved; account number, transaction number, and contract or MOU/MOA; DD 250 partial shipment numbers, when applicable; date of report (entered: year, month, day, e.g. 870107 indicates 07 January 1987); typed or stamped names of individuals signing the report; and signatures in ink.

(2) All short titles will be listed in alphanumeric order, with the "TSEC" designator omitted. For equipment controlled by Government Serial Number, the "GSN" prefix will also be omitted.

(3) All line item entries on a report must be single spaced. The last line item will be followed by the remark "NOTHING FOLLOWS" in capital letters on the next line.

(4) For items having accounting numbers running consecutively, the inclusive accounting numbers will be entered as a single line entry, e.g., 1-10 in block 11.

(5) Enter "N/N" in block 11 for those items not having an accounting number or for which accounting by number is not required.

(6) Ensure that the consecutive accounting numbers agree with the entries made in the "quantity" column.

(7) Include any clarifying remarks deemed appropriate for the receiving COMSEC Custodian or the COR in Block 13 or below the "NOTHING FOLLOWS" line. Required remarks are contained in the instructions for the specific report being prepared, as well as in the figures in Appendix V to this supplement.

(8) Initial all deletions or corrections in ink.

(9) Each accounting report (i.e., incoming and outgoing transfers, possession, inventory, and destruction reports) will be assigned a transaction number. Transaction numbers will be derived by the addition of a sequential set of numbers commencing with 001 each calendar year, to the last three digits of the account number (e.g., the first yearly transaction number of COMSEC Account 870342 would be 342001).

(10) Review all reports for completeness and accuracy.

(11) Ensure the legibility of each copy of each report.

NOTE: Transaction numbers are not assigned to hand receipts, INFOSEC Procedural and Material Control Bulletins, or reconciliation statements.

40. Hand Receipts.

a. When COMSEC material is to be issued by the COMSEC Custodian to a user, it will be issued on a hand receipt. A hand receipt may be executed on an SF-153 (see Figure 9), the reverse side of Form L6061 (see Figure 11) or Form A1721 (see Figure 10). Transaction numbers described in Paragraph 39b, above, will not be assigned to hand receipts. Prior to effecting such issue, the COMSEC Custodian will verify that the proposed recipient:

(1) Has a need to know, and if the material is classified, possesses the required clearance and has received a COMSEC briefing.

(2) Will be the actual user of the material (clerical or other personnel who are not the user will not sign hand receipts).

(3) Knows the physical security measures necessary to protect the material, and the possible consequences of compromise.

(4) Has the necessary physical secure means for storage and use commensurate with the classification of the item. The file safe should be located in the user's immediate work area.

(5) Is fully aware that pages are not to be removed from basic documents, nor is reproduction of a document in whole or in part authorized.

b. COMSEC material received on a hand receipt will never be reissued by a user. If the material is needed by another individual outside the immediate office of the recipient, it must be returned to the COMSEC Custodian for reissue.

c. The hand receipt user must be made aware that any possible compromise, access by unauthorized persons, or violations of security regulations affecting the material (e.g., user cannot locate or suspects material was borrowed, or container securing the material was left open while unattended) must be immediately reported to the COMSEC Custodian.

d. Users who need to transport COMSEC material on hand receipt outside their facilities for valid contract-related activities must have prior concurrence of the COMSEC Custodian. COMSEC material to be transferred outside the facility should be handled in accordance with the applicable portions of this Section.

e. A user will be relieved of responsibility for material received on a hand receipt when the material has been returned to the COMSEC Custodian and the original copy of the hand receipt (SF-153) is given to the user, or by the Custodian's initialing and dating the reverse side of Form L6061 or Form A1721, as appropriate.

41. Possession Reports.

a. Possession reports will be prepared under the following circumstances:

(1) When COMSEC material is received without accompanying transfer reports.

(2) When COMSEC material fabricated by a contractor reaches a final state and is accepted by the Government, and will remain in the contractor's facility over 30 days. Material which has been accepted by the Government but does not remain in the plant for over 30 days will not require a possession report but accountability becomes the responsibility of the COMSEC Custodian.

(3) When reporting conversion of COMSEC material (see Paragraph 42).

(4) When COMSEC material was previously lost or removed from accountability but subsequently recovered.

(5) When a new COMSEC Custodian is appointed because of the sudden permanent departure or unauthorized absence of the COMSEC Custodian. In those cases where the holdings of the COMSEC account are large, a preprinted inventory may be requested from the COR and utilized for this purpose.

(6) When a TSEC nomenclatured document which requires control in the CMCS is reproduced by a contractor.

b. To submit a possession report, the COMSEC Custodian will prepare an SF-153 (see Figure 7) and will enter appropriate remarks below the "NOTHING FOLLOWS" line, citing the reason for submission of the report. The signed original copy of the possession report will be forwarded to the COR and a signed duplicate copy will be retained for file. In those instances where COMSEC material is received without an accompanying transfer report, a copy of the possession report will be forwarded to the shipping COMSEC account, if known, and to the Military Department Accounting Headquarters, if applicable.

42. Conversion of COMSEC Material. When it becomes necessary to convert the short title and/or accounting number of an item of COMSEC material, the conversion will be reported to the COR for proper adjustment of accounting records. A conversion can result from major modification of an equipment requiring the equipment to be redesignated (e.g., TSEC/KL-60, redesignated as TSEC/KL-60A). A conversion will be reported by simultaneously submitting a possession report and a destruction report prepared on SF-153s. The possession report will list the item by its new short title and accounting number, and will contain a remark referencing the associated destruction report. The destruction report will list the previous short title and accounting number and include a remark that the destruction is for record purposes only and a reference to the associated possession report. One signed copy of each report will be forwarded to the COR, and one signed copy of each report will be retained for file.

43. Inventory Report.

a. Semiannual Inventories. Semiannual preprinted inventories are issued by the NSA COR and reflect all COMSEC material (legends 1 and 2) charged to the account as of the date the report is prepared. Preprinted inventories (See Figure 5) are arranged so that distribution among contractor COMSEC accounts occurs evenly throughout the inventory period. The inventory will always be dated within the inventory period and will be forwarded approximately six months after the date of the previous inventory. Physical (sight) inventories will be conducted and inventory reports returned to the NSA COR no later than ten working days after receipt.

Note: Inventories which reflect the account's holdings of classified operational keying material will be classified CONFIDENTIAL. These inventories may be returned via certified mail.

(1) To complete the inventory, the COMSEC Custodian will accomplish the following:

a. With a properly cleared witness, conduct a physical (sight) inventory of all COMSEC material held by the account. COMSEC material issued on hand receipt must be physically sighted by the COMSEC Custodian and a properly cleared witness at least semiannually. STU-111s held on hand receipt by distant users, however, need not be physically sighted by the COMSEC custodian. The user to whom the equipment was issued will physically sight the unit when so notified by the COMSEC custodian and will certify in writing to the custodian that this has been accomplished. The physical sighting will be conducted immediately upon request in order for the COMSEC custodian to return the completed inventory to the COR. COMSEC equipments which have been accepted by the Government and are being held in storage by the contractor may be assumed to contain all the required subassemblies and elements and need not be opened to check individual items; the inventory can be made from external listings of components. Equipments in operation or which are being subjected to tests are exempt from this provision, as opening them would be impractical. Sealed or unit packed material will be inventoried in the manner prescribed in paragraph 51.

b. Compare the results of the physical (sight) inventory against the preprinted inventory. Any discrepancies that exist should be resolved by comparing the preprinted inventory against the COMSEC Register. Normally, any accounting transactions occurring after the date of the preprinted inventory will not be added to or deleted from the inventory. (If the inventory is being conducted for the purpose of a change of COMSEC Custodian, all transactions must be accounted for so that the completed inventory reflects that material actually held by the account on the date of COMSEC Custodian changeover.) Particular attention should be given to additions to, or deletions from, the account which were accomplished just prior to the date of the report. In some instances, accounting reports may not reach the COR in time for processing against the account, and the COMSEC Custodian must update the report by deleting an item or by supplementing the report with an SF-153. Each item to be deleted will be lined out in ink by the COMSEC Custodian (erasures are not authorized). Complete details to support the deletion will be given in the "remarks" column opposite the item. In the case of a transfer, this will include the addressee's name and account number, the outgoing transfer number, and the transfer report date (e.g. transferred to Army Account 5AP111, Transaction Number (TN) 111003, dated 870310). If the deletion is based on a destruction report, the date and transaction number will be provided. In the case of material held and not listed on the inventory, the material will be listed on an SF-153, appropriately classified, signed by the same individuals signing the inventory, and attached as a supplement to the preprinted report. The "remarks" column of the SF-153 will indicate the name, account numbers, transaction number, date of incoming transfer, and details, as appropriate, to support the supplement. The supplement to the preprinted inventory will be assigned the same transaction number as that given the inventory (Figure 6).

c. During each inventory, cognizant personnel of the company will review each item on the inventory to determine whether the material is still required in the performance of a current contract. If any material is no longer required, a remark to that effect will be placed in the "remarks" column opposite each item, with an indication of the approximate date a request for disposition is to be forwarded to the Contracting Officer.

d. When the preprinted inventory has been reconciled to agree with the account's actual holdings, the COMSEC Custodian and witness will sign and date the certifications on the preprinted inventory and any supplemental SF-153. The number of supplemental forms will be indicated in the space provided in the COMSEC Custodian's certification block. If supplemental forms are not used, mark "NONE" in the COMSEC Custodian's certification block. The COMSEC Custodian should then make a final review of the inventory to ensure that any deletions or additions are fully documented and that the certification blocks are signed and dated, and that a transaction number has been assigned. A signed copy of the report will be retained by the COMSEC Custodian for his files.

e. Return all semiannual preprinted inventories to the COR within ten working days after receipt. (Exceptions are those inventories submitted to an account preparatory to an auditor's visit. These inventories will be held by the account until the auditor arrives, at which time the inventory will be jointly conducted by the COMSEC Custodian and Auditor.)

f. Upon receipt of the certified inventory by the COR, it will be reconciled with the COR records. The COMSEC Custodian will be advised only if discrepancies are noted. If the account is cited with any discrepancy, the COMSEC Custodian will take corrective action within 48 hours of receipt of such notice, advise the COR of the action taken, and submit therewith any substantiating reports required.

g. Change-of-Custodian Inventories. The inventory required upon change of COMSEC Custodian will be accomplished as prescribed above.

h. Special Inventories. The COMSEC Custodian will conduct a special inventory when directed by the COR, Contracting Officer, or Facility Security Officer for reasons of suspected loss of COMSEC material or frequent deviation from accounting procedures. Special inventories will be recorded on an SF-153. They will not be forwarded to the COR unless requested by the COR or unless the authority directing the special inventory desires that the COR verify its accuracy.

i. Negative Inventories. Even though a COMSEC account may not hold COMSEC material, semiannual inventories will still be forwarded to the COMSEC account from the COR. The COMSEC Custodian with a properly cleared witness (usually the Alternate COMSEC Custodian) will sign the negative inventory, thereby certifying that the account does not hold COMSEC material. COMSEC accounts will continue to receive semiannual inventories until a requirement for the COMSEC account no longer exists, and the COMSEC account is formally closed. If the COMSEC account has received, or still holds COMSEC material when a negative preprinted inventory is received, the inventory should be supplemented to reflect the COMSEC material held by the COMSEC account.

44. Classification of COMSEC Accounting Reports and Files. All accounting reports and files are classified if they list short titles for "two-person control" material; if the remarks are classified; if they contain a complete or substantially complete record of an account's holding of classified operational keying material; or if they contain reports which supply classified keying material effective dates, in which case a minimum

classification of CONFIDENTIAL will apply. Otherwise, each accounting report and file will be marked FOR OFFICIAL USE ONLY (FOUO). Additionally, the following guidance is provided:

a. COMSEC Register Files. If the file contains L6061s for classified operational keying material, the entire container will be classified CONFIDENTIAL. In those cases where the account maintains a separate container for the Inactive Register Files, this container will also be classified CONFIDENTIAL, if it contains inactive L6051s for classified keying material. If the register file is automated, the disk containing the register file information will be classified CONFIDENTIAL.

b. Accounting Files. Although individual destruction reports/transfer reports for classified operational keying material are FOUO, a compilation of these reports becomes CONFIDENTIAL; therefore, a file holding these reports must be so classified. Likewise, an accounting file holding classified inventories must also be stamped CONFIDENTIAL.

c. Any accounting report or file containing classified information will be classified according to the highest level of classified information contained therein.

d. Classification of accounting files is the responsibility of the COMSEC Custodian and will be determined by evaluating the content of each COMSEC accounting report, COMSEC accounting file, or DD Form 254. If any doubt arises, the matter should be referred to the FSO.

e. Each report or file which contains classified COMSEC information will also bear, in addition to the classification, the following statement: "Classified by: (the appropriate Agency/Department Directive), Declassify on: Originating Agency's Determination Required."

45. Retention and Disposition of COMSEC Accounting Records. All COMSEC accounting records will be retained for minimum of three years, at which time they may be retired or destroyed in a manner commensurate with their classification.

46. Accounting for and Entering Amendments to COMSEC Publications.

a. Message Amendments. A message amendment is used to announce information which must be immediately entered into a COMSEC publication. After posting the amendment and noting the entry on the "Record of Amendments" page, classified message amendments will be destroyed in compliance with the procedures outlined in the ISM. Destruction of message amendments will not be reported to the COR.

b. Printed Amendments. Printed amendments will be accounted for as COMSEC publications until they have been posted, the residue destroyed, and the destruction reported to the COR.

c. Posting the Amendments. An amendment will be posted as soon as possible after receipt or effective date in order to keep the basic publication current. An amendment will be posted by the COMSEC Custodian, other

cleared individuals working under his direct supervision, or by the individual holding the basic document on hand receipt. The following guidance will assist COMSEC Custodians in avoiding errors which commonly occur in posting amendments:

(1) Untrained personnel will not post amendments unless they are closely supervised.

(2) Specific instructions contained in the letter of promulgation or handling instructions will be read and understood prior to posting. The entire amendment will be posted at one time and not extended over a period of time.

(3) If replacement pages are included in the amendment, a page check of both the basic publication and residue of the amendment will be made prior to destruction of the residue. Inadvertent destruction of effective portions of documents together with residue from amendments is a major cause of COMSEC material security violations.

(4) The individual posting the amendment will note the posting of the amendment on the "Record of Amendments" page and, if pages were added to or removed from the publication, date and sign the "Record of Page Checks" page.

(5) If the amendment was posted by an individual other than the COMSEC Custodian, all residue of the amendment, including any pages removed from the basic publication, will be returned to the COMSEC Custodian for destruction.

(6) To preclude loss, the residue of an amendment which is being held pending destruction will be placed in a sealed envelope marked with the short title, accounting number, and classification of the amendment.

47. Accounting for COMSEC Material Prior to Acceptance by the U.S. Government.

a. When COMSEC material is transferred outside a contractor's facility for test and evaluation prior to acceptance by the U.S. Government, the COMSEC Custodian will put the following notation on the transfer report:

"The above-listed material has not been accepted by the U.S. Government and is the property of (name of contractor). The material is being transferred on a temporary basis for test and evaluation. Upon completion of test and evaluation, return the material to (name of contractor)."

b. The following remark will appear on the transfer report returning the material: "The above-listed material has not been accepted by the U.S. Government and is the property of (name of contractor). The material was transferred to (account number) for test and evaluation."

c. When COMSEC material transferred for test and evaluation is returned to the originating contractor and accompanying transfer reports are signed and distributed, no further accounting at the COR is required until final

acceptance of the material by the Government.

d. In addition to the remarks prescribed in Paragraph 47a and b, above, these transactions should be conducted under the guidelines set forth in Paragraph 52, with the exception that no DD-250 will be necessary.

e. Classified material, such as microcircuits, printed circuit boards, etc., produced by a subcontractor and provided to the prime contractor will not be entered into the COMSEC Material Control System (CMCS) by the prime contractor. Instead, such material shall be placed in the in-process accounting system by the prime contractor and controlled in accordance with Section VII of this Supplement.

48. Accounting for Government-Furnished Property and New Material. To facilitate COMSEC accounting, all COMSEC material shipped by a contractor will be categorized as either government-furnished property (GFP) or new material.

a. COMSEC material accepted by the Government which has been entered into the CMCS on a previous transaction is considered GFP material, e.g., material returned to the contractor for rework, material accepted by the Government and picked up by the contractor on a possession report.

b. COMSEC material which has been accepted by the Government and is being entered into the CMCS initially is considered new material. COMSEC material which is produced under the CCEP or Authorized Vendor Program remains the property of the producing facility and will be retained under "in-process" controls until sold. At that point, the COMSEC item will be issued as new material.

c. GFP material will be identified as such in the "remarks" column of the transfer report. Material not identified as GFP will be considered new material. When GFP and new material are listed on the same transfer report, the GFP material will be listed as a separate line item and identified as GFP in the "remarks" column.

d. COMSEC material received by the contractor as GFP is not to be entered into the Company's Government Industrial Property Account or Document Control System.

49. Residual Inventory and Master Disposition Record.

a. Procedures for Preparing Residual Inventory

(1) Upon completion of a contract, the contractor will prepare a residual inventory of all COMSEC material (including unclassified elements and subassemblies (e.g., E-___, Z-___), generated and retained by the contractor or furnished by the Government under contract. The residual inventory will be forwarded to the appropriate COR through the Contracting Officer.

(2) Those items listed on the residual inventory which have not been accepted by the Government and those items which will be required for the performance of current contracts will be so notated.

(3) Upon receipt of the residual inventory, the COR will review the COMSEC material listed and provide the contractor with disposition instructions.

b. Master Disposition Record. The contractor will be required to maintain a disposition record for all items of COMSEC equipment and assemblies. (Not applicable to elements, E-___, or subassemblies, Z-___.) A form similar to that shown in Figure 13 can be utilized to maintain the record which will include, for each item, the following:

- (1) The accounting or serial number of the item.
- (2) The number of the COMSEC account to which the material was shipped.
- (3) The date of shipment.
- (4) The contractor's transaction number.
- (5) The shipment control number (DCS, Registered Mail, etc.).
- (6) The DD-250 partial shipment number.

Upon completion of the contract, the contractor will submit to the appropriate COR, a copy of the Master Disposition Record of Accountable COMSEC Material, similar to that shown in Figures 13 and 14.

50. Receipt of COMSEC Material.

a. Sources. COMSEC material may be received from the military departments, governmental agencies, and contractors. COMSEC material may arrive at a facility via one of the methods of shipment outlined in this Supplement. The COMSEC Custodian will notify the contractor's mail and receiving departments that a COMSEC account has been established and provide them with an adequate internal address so that mail or material received addressed to the account may be forwarded unopened to the COMSEC Custodian.

b. DCS Form 10. The Defense Courier Service (DCS) regulation requires contractor personnel who may be required to accept DCS material to complete a Defense Courier Service Authorization Record (DCS Form 10) prior to receipt for material. DCS Forms 10 may be obtained from the servicing DCS station. Figure 10 lists DCS addresses. (ARFCOS Form 10 may be used until exhausted.)

c. DCS Form 1. Material shipped via DCS will be listed on Defense Courier Service Receipt to Sender (DCS Form 1). (ARFCOS Form 1 may be used until exhausted.)

d. Receipting For Packages and Examination of Container (refer to paragraph 50e, below, for equipment). Upon delivery of COMSEC material to the COMSEC Custodian or other individuals authorized by the contractor to receipt for packages, the packages will be carefully examined for evidence of tampering or exposure of their contents. If either is evident and the contents are classified or marked CCI or CRYPTO, a "possible physical

insecurity" report will be submitted as outlined in Section XVI. Packages received for by an individual other than the COMSEC Custodian will be delivered to the COMSEC Custodian unopened. If the package contains TOP SECRET keying material, the receiving COMSEC Custodian must immediately initiate two-person integrity (TPI) controls and place the TOP SECRET key in TPI storage (refer to paragraph 90), and both TPI participants must carefully inspect the protective packaging for evidence of damage or tampering, as this is done. Any such evidence should be immediately reported as prescribed in Section XVI. The COMSEC Custodian will carefully inventory and check contents against the enclosed transfer report. Any discrepancies in short titles, accounting numbers, or quantity will be reported to the sender and the COR; and the transfer report will be corrected to agree with the material actually received. If the material is classified or marked CCI or CRYPTO and the discrepancy cannot be resolved between the sender and receiver, a report of possible compromise will be submitted by the receiver. When the incoming check has been completed, the transfer reports will be signed and distributed as follows:

- (1) One copy to the COR.
- (2) One copy to the cognizant Military Department Accounting Headquarters, when applicable.
- (3) One copy to the shipment originator (when corrections of the SF 153 are required).
- (4) One copy for file.

NOTE: It may be necessary to reproduce additional copies of the SF-153.

e. Receipting for Equipment.

(1) Equipments received in sealed shipping cartons which have not been opened or do not exhibit signs of tampering may be receipted for without physically sighting the material on the inside as long as the label on the carton agrees with the transfer report; if not, the contents must be physically inventoried. The COMSEC Custodian must bear in mind that, although the opening of certain types of material need not take place prior to actual usage, time must be allowed between opening and usage to obtain replacements for incomplete or defective items. Additionally, it is the COMSEC Custodian's responsibility to report all shipment discrepancies to the COR as soon as they are discovered.

(2) With the introduction of the new CCI category of COMSEC equipment, many existing/new stand-alone cryptographic equipments, telecommunications and information handling equipments with embedded cryptography, and associated ancillary equipments may now be controlled outside of traditional COMSEC control channels. For example, the Departments of the Army and the Air Force have initiated control of CCI equipment through their standard logistics system. When CCI equipment is received at a contractor facility via other than traditional COMSEC control channels, it is the COMSEC Custodian's responsibility to sign the accompanying paperwork (the Air Force utilizes DD Form 1348-1), and return a copy to the shipper. The

COMSEC Custodian will also be responsible for initiating an SF-153 possession report for the receipted material as prescribed in paragraph 41 and submitting a copy to the NSA COR.

f. Receipting for Tapes (Magnetic/Paper). The COMSEC Custodian will, upon receipt of a shipment of tapes, inventory each reel by short title and accounting number. Discrepancies will be reported to the COR.

g. Receipting for Hardware Keying Material and Manufacturing Aids. Upon receipt of hardware keying material and associated aids, each item will be inventoried by short title and accounting number.

h. Receipting for Protective Packaged Keying Material. Certain items of COMSEC material are protectively packaged at the time of production and will not, in most cases, be opened until they are to be employed by the actual user. Protective packaging applied to individual items of TOP SECRET key must not be removed except under TPI conditions.

i. Receipting for Other Material: Upon receipt of a classified COMSEC document, the COMSEC Custodian or Alternate COMSEC Custodian will stamp or annotate the document "COMSEC MATERIAL--ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE." The publication must also be page checked upon initial receipt, upon completion of entering an amendment requiring the removal and/or insertion of pages, prior to destruction, and prior to shipment to another COMSEC account. Page checks will be accomplished within two working days after receipt of material, immediately after entering an amendment, and two working days prior to shipment or destruction.

j. Page Checking Procedures: The COMSEC Custodian, or an appropriately cleared individual working under his/her direct supervision, will conduct page checks of unsealed material to ensure the presence of all required pages. To conduct the page check, the presence of each page will be verified against the "List of Effective Pages" or the "Handling Instructions," as appropriate. The "Record of Page Checks" page will then be signed and dated; or, if the publication has no "Record of Page Checks" page, the notation will be placed on the "Record of Amendments" page or the cover. If any pages are missing, the "Record of Page Checks" page will be annotated accordingly. If the publication is classified, an insecurity report will be submitted as outlined in Section XVI. Requests for disposition instructions and a replacement publication will be submitted through the Contracting Officer. In case of duplicate pages, the duplicate pages(s) will be removed and destroyed. One copy of a destruction report will be prepared citing the page number and the accounting number of the basic publication, e.g., duplicate page number 72 removed from KAM-130, Number 183. The destruction report will be signed by the COMSEC Custodian and witness and will be filed locally. No notification to the COR is required, and this locally retained destruction report will not be assigned a COMSEC Account Transaction Number. In addition, a notation of the duplicate page and the resultant destruction will be entered on the "Record of Page Checks" page. In those instances where a change of COMSEC Custodian has occurred, the incoming COMSEC Custodian must perform a page check of all unsealed material within 30 days after the change

of COMSEC Custodian takes place. Where the COMSEC account has a prohibitive number of documents requiring page checks, the incoming COMSEC Custodian must submit a request for an extension to allow more time to complete all page checks. It is recommended that the outgoing COMSEC Custodian complete page checks prior to transferring control of the COMSEC account to the incoming COMSEC Custodian. Specific procedures for page checking keying material are outlined below:

(1) Key cards and/or key lists that are shipped in sealed transparent plastic wraps will not be opened until 72 hours prior to the effective date; therefore, a page check upon receipt of the material is not authorized. Test keying material will not be opened until it is to be used. In preparation for actual use, keying material will be opened and page checked in accordance with the handling instructions provided with the material. If no special handling instructions are provided, the keying material will be opened and page checked as outlined in paragraph 50j, above.

(2) Key tapes or key lists in protective canisters must not have the tape or lists removed for inventory or check purposes.

51. Procedures for Handling Keying Material. Keying material must be stored in containers approved for the classification level of the key (refer to paragraph 90). Access to the container storing future editions of classified keying material marked CRYPTO, however, must be restricted to the FSO, COMSEC Custodian and Alternate COMSEC Custodian(s). Where this restriction cannot be applied because others must have access to the container for either current editions of keying material or other material contained therein, future editions of keying material must be stored separately in a locked strongbox which can be opened only by the FSO, COMSEC Custodian and Alternate COMSEC Custodian(s). The strongbox must be kept in the security container. Exceptions may be made in operational areas to allow shift supervisors access to the next future edition of keying material, but not to later future editions.

a. Key Cards. When it is necessary for the COMSEC Custodian(s) to relinquish physical control of operational key cards to a user, the book will be issued on a hand receipt basis. If, in the opinion of the COMSEC Custodian, issue of individual cards is warranted, the user's initials in the "USED" column of the key card "USAGE RECORD" will serve in lieu of a hand receipt. When a card is removed from the book for use, the user will place his initials and the date in the "USED" columns of the "USAGE RECORD" on the inner front cover of the book by the appropriate card number. Handling instructions may contain details applicable to a particular short title.

b. Key Lists/Key Tapes.

(1) Operational key lists packaged in sealed transparent plastic envelopes will not be page checked until 72 hours prior to the effective date. When it is necessary for the COMSEC Custodian to relinquish physical control of operational key lists to a user, he or she will do so on a hand receipt basis. If the issue of individual settings is warranted, the user will sign and date the "ISSUED TO" column on the "DISPOSITION RECORD" on the inside front cover of the publication. This will serve in lieu of a hand receipt.

(2) Key lists/key tapes packaged in plastic protective canisters do not require a page check. Upon receipt of this material, the COMSEC Custodian will annotate the accompanying record of usage card with the short title, edition, and register number of the material. (NOTE: NSA will no longer provide plastic zip-lock bags with this material; however, zip-lock containers are available through the Federal Stock System - Stock Number 8105-00-837-7754 (1000 per box).) Labels will not be affixed to keying material canisters for purposes of identifying the classification of the material contained therein. Should additional identification of the classification be necessary beyond that visible through the window of the canister itself, the preferred means is to mark or affix a label or tag to the zip-lock bag, if available, or mark the classification on the plastic canister using a grease pencil. If the situation warrants, the COMSEC Custodian may issue the entire canister to the user on a hand receipt basis. The user, however, must not remove more tape settings from the canister than are required for current use. As each setting is removed, the user will place his initials and the date in the "USED" column of the "USAGE RECORD" card applicable to the material.

52. Transfer of COMSEC Material.

a. General. COMSEC material may be transferred from one COMSEC account to another only as prescribed by the procedures in this Supplement. It is the responsibility of the Contracting Officer or the COR to provide the contractor with the authority for transfer and shipping instructions when material is to be transferred outside the contractor's facility. When the validity of a shipping address or authority for shipment is in question, it is the responsibility of the COMSEC Custodian to initiate action to contact the COR before making the shipment. Accountable COMSEC material, regardless of the accounting legend code assigned, will not be shipped unless a COMSEC account number is provided with the shipping address. A contractor may, however, be directed to transfer CCI equipment to a military department standard logistics system account. Where validation of the account number and shipping address is necessary, the COMSEC Custodian will obtain the verification from the appropriate Military Department's Accounting Headquarters. The COMSEC Custodian will utilize an SF-153 for such transfers, just as with any other outgoing transaction of COMSEC material. The COMSEC Custodian is responsible for ensuring that the equipment and page checking provisions outlined in paragraph 50 are accomplished prior to packaging COMSEC material for transfer. Such checks will normally be conducted no earlier than 48 hours prior to packaging the material.

The COMSEC Custodian is also responsible for ensuring that such shipments are only by one of the authorized modes of transportation prescribed in paragraph 55. When transferring Government Furnished Property (GFP), the SF-153 will be annotated in the remarks section identifying those items as GFP.

b. Transfer of COMSEC Material to the U.S. Military Departments. The shipping COMSEC Custodian will prepare five copies of the SF-153 and enclose the original and one copy with the shipment (see Figure 2). He/she will put the notation "ADVANCE COPY" on two of the copies, stapling a copy of the Material Inspection and Receiving Report (DD-250), if applicable, to each and forward one copy to the NSA COR and one copy to the appropriate Military Accounting Headquarters. The COMSEC Custodian will retain the final copy for

file. Additionally, in those instances where the address listed in Block 13 of the DD-250 is not an element of the same department or agency listed in Block 14, the shipping COMSEC Custodian will prepare an additional advance copy of the transfer report and DD-250 and forward them to the Accounting Headquarters of the Department or Agency listed in Block 14. For example, if the material is being shipped to a Navy COMSEC account, but Block 14 indicates that Air Force purchased the equipment, an advance copy of the transfer report and DD-250 will be forwarded to both the Navy and Air Force Accounting Headquarters. The following notations, as appropriate, will be included on all copies of the transfer reports going to the U.S. Military Departments:

- (1) Ownership of the equipment (NSA, Air Force, etc.)
- (2) Purpose of transfer/loan, loan term, and authority for transfer.
- (3) Contract number/project name (if appropriate).

Additionally, the following statement must be placed on all SF-153s reporting the transfer of COMSEC material:

"Custodian:

Sign all copies and distribute as prescribed by the accounting instructions of your Service. This shipment consists of _____ containers."

c. Transfer of COMSEC Material to All Other Activities. The shipping COMSEC Custodian must prepare an original and three copies of the SF-153 (see Figure 3) and enclose the original and one copy with the shipment. He/she will put the notation "ADVANCE COPY" on the fourth copy, staple a copy of the Material Inspection and Receiving Report (DD-250) thereto (if applicable), and forward it to the NSA COR. The COMSEC Custodian will retain the third copy for file. The following notation will be put on all copies of transfer reports going to activities other than the U.S. Military Departments:

"Custodian:

Sign all copies. Return the original to:

Director
National Security Agency
Operations Building Number 3 (Y13)
Room C1B51
Fort George G. Meade, MD 20755-6000

Dispose of remaining copies as prescribed by the accounting instructions of your organization."

d. Receipt/Tracer Responsibility. Upon shipment of COMSEC material from the contractor's facility, NSA and the Service Accounting Headquarters, when appropriate, assume responsibility for ensuring that the material is received by the intended recipient on a timely basis. Upon receipt of an advance copy of an SF-153, NSA and the Service Accounting Headquarters will

establish a receipt suspense date and take any subsequent tracer action required. Tracer actions for shipments to Military Department standard logistics system accounts, however, rests solely with the appropriate Military Service Accounting Headquarters. The contractor will not receive a signed copy of the transfer report and is not responsible for ensuring that the material reaches the intended recipient, provided packaging, addressing, and shipping instructions are complied with. The procedure in no way relieves the contractor of responsibility for errors which normally can only be detected upon opening of the package by the recipient; e.g., shipment of the wrong item, incorrect nameplate, etc. In lieu of a signed copy of the transfer report, the contractor's recorded proof of shipment will be his file copy of the transfer report combined with either a signed DCS Form 1, Government Bill of Lading (SF-1103), U.S. Registered Mail receipt, or other documentation of shipment from the contractor's facility.

e. Forwarding an Advance Copy of Transfer Report and Material Inspection and Receiving Report (DD-250) to the NSA COR and U.S. Military Service Accounting Headquarters. Timely input to COMSEC accounting, financial, and property records and establishment of receipt suspense are dependent on the shipping COMSEC Custodian forwarding an advance copy of the transfer report and DD-250 (e.g., production contracts), when applicable, to the NSA COR and the Service Accounting Headquarters, when appropriate, as soon as the material has been readied for shipment.

f. Nonroutine Disposition of COMSEC Material. COMSEC material which is lost, compromised, or inadvertently destroyed may be removed from a COMSEC account only with the specific written approval of the Chief, Information Security Support Group, NSA.

53. NSA COR and Military Department Accounting Headquarters.

- a. NSA COR
Director
National Security Agency
Operations Building No. 3 (Y13)
Room C1B51
Fort George G. Meade, MD 20755-6000
- b. Army Accounting Headquarters
Commander
U.S. Army Communications Security
Logistics Activity
ATTN: SELCL-NICP-OR
Fort Huachuca, AZ 85613
- c. Navy, Marine, and Coast Guard Accounting Headquarters
Director
COMSEC Material System
3801 Nebraska Avenue, N.W.
Washington, DC 20390

- d. Air Force Accounting Headquarters
Commander
U.S. Air Force Cryptologic Support Center
Electronic Security Command
ATTN: MMKD
San Antonio, TX 78243

Verification of Air Force standard logistics system account number and shipping addresses may be obtained by calling (512)925-2771.

54. Packaging COMSEC Material for Shipments Outside the Facility. Movement of COMSEC material from the contractor's facility to any other location will be accomplished only with permission of, or as instructed by, the Contracting Officer or the COR, and in accordance with the following:

a. Classified COMSEC material will be securely packaged for shipment in two opaque wrappers with no indication of the classification on the outside wrapper. Each wrapper will be marked with the "TO" and "FROM" addresses. The outer wrapper must never carry identification of the contents which directly discloses a cryptographic or COMSEC association; e.g., a system indicator and, where applicable, the acronym "TSEC," etc. The short title of an equipment less the "TSEC" designation followed by the accounting number, e.g., KW-59/101, will be marked on the crate or outer wrapper to identify the contents. Assemblies, ancillary devices, elements, and subassemblies shipped individually will be identified by their short titles, accounting numbers, and the short titles of the equipments in which the items are to be used. Items not accountable by accounting number will be identified by short title and quantity. Figure 12 provides examples of COMSEC material identification markings. NOTE: The markings on the crate or outer wrap identifying the COMSEC material within must always agree with the accompanying COMSEC Material Report (SF-153).

b. The inside wrapper of cryptomaterial will be marked CRYPTO together with its classification, if any. Additionally, if the shipment contains keying material designated for "U.S. Use Only," the inner wrapper will also be marked "Special Handling Required; Not Releasable to Foreign Nationals." Likewise, if the shipment contains cryptomaterial which is releasable, the inner wrap will be marked "Special Handling Required; For U.S. and Specified Allies only."

c. The inside wrapper of all COMSEC material addressed to COMSEC accounts will be marked with the notation "TO BE OPENED ONLY BY THE COMSEC CUSTODIAN."

d. Keying material will be packaged separately from its associated crypto-equipment, unless the application or design of the equipment is such that the corresponding keying material cannot be physically separated from it. Where practicable, individual shipments will be limited to not more than three editions or three months' supply of a particular item of keying material (whichever is the greater amount). This restriction does not apply to packaged irregularly superseded materials and may be waived when issuing material to a newly established COMSEC account or in cases where supply is difficult and the number of shipments is limited.

e. Cryptographic equipment shall not be shipped in a keyed condition unless the physical configuration of the equipment makes segregation of the keying material impossible. For equipments utilizing a crypto-ignition key, removal of the crypto-ignition key permits the equipment to be considered unkeyed.

f. CCI equipment must be securely packaged in a manner that will guard against damage or loss in transit. The equipment designator must be annotated on the package. The "CCI" marking may be placed on the exterior of the package when so requested by the procuring activity. The accompanying paperwork will be placed in an envelope securely affixed to the outside of the package and the envelope marked with the "TO" and "FROM" addresses, including the account number without the word "COMSEC."

g. Unclassified COMSEC material will be wrapped in the same manner as any other unclassified material in accordance with the packaging requirements of the contract.

h. All transfer reports and other forms (e.g. DD Form-250) covering an individual DCS shipment must bear the individual shipment control number and will be affixed to the inner wrapper of the package. NOTE: The transfer report and DD Form-250 will never be placed inside the sealed container with the COMSEC material, as this defeats the purpose of marking the short title and accounting numbers on the outside of the container.

i. For multiple-package shipments, the COMSEC material will be packaged beginning with package number 1, followed by a slant and the total number of packages comprising the shipment. Package numbers will continue to be assigned in ascending order until the entire shipment is packaged (e.g. for a shipment consisting of three packages, the first box would be marked 1/3; the second one marked 2/3; and the third (last) one marked 3/3. The shipping documents (SF-153, DD-250, etc.) will be affixed to the inner wrapping of the first package of multiple-package shipments. The serialized package number will not be annotated in the immediate vicinity of DCS control numbers.

55. Authorized Modes of Transportation. The provisions of this paragraph apply only to physical transfers between accounts; local movements (i.e., within a complex) may be performed by any contractor personnel who are U.S. citizens cleared to the level of the material, and who have been COMSEC briefed. There are various authorized modes of transportation for COMSEC material. The authorized mode for each specific type of COMSEC material is as follows:

a. Classified Keying Material Marked CRYPTO. The cognizant U.S. Government Contracting Officer may authorize the use of U.S. Registered Mail for the shipment of individual editions of CONFIDENTIAL keying material to user activities served by U.S. postal facilities, provided the material does not at any time pass out of U.S. citizen control, and does not pass through a foreign postal system or any foreign inspection. Keying material classified SECRET or higher may not be sent through the mail without prior approval of the Director, NSA. In time-critical situations, the cognizant U.S. Government Contracting Officer or his/her representative may approve the use of commercial passenger aircraft for transportation of classified COMSEC information, provided departmental and Federal Aviation Administration

procedures are followed. The use of commercial passenger aircraft for the transportation of current or superseded keying material is normally prohibited. Except when using systems specifically designed for electronic rekeying, operational keying variables may be transmitted electrically only under emergency conditions and only when the communications system provides end-to-end security equal to the classification of the transmitted key setting, and the key setting does not appear in plain text anywhere in the communications path. Under normal conditions, however, classified keying material must be transported by one of the following means:

(1) Defense Courier Service (DCS).

(2) Appropriately cleared and properly designated U.S. military or Government civilian personnel.

(3) Appropriately cleared contractor personnel who have been designated in writing, as couriers by the Facility Security Officer, provided the material is classified no higher than SECRET. For TOP SECRET keying material, courier authorization must be obtained on a case-by-case basis from the cognizant Contracting Officer or his/her representative.

(NOTE: Two-person integrity (TPI) controls will be applied whenever local couriers transport TOP SECRET keying material from a user COMSEC account to another user account or user location. The keying material must be double-wrapped while in transit, and receipts for this material must be signed by two persons who are cleared TOP SECRET and are authorized to receive the material. TPI controls are not required for TOP SECRET keying material while it is in the custody of the Defense Courier Service or the Diplomatic Courier Service.)

b. Classified COMSEC Equipment and Components.

(1) COMSEC equipment and components classified higher than Confidential may be transported by any of the means identified above as authorized for keying material or by a cleared commercial carrier under Protective Security Service (PSS).

(2) COMSEC equipment and components classified Confidential may be transported by any of the means specified above, or any of the following:

a. U.S. Registered Mail, provided it does not at any time pass out of U.S. control and does not pass through a foreign postal system or any foreign inspector

b. Commercial carriers under Constant Surveillance Service (CSS) in CONUS only.

c. U.S. military or military-contractor air service (e.g., MAC, LOGAIR, QUICKTRANS), provided the requirements for CSS are observed.

c. Other Classified COMSEC Material.

(1) Media which embody, describe, or implement a classified

cryptographic logic, such as full maintenance manuals, cryptographic logic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic computer software may not be transported through any postal system. The following transportation methods must be utilized:

(a) Defense Courier Service (DCS)

(b) Appropriately cleared U.S. military or Government civilian personnel who have been designated in writing by NSA or the cognizant Contracting Officer to act as courier for the material.

(c) Appropriately cleared contractor personnel who have been designated in writing by NSA or the cognizant Contracting Officer to act as courier for the material.

(2) Media which does not embody, describe, implement, or contain a classified cryptographic logic may be transported by any of the means listed below. (NOTE: The use of Standard First Class Mail service is not acceptable for the transportation of any classified COMSEC material.)

(a) Any of the means authorized in subparagraph c(1), above.

(b) If classified SECRET, it may also be transported via U.S. Registered Mail or by a cleared commercial carrier utilizing PSS.

(c) If classified CONFIDENTIAL, it may be transported via U.S. Registered Mail or U.S. Postal Service Certified Mail.

d. Unclassified Keying Material Marked Crypto.

(1) Within CONUS:

(a) Authorized commercial courier.

(b) U.S. Registered Mail. Where practicable, no more than one edition should be transported via this method.

(c) Authorized U.S. military or Government civilian personnel.

(d) Authorized contractor personnel.

(2) Outside CONUS

(a) DCS.

(b) Authorized department, agency, or contractor courier.

e. Controlled Cryptographic Item (CCI).

(1) Within CONUS:

(a) Commercial carrier providing DoD Constant Surveillance

Service (CSS). (NOTE: Contact the Transportation Officer of the nearest Defense Contract Administration Service Management Area (DCASMA) office for information concerning the carriers servicing your area or where DCASMA does not administer your contract, the cognizant Contracting Officer.

(b) U.S. Registered Mail.

(c) Authorized department, agency, or contractor courier. For contractor couriers, the authorization to act as a courier or escort for CCI equipment and components may be granted by the company FSO.

(2) Outside CONUS:

(a) DCS will accept CCI for shipment outside the 48 contiguous states only when it has been proven that no other means of secure transportation is available.

(b) CCI equipment may be transported by company courier to countries specifically listed in the MOU/MOA between NSA and vendor as authorized for marketing of the equipment, or as otherwise approved, in writing, by NSA. Couriers must be issued passes by the FSO which contain the employee's full name, social security number; issue date; pass expiration date (no longer than one year from the date of issue); identification of company, with name and signature of issuing official; and employee's signature. The FSO must ensure that the courier is briefed on proper security procedures and that all requirements for access and the physical security of the equipment or materials can be complied with. The FSO must maintain for a period of three years, a record of each instance in which material or equipment is couriered, identifying each piece of couriered material, the date/time of departure, the commercial flight number, any flight transfers, and destination. Transportation may be by any means that permit the courier to maintain continuous accountability and provide protection against losses and unauthorized access while in transit. Where transportation is by commercial aircraft, the CCI equipment should be stowed in the cabin where the courier can maintain constant surveillance. If equipment bulk will not permit cabin storage or creates an excessive burden for the courier, CCI circuit boards may be removed for cabin storage, and remainder of the equipment may be checked as hold baggage. For sales to foreign governments, the contractor is responsible for being fully knowledgeable regarding the customs regulations and procedures of countries where the CCI equipment will be demonstrated. The contractor also is responsible for arranging with the governments of such countries for the entry of CCI equipment into their countries and for the removal of the equipment without customs inspection. Arrangements must be made through the U.S. Military Services to provide the same exemption from customs inspection for CCI equipment being transported to U.S. Military Forces abroad. Contractors must not transport CCI equipments through countries other than those which have been approved as stated above. All incidents of impoundment, seizure, or loss of CCI equipment while it is being couriered must be reported in accordance with Section XVI of this Supplement.

f. All Other Unclassified COMSEC Material. Material may be shipped by

any means which will reasonably assure safe and undamaged arrival at its destination. Unclassified COMSEC items may be shipped with classified COMSEC material when there is an operational need to provide both types of material together.

56. CCI Equipment Distribution. Contractors who purchase CCI equipment must arrange for equipment distribution with the vendor, and in coordination with the U.S. Government Contracting Officer (if applicable), as follows:

a. Direct shipment to primary COMSEC accounts - CCI equipment destined for either the primary COMSEC account or its subaccounts will normally be shipped directly to the primary COMSEC account. The SF-153 will be addressed to the primary COMSEC account and will be included with the shipment. An advance copy will be provided to the NSA COR and to the appropriate Department or Agency COR, if applicable. Upon receipt of the equipment at the primary COMSEC account, the COMSEC Custodian must verify the contents of the shipment against the accompanying paperwork. If no discrepancies exist, the COMSEC Custodian will sign the SF-153 and return a copy to the vendor, reproducing additional copies for the NSA COR, the Department or Agency COR, if applicable, and for his/her files. If a discrepancy is noted, follow the procedures specified in paragraph 50.

(1) Redistribution to COMSEC subaccounts: Upon receipt of the shipment at the primary COMSEC account, the COMSEC Custodian will prepare the appropriate equipment for shipment to its subaccounts, following the packaging procedures specified in paragraph 54. An SF-153 will be included in each separate subaccount shipment identifying the contents therein. The SF-153 will be assigned a transaction number as prescribed in paragraph 39b(9).

(2) Receipt by subaccounts: Upon receipt of the equipment by the COMSEC subaccount, the subaccount COMSEC Custodian must verify the contents of the package against the accompanying SF-153.

If no discrepancies exist, he/she will sign the SF-153, assign it an incoming transaction number, return a copy to the primary COMSEC account, and retain the original for file.

b. Direct shipment to COMSEC subaccounts - When a direct shipment of CCI equipment is made to a COMSEC subaccount, the vendor will include a copy of the SF-153 along with the shipment, and provide advance copies to the primary COMSEC account, the NSA COR and the appropriate Department or Agency COR, if applicable. The advance copy will serve as notice to the primary COMSEC account of the shipment of the equipment directly to one of its subaccounts. Upon receipt of the signed SF-153 from its COMSEC sub-account, the COMSEC Custodian of the primary COMSEC account will sign the advance copy of the SF-153 (thus attesting to the receipt of the equipment by the intended recipient) and will assign it an incoming transaction number. Prior to forwarding the signed copy of the SF-153, the COMSEC Custodian of the primary COMSEC account will duplicate a sufficient number of copies and will forward one to the NSA COR, one to the Department or Agency COR, if applicable, and will retain one for his files along with the signed SF-153 received from the subaccount. It will be the responsibility of the COMSEC Custodian of the

primary COMSEC account to ensure that his/her subaccount COMSEC Custodians execute their SF-153s within 48 hours after receipt of the equipment, thereby alleviating the need for tracer action. Tracer action for equipment shipped directly to COMSEC subaccounts rests with the COMSEC Custodian of the primary COMSEC account.

c. Accountability to the COR - All CCI equipment resident at a COMSEC subaccount will be charged to the primary COMSEC account.

SECTION VII. HANDLING AND CONTROL OF CLASSIFIED COMSEC MATERIAL DURING
DEVELOPMENT AND MANUFACTURE/ASSEMBLY

57. General. The security of classified COMSEC material generated by a contractor is dependent upon adequate controls from inception of the material through eventual destruction. While the CMCS provides the desired degree of control over the finished COMSEC material after it has been accepted by the Government, the procedures would entail a prohibitive amount of paperwork if applied to classified COMSEC material in the various stages of fabrication within a contractor facility or when transmitted between a prime contractor and subcontractor. In lieu of entering such in-production material into the formal CMCS, contractors engaged in COMSEC contracts will control the material under internal in-process accounting, leaving the methods and details to the discretion of each contractor. Where the contract requires the production of TOP SECRET keying material, the mandated no-lone zone controls must be implemented and addressed in the in-process procedures. Prior to commencing fabrication of classified COMSEC material, the contractor must prepare written in-process accounting procedures to be employed to support a particular classified contract. If the procedure applies to more than one contract, it will so state. The written procedure will clearly establish the point in the production process when the item becomes classified and subject to in-process accounting. The procedure will provide specific instructions for the method of control, the proper records to be maintained, and instructions for the reconciliation of in-process accounting records (see Paragraph 58), and the maintenance of the Master Disposition Record (see Paragraph 49b). The in-process accounting procedure will also stipulate the individuals or department responsible for ensuring that the required records are maintained and that the requirements stated in the procedure are followed. NSA will assist contractors in identifying the point in the production process when an item becomes classified and, if requested, will provide a sample procedure which may be used as a guide in the preparation of their in-process accounting procedure. Ninety days prior to start of production and implementation of the procedures, a draft procedure will be forwarded to the NSA COR through the Contracting Officer for approval. Likewise, if the contractor decides, due to changes in the production process, to revise the procedure, the revision must again be submitted to the NSA COR for approval prior to implementing any changes. The contractor should note that the fabrication process cannot begin until this procedure has been approved by the NSA COR.

58. Requirements.

a. Within a Facility, in-process accounting procedures will include the following information for each end item of COMSEC material from the point the material reaches a classified stage and is subject to in-process controls:

(1) Date introduced into the in-process accounting systems within the facility.

(2) A brief unclassified description of the items to be controlled. This may be one or a combination of the following:

- (a) Federal Stock Number
- (b) NSA or Contractor Part Number
- (c) TSEC Short Title.

(3) Quantity

(4) Serial or Control Number. (NOTE: While quantitative accounting is acceptable, the contractor may elect to maintain accountability by serial or control number).

(5) A detailed explanation of the production process and the control points and types of records to be maintained which will reflect an accurate count of classified items in a particular production process at any given time.

(6) Disposition: For example:

(a) Incorporated in or otherwise made a part of another item of classified material.

(b) Entered into the CMCS as an individual accountable item.

(c) Destroyed or declassified.

(d) Returned to a subcontractor for rework or returned to the prime contractor after rework.

(e) Any other disposition not covered in (a) through (d), above.

b. Integrated Circuits (IC's). Rigid accountability of IC's and associated manufacturing aids; e.g., reticles, masks, masters, test samples, pattern generation tapes, etc., will be accomplished in accordance with the following criteria:

(1) Individual classified wafers, masks, reticles, masters, test samples, pattern generation tapes, etc., are accountable and must be controlled on a continuous receipt system from one manufacturing process to another and from one company to another. Each facility will maintain a control record to show the receipt or fabrication of a classified item and the disposition of such items to provide for an audit trail in each stage of fabrication. Lots, runs, etc., of classified material will be accompanied by a record which shows the description and quantity of the material, and bears the signature(s) of responsible person(s); e.g., shift chief, team leader production supervisor, etc.

(2) Less than full wafers (fragmented, cut) will be controlled as individual dies in accordance with Paragraph 58b(1), unless wafers are reconstructed on an

adhesive base. In this case, accountability resumes by wafer count and the records which show the number of dies removed. Contractors will attempt to determine the number of possible full dies in a wafer prior to dicing the wafer. If this cannot be accomplished, the number of full die must be established immediately after dicing the wafers. Less than a full die will be considered as classified scrap and controlled accordingly. The practice of sealing classified scrap in an envelope has proved to be an effective method for controlling the material.

(3) Any area in which the breakage of a classified wafer has occurred must be immediately safeguarded. Every effort must be made to reconstruct the broken wafer onto an adhesive base. If any chip or portion thereof cannot be accounted for, an insecurity report must be made as prescribed in Section XVI. If, however, the missing portion or the entire wafer has fragmented to such a degree that reconstruction is impossible, all particles will be removed from the breakage area by vacuuming. Once the area has been vacuumed, the bag will be marked with the wafer number or, where applicable, with the identification of the chip or portion thereof belonging to the wafer number, and its classification. The vacuum cleaner bag will be controlled as classified COMSEC material until its contents can be transported to NSA for destruction or destroyed locally by an NSA-approved destruction method. Other normally occurring waste (e.g., failures, partial die, etc.) which leave the manufacturing and assembly process shall also be controlled until approved destruction can be accomplished. These failures or breakages will be reflected in the in-process accounting records.

c. Destruction. Destruction of COMSEC equipment (including ICs and associated reticles, masks, masters, test samples, etc.) shall not be performed by the contractor unless the method or device to be used is approved by NSA. Contractors must ensure that the destruction methods selected meet Occupational Safety and Health Administration (OSHA) standards. When COMSEC material is to be destroyed by the contractor, it must be turned over to the COMSEC Custodian or Facility Security Officer. The responsible recipient will maintain a record of the material received for destruction and, when the material is destroyed, he/she shall prepare a local destruction record. The destruction of classified in-process accounting material must be performed by two appropriately cleared individuals. When material is to be forwarded to NSA for destruction, the material may be sent by the Facility Security Officer or the COMSEC Custodian via DCS to the National Security Agency, ATTN: Account 880099, Fort George G. Meade, MD 20755-6000, marked for destruction. This material must be forwarded, using a COMSEC Material Report (SF-153) with an in-process control number assigned (NOTE: Do not use a COMSEC account transaction number). COMSEC material sent for destruction should be identified by TSEC nomenclature, or part number when a nomenclature has not been assigned. When the contractor decides to send material to NSA for destruction, the following accounting and packaging procedures must be followed:

(1) All like items will be packaged in the same container, i.e., all reticles in one package, wafers in another, and ICs in another, etc.

(2) The container will be sealed.

(3) The container will be marked as to its exact contents, quantity, and classification.

(4) The Facility Security Officer or the COMSEC Custodian and witness will sign and date the transmittal receipt attesting to the accuracy of the information and the material being forwarded. The individuals signing the receipt are held totally responsible for ensuring that all material is properly packaged and the inventory is complete and accurate.

(5) Classified ICs which have already been mounted on printed circuit boards will be removed from the boards prior to return and the boards and ICs will be packaged separately.

(6) NSA Account 880099 will not accept material for destruction unless packaged according to the above procedures.

d. Subcontracting. When awarding subcontracts which will involve the fabrication of classified COMSEC material, prime contractors must require subcontractors to develop in-process accounting procedures and submit them to NSA through the prime contractor for approval. These procedures will be developed in accordance with the criteria outlined in Paragraph 58a., above, and must be submitted to NSA for review a minimum of 90 days prior to the start of fabrication of classified material. Prime contractors will require that subcontractors do not commence fabrication of classified materials until the applicable in-process accounting procedure has been reviewed and approved by the NSA COR. Prime contractors must ensure that the requirements for in-process accounting are specified in the subcontractor's Contract Security Classification Specification (DD 254).

59. Reconciliation of In-Process Accounting Records. Both the prime contractor and the subcontractor are required to reconcile their own in-process accounting records and to perform a record reconciliation between each other to ensure accountability for all items requiring such control. Reconciliation shall be effected at least semiannually and at the close of fabrication of a particular item. Records attesting to the accuracy of the reconciliation must be signed by the two individuals performing the reconciliations and will be retained for a minimum of three years. Randomly selected lots or batches of materials, as appropriate, will be tracked through the manufacturing process as part of the reconciliation effort. Any items which cannot be accounted for shall be immediately reported in accordance with procedures outlined in Section XVI.

60. Auditing of In-Process Accounting Records. Audits of prime and subcontractor's in-process accounting records will be conducted annually or as deemed necessary by NSA. The prime contractor will make provisions in the contract for NSA to audit the in-process accounting records of subcontractors. A written record indicating the results of the in-process accounting reconciliation conducted between the prime contractor and his subcontractor must be signed by the persons performing the reconciliation, retained for a minimum of three years, and made available to the Auditor during the annual COMSEC audit.

SECTION VIII. HANDLING AND CONTROL OF CLASSIFIED COMSEC
MANUALS DURING DEVELOPMENT

61. General: For purposes of positive control, incomplete manuscripts of classified COMSEC manuals generated by a contractor engaged in COMSEC contracts will be categorized as "In-Process Manuscripts." In lieu of entering such in-production material into the formal CMCS, contractors will control the material under internal in-process accounting systems. An in-process manuscript is a classified item, which, in any form (e.g., computer printout, artwork, mag card, mag tape, etc.) provides information relative to COMSEC design, operability, repair and maintenance, and is used as input to the publication of a TSEC-nomenclature document. An in-process manuscript will remain under in-process accounting controls until such time as it reaches a final state for publication or when the contracting activity has a requirement to release the unpublished manuscript to a field activity for training or evaluation. At this time, the manuscript will be brought into the formal CMCS as specified in paragraph 62.

a. Requirements: Prior to commencing development of classified manuscripts, the contractor shall prepare written in-process accounting procedures which provide specific instructions for the methods of control, prescribe the proper records to be maintained, and which provide for a complete audit trail for all portions and quantities of the manuscripts being produced. These procedures must be submitted to NSA for review and approval at least 90 days prior to commencing development of classified manuscripts.

b. Procedures: Technical writers involved in the development of COMSEC manuscripts will treat all drafted material as "working papers" ensuring that appropriate security controls are in place for the safeguarding of the COMSEC material according to classification and content. When automatic data processing equipment is used for this purpose, all security requirements prescribed in Section XIII of the ISM must be complied with. All working papers and/or hard-copy printouts held by the technical writers for a period of 30 days will, at that time, become accountable under the contractor's in-process accounting system. Once entered into the in-process accounting system, records must be maintained of their existence, location, quantity, and disposition. This will be a continuing process until all portions of the manuscript are developed and entered into in-process control.

c. Marking of In-Process Manuscripts. A special in-process manuscript cover will be made available by NSA to contractors engaged in controlled manuscript developments. The manuscript cover of the in-process manuscript must be marked with the manufacturing aid short title provided at the time the contract is issued (e.g., MAMM XXX, etc), the edition, copy number, classification, and the special marking "COMSEC MATERIAL--ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING A FINAL GOVERNMENT CLEARANCE." Internal pages will be marked in accordance with paragraph 11 of the ISM. Where the manuscript is in a media other than hard copy, the label will contain the identification "text" or "art", as appropriate, as well as the short title, edition, copy number, classification and the special marking described above.

d. Movement of In-Process Manuscripts. When it is necessary to release portions of the incomplete in-process manuscript to the contracting activity, or between subcontractor and prime contractor, the contractor's in-process records must reflect the number of pages comprising the initial release. The number of pages will also be annotated on the in-process manuscript cover. When the release is in a form other than hard copy, the label identifying the contents will also be annotated with the number of pages contained therein. In-process manuscripts released to the contracting activity or between prime and subcontractor will be covered with an SF-153 which will be assigned an "in-process" transaction number (NOTE: Do not use a COMSEC account transaction number), and a notation placed after the "NOTHING FOLLOWS" line indicating that the item is IN-PROCESS MATERIAL. Classified in-process manuscripts must be transported by the method prescribed in paragraph 55, or as specified by the cognizant U.S. Government Contracting Officer.

e. Destruction of In-Process Manuscripts. In-process manuscripts will be destroyed by the holding activity as soon as a requirement for the material no longer exists, utilizing the same method as is approved for other classified COMSEC paper products. Magnetic media may be declassified in accordance with Section XIII of the ISM. A notation of the destruction will be recorded in the in-process disposition records.

f. Subcontracting. When awarding a subcontract which will involve the development of a classified controlled manuscript, the prime contractor must require that the subcontractor develop in-process accounting procedures and will submit them on the subcontractor's behalf to NSA for approval. The prime contractor will ensure that the requirements for in-process accounting are specified in the contract with the subcontractor. In-process controlled material must not be released to, or developed by, the subcontractor until NSA has approved the procedures.

62. Entering Manuscripts into the COMSEC Material Control System (CMCS). When a manuscript has reached a final state for publication or the contracting activity has a requirement to release the unpublished manuscript to a field activity, the holding activity's COMSEC Custodian will prepare a possession report for the quantity of copies being held and/or a transfer report for the quantity being issued, annotating in the Remarks column of the SF-153 "New Material." The document must have a "Controlled Manuscript" cover attached, and the short title, edition, accounting number, number of pages, classification, and any special markings required, typed or stamped on the cover. Once entered into the CMCS, a controlled manuscript will remain in the system until destruction or final disposition and will be subject to the same accounting and physical controls pertaining to other comparable COMSEC material.

SECTION IX. HANDLING AND CONTROL OF CONTROLLED CRYPTOGRAPHIC ITEMS
DURING DEVELOPMENT AND MANUFACTURE/ASSEMBLY

63. Background and Scope.

a. Background. The concept of a Controlled Cryptographic Item (CCI) was introduced in March 1985 with the issuance of National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items." It was designed to facilitate the production, acquisition, and use of Communications Security (COMSEC) equipment. CCIs are endorsed by the NSA for use in telecommunications and automated information systems to secure classified as well as sensitive information. CCIs are so designated because they either embody classified cryptographic or other classified COMSEC designs, or because they perform critical COMSEC ancillary functions (e.g., certain key fill devices).

b. Scope. This section sets forth the Government requirements for the handling and control of CCIs which embody classified cryptographic or other classified COMSEC designs during their development and manufacture/assembly. These requirements do not apply to COMSEC ancillary devices designated CCI that do not embody classified COMSEC designs (e.g., certain key fill devices).

64. Requirements.

a. Development. Normally, all phases of development of the COMSEC functions for a CCI, including the fabrication of developmental models, will be classified. However, the fabrication of developmental models need not be classified if the controls set forth in this section are applicable and are applied. Exceptions will be handled on a case-by-case basis and must be approved by NSA. Handling and control of classified information must be in accordance with the ISM and this Supplement.

b. Embodiment of Classified COMSEC Functions. The embodiment of classified COMSEC functions in a CCI will afford protection to these functions as specified below:

(1) Hardware Embodiments. Unless it can be demonstrated that it is technically not feasible to do so, hardware embodiments of classified COMSEC functions will be in custom microcircuit form; i.e., embodiments composed of discrete components and/or standard microcircuits are not permitted. In addition, the microcircuit chips must be protectively coated by an NSA-approved process which will resist recovery of classified design information by reverse engineering, unless, as verified by the NSA Program Manager (PM), one of the following applies:

(a) The protective coating is incompatible with the microcircuit chip and the reduced effectiveness inherent with the use of the coating is unacceptable.

(b) The production contract for the microcircuit was in process as of 16 January 1987 and retroactive coating would jeopardize the

timely production or employment of the product to the extent that a waiver is warranted for the initial production requirement. Subsequent production requirements will include the coating unless additional waivers are obtained.

(c) Other equally protective measures have been adopted to resist reverse engineering.

(2) Firmware Embodiments. Firmware embodiments of classified COMSEC functions must be in microcircuit form (custom or standard) and must:

(a) Employ an irreversible security feature that prevents both readout and modification of the programmed information in the on-board memory from external, physically accessible pins; and

(b) The microcircuit chips must be protectively coated by an NSA-approved process which will resist attempts to defeat the security feature or to otherwise recover information in memory (e.g., by external probing). The requirement for protective coating may be waived when, as verified by the NSA PM, one of the following applies:

(1) The protective coating is incompatible with the microcircuit chip and the reduced effectiveness inherent with the use of the coating is unacceptable.

(2) The production contract for the microcircuit was in process as of 16 January 1987 and retroactive coating would jeopardize the timely production or employment of the product to the extent that a waiver is warranted for the initial production requirement. Subsequent production requirements will include the coating unless additional waivers are obtained.

(3) Other equally protective measures have been adopted to resist attempts to defeat the security feature or to otherwise recover information in memory (e.g., by external probing).

65. Manufacture and Assembly in Production. The manufacture and assembly of a CCI equipment in production may begin with either:

a. A classified design which goes through a transition during production and becomes a CCI component or assembly which the vendor further processes into a CCI equipment; or

b. A CCI component or assembly which the vendor receives from an authorized source and further processes the component or assembly into a CCI equipment.

The following paragraphs describe the handling and control requirements when the starting point is a classified design. They also cover the handling and control requirements when the starting point is a CCI component or assembly, or when the final manufactured product is a CCI component or assembly.

66. Transition from Classified to CCI. When the manufacture and assembly process begins with a classified design, the transition from classified to CCI will be as set forth below.

a. Hardware Embodiments. For hardware embodiments, the transition from classified to CCI will occur at the microcircuit photomask stage. Design automation by-products leading to and including the reticle for each layer of the microcircuit must be handled at the same classification level as the engineering drawings from which they were derived. The photomasks ultimately used as tooling in the actual production process, as well as the resulting semiconductor wafers and their subsequent forms (e.g., individual chips), leading to sealed devices, will be controlled as CCI material as set forth in this section.

b. Firmware Embodiments. For firmware embodiments, the transition from classified to CCI will occur after the classified design information has been entered into the microcircuit memory, and the security feature described in paragraph 64b(2) has been set. Thereafter, the microcircuits will be controlled as CCI material as set forth in this section. Software source data for firmware embodiments of classified design information remain classified and must be safeguarded in accordance with this Supplement.

67. Access.

a. Access to classified COMSEC information will be restricted in accordance with the provisions of this Supplement.

b. Access to CCI material will be restricted to U.S. citizens whose duties require such access. Non-U.S. citizens, including immigrant aliens, may be authorized access to CCIs and other unclassified COMSEC information and material in the manufacturing and assembly process only with the prior written approval of NSA. Such access will only be permitted when it is determined by NSA that adequate security protection exists.

68. In-Process Controls. Following the transition from classified to CCI as described in paragraph 66, CCI material must be controlled throughout the remainder of the manufacturing and assembly process as set forth in this section.

a. Microcircuit Devices. Photomasks and wafers will be marked "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI", and each must bear a serial number for accounting purposes. The marking and serial number must be legible with the naked eye. Photomasks and wafers will be accounted for by serial number: the photomasks until they are securely destroyed and the wafers until they are diced. After the wafers are diced, accounting for chips by quantity is sufficient. When the microcircuit is completely fabricated, if it is an end item for shipment, then accountability will be in accordance with paragraph 73. Otherwise, it is maintained in the vendor's in-process accounting system as it moves to the next level of assembly. Labeling of CCI components is covered in paragraph 77.

b. Printed Wiring Assemblies. A printed wiring assembly (PWA) assumes CCI status when a CCI microcircuit is installed on it. At that point, accountability for the microcircuit ceases and accountability for the PWA begins. This disposition of the microcircuit and accountability for the PWA must be reflected in the in-process accounting records. During further assembly, PWAs will be accounted for by quantity. When the PWA is completely

fabricated, if it is an end item for shipment, then accountability will be in accordance with paragraph 73. Otherwise, it is maintained in the vendor's in-process accounting system as it moves to the next level of assembly. Completely fabricated PWAs are accountable by quantity when they fit the definition of "CCI " component and by serial number when they fit the definition of "CCI assembly". (Refer to paragraph 77 for definitions of these terms.) Labeling of CCI components and assemblies is also covered in paragraph 77.

69. In-Process Procedures

a. Prior to commencing the manufacturing and assembly process for hardware embodiments, or the programming of microcircuits for firmware embodiments, the vendor must prepare detailed, written procedures to satisfy the in-process accounting requirements of this Section.

b. The procedures will provide for continuous tracking of each category of material (photomasks, wafers, microcircuit chips, finished microcircuits, printed wiring assemblies) as the material moves through the manufacturing and assembly process.

c. The accounting system must be capable of detecting a loss and identifying the work station at which the loss occurred as well as the individual(s) operating the work station at the time of the loss.

d. The procedures must provide specific instructions for the methods of control, the proper records to be maintained, and instructions for the reconciliation of in-process accounting records (refer to paragraph 76).

e. The procedures will identify the individuals or departments responsible for ensuring that the in-process accounting requirements are followed. Vendor employees which act in this capacity must be U.S. citizens.

f. The procedures must demonstrate that the vendor understands the accounting requirements.

g. Ninety days prior to start of production and implementation of the procedures, a draft must be forwarded to the NSA Project Manager for approval. Revision of the procedures require NSA approval prior to implementation. Production will not begin until NSA has approved the procedures.

h. Upon request, NSA will review the vendor's normal in-process accounting procedures for compliance with these requirements and provide guidance on adaptation of those procedures to meet NSA requirements.

70. Required Item Information. To be effective, the control system must track material in manageable units of production (e.g., lots, runs) that can each be uniquely identified in accounting records. The accounting records must indicate, as a minimum, the following information:

a. Date the material was introduced into the in-process accounting system within the facility.

b. Identification of the material to be controlled. This may be one or a combination of the following, as applicable:

- (1) Federal stock number.
- (2) NSA or Vendor part number.
- (3) NSA short title (trigraph).

c. Quantity, when accounting by quantity, or serial number if individual item accounting is required.

71. Breakage and Scrap. It is recommended that any area in which breakage of a CCI wafer has occurred be immediately safeguarded and every effort made to reconstruct the broken wafer onto an adhesive base. If, however, any portion, or the entire wafer, has fragmented to such a degree that reconstruction is impossible, it is recommended that all particles be removed from the breakage area by vacuuming. All materials under in-process accounting controls which leave the manufacturing and assembly process due to failure or breakage and normally occurring waste (e.g., broken wafer, partial die, etc.) must be controlled until securely destroyed as set forth in paragraph 74. In-process accounting records must reflect the failure or breakage.

72. Loss of In-Process Controlled Material. A reasonable search must be made for lost items which are under in-process accounting controls. All such losses must be documented in the vendor's records and must be reported to NSA (S213) within 24 hours of discovery of the loss. During normal duty hours, telephone (301) 688-6010. After normal duty hours, telephone the Senior Information Security Coordinator at (301) 688-7003. A written follow-up report shall be submitted within 30 days to NSA (S213). The written report shall include identification of the item involved, a description of the incident (when, where, and what happened; who discovered the loss; etc.), conclusions as to the cause, and actions taken to prevent future occurrence.

73. Transition from In-Process Controls to Control Within the Formal COMSEC Accounting System. Upon completion of the manufacturing and assembly process, CCI equipments, assemblies, and components which are destined for sale to authorized buyers will transition from in-process accounting controls into the formal COMSEC accounting system, and will be picked up in the vendor's COMSEC account. The transition will be reflected in the vendor's in-process accounting records. However, CCI components and assemblies produced by a subcontractor and provided to the vendor will not be entered into the formal COMSEC accounting system by the vendor. Instead, such material will be placed in the in-process accounting system by the vendor and controlled in accordance with this section. CCI equipments and assemblies will be accounted for by serial number; CCI components will be accounted for by quantity.

74. Destruction of CCI Materials. All material designated CCI which leaves the manufacturing and assembly process due to unserviceability (e.g., faulty photomask), breakage/reject (e.g., broken/reject wafer, failed microcircuit), or normally occurring waste (e.g., partial die) must be securely destroyed. Secure destruction is best accomplished by high-temperature incineration (MOS

microcircuit materials require temperature on the order of 3,000 degrees F). NSA has the capability for high-volume destruction of these materials, and it is preferred that the material be forwarded to NSA for destruction. Alternatively, the vendor may elect to destroy the material locally. To do so requires the written permission of the NSA PM. Vendor requests to destroy the material locally must include a detailed description of the proposed process to be employed.

a. Destruction by the Vendor. Where material under in-process accounting controls is to be destroyed by the vendor, the material will be turned over to a U.S. citizen employee who has been designated to be responsible for the destruction operation. This person must maintain a record of the materials received for destruction. The actual destruction of all such material must be witnessed by one other designated individual who must also be a U.S. citizen. Both the person responsible for destruction and the witness will sign a local destruction record attesting to the destruction of the recorded material. Destruction records must be retained by the vendor for a minimum of two years.

b. Destruction by NSA. Where material under in-process accounting controls is to be forwarded to NSA for destruction, all like items will be packaged together (e.g., photomasks in one package, wafers in another, PWAs in another, etc.). A transmittal (SF-153) with an in-process transaction number (NOTE: Do not use a COMSEC account transaction number) will be included in each container. The transmittal will include a statement that the listed material is for destruction. Items must be identified sufficiently to allow crosschecking against the transmittal. The transmittal will be signed by two U.S.-citizen employees, designated to be responsible for this function, attesting to the accuracy of the inventory and the proper packaging of all material forwarded to NSA for destruction. The container must be securely sealed and labeled with the following address:

Director
National Security Agency
Operations Building No.3
ATTN: Y133
Fort George G. Meade, MD 20755-6000

75. Subcontracting. When awarding a subcontract which will involve the manufacture or assembly, or other handling, of CCI materials which are subject to in-process controls, the prime contractor must require that the subcontractor develop in-process accounting procedures and will submit them on the subcontractor's behalf to NSA for approval. The prime contractor will ensure that the requirements for in-process accounting, as well as all other applicable requirements as set forth in this section, are specified in the contract with the subcontractor. In-process controlled material must not be released to, or produced by, the subcontractor until NSA has approved the procedures.

76. Reconciliation of In-Process Accounting Records. Both vendor and subcontractor are required to reconcile their own in-process accounting records and to perform a records reconciliation between each other to ensure accountability for all in-process controlled material. Reconciliation must

be effected at least semiannually and at the conclusion of all work on a particular item. Any shortage discovered as a result of the records reconciliation process must be documented in the vendor's records and is reportable as loss in accordance with paragraph 72. The individuals performing the reconciliation must be U.S. citizens and records attesting to the accuracy of the reconciliation will be signed by them. These records must be retained by the vendor for a minimum of two years.

77. Labeling of Components, Assemblies, and Equipments. CCI components, assemblies, and equipments will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI" in accordance with standard drawings available from NSA and the following:

a. CCI components 1/ will be labeled "CCI" at the same time as other part-specific nomenclature is applied.

b. CCI assemblies 2/ will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" (space permitting) or "CCI" otherwise. CCI assemblies will also bear a government serial number (GSN) for accounting purposes, in accordance with the criteria to be furnished by NSA. Labeling may be applied at any stage of the assembly process, but must be applied by the end of the assembly process. CCI controls applicable to the assembly need not take effect until a CCI component is installed.

c. CCI equipments 3/ will be labeled "CONTROLLED CRYPTOGRAPHIC ITEM" in a conspicuous external location. CCI equipments will also bear a GSN for accounting purposes, in accordance with criteria to be furnished by NSA. Labeling may be applied at any stage of the assembly process, but must be applied by the end of the assembly process. CCI controls applicable to the equipment need not take effect until a CCI component or assembly is installed.

1/ A CCI component is a device which embodies a cryptographic logic, or other COMSEC design, approved by NSA for designation as a CCI, where the device does not perform the entire COMSEC function and is dependent upon the host equipment or assembly to complete the COMSEC function as well as to operate.

2/ A CCI assembly is a device which embodies a cryptographic logic, or other COMSEC design, approved by NSA for designation as a CCI, where the device performs the entire COMSEC function but is dependent upon the host equipment to operate.

3/ A CCI equipment is a telecommuunications or information handling equipment which embodies a CCI-designated component or assembly and which performs the entire COMSEC function without dependence on a host equipment to operate.

78. Auditing of In-Process Accounting Records. Audits of vendor and subcontractor in-process accounting records will be conducted by NSA annually or as deemed necessary. The vendor must make provisions in the contract for NSA to audit the in-process accounting records of subcontractors. Written records indicating the results of the in-process accounting reconciliations at the vendor or between the vendor and its subcontractor, as well as documentation of lost, broken, scrap, or destroyed CCI material, must be made available to NSA during audits.

SECTION X. KEYING MATERIAL MANAGEMENT

79. General. This section is applicable to those contractors who purchase CCI equipment and it only addresses what is termed "hard copy" key, i.e., physical keying material such as printed key lists, punched key tapes, punched key cards, etc. "Soft key" in electronic form is often employed in newer cryptographic equipments for key updating and similar functions, and is addressed in the operating instructions for the particular equipment.

80. Keying Material Source. Keying material for CCI equipment is produced by, and provided by the Government. When CCI equipment is acquired, it is used to protect information in a communications net which, from a cryptographic point of view, is known as a "cryptonet." CCI equipments operating in a single cryptonet must have compatible keying material to be able to correctly encrypt and decrypt communications. In order to manage the establishment of a cryptonet, and to ensure the provision of the correct keying materials to the proper members of the cryptonet, one party associated with the cryptonet is designated as the "Controlling Authority."

81. Designation of the Controlling Authority. Controlling authorities should be designated primarily on the basis of their ability to perform their responsibilities. A controlling authority must be a member of the cryptonet and have some seniority or authority over the other members of the cryptonet. A controlling authority must have a means of communicating with cryptonet members (preferably multiple means) and with interested parties who may not be members of the cryptonet (e.g., Government contracting officers), and must be in a position to monitor the status of the cryptonet, i.e., to identify problems, or receive adequate information about net problems. The contractor who purchases the cryptographic equipment may work with the vendor, his Government contracting officer(s), or with the NSA (Y1) in proposing a controlling authority for the new cryptonet. The following guidance for the designation of a controlling authority is provided:

a. If there is a single Government Contracting Office involved, or if there is an identifiable lead Service/Department/Agency, the Contracting Officer, following his Department or Agency's procedures, may designate who the controlling authority will be.

b. If there are multiple Government Contracting Offices involved with no identifiable lead service, then the contractor will coordinate with each of them and propose a controlling authority designation to NSA (Y1).

c. It is the purchasing contractor's responsibility to ensure that a controlling authority designation proposal is made to NSA (Y1) early in the process of establishing a cryptonet, as this is the first step in obtaining the keying material necessary for cryptonet operation. The proposal can be developed by the leading Government Contracting Officer, by the purchasing contractor, or by the vendor, but it remains the responsibility of the purchasing contractor to ensure that the proposal is made to NSA (Y1).

d. All proposed designations of controlling authorities are subject to review by NSA (Y1).

For existing cryptonets which are significantly modified or expanded by the addition of new members, the current controlling authority must revalidate his role. This should be accomplished through existing Department and Agency regulations and procedures, if applicable, or directly to NSA (Y1). Although in most cases the designation of the controlling authority will not change, there may be some net membership changes for which redesignation of the controlling authority becomes practical. If there is any difficulty, confusion, or dispute involved in the selection of a controlling authority, and it cannot be resolved in coordination with the lead Government Agency, the problem should be referred to NSA (Y1).

82. Responsibilities of the Controlling Authority. The controlling authority for a cryptonet has responsibilities which fall into three broad categories: cryptonet management, logistics, and security. The responsibilities of the controlling authority include:

a. Cryptonet Management:

- (1) Establishing a cryptonet by designating cryptonet members.
- (2) Specifying the status of the keying material, to include the date on which the first edition will become effective, the effective dates for remaining material; and keeping all cryptonet members informed of this information. (NOTE: For classified keying material, the effective dates are classified CONFIDENTIAL.)
- (3) Specifying the key change time for the cryptonet.
- (4) Authorizing local reproduction of copies of keying material controlled by the controlling authority in situations where established cryptologic channels cannot supply the material in time to meet urgent, unprogrammed, operational requirements; and ensuring that the reproduced material is properly controlled and destroyed in the same manner as the original material.
- (5) Reporting to NSA (Y1 and S042) incidents of faulty keying material or the unauthorized transmission of keying information.
- (6) Ensuring that COMSEC insecurity reporting instructions are disseminated to all cryptonet members (with special emphasis on how and where to send insecurity reports to the controlling authority).
- (7) Ensuring that prescribed allowances of on-hand keying materials at cryptonet member locations are adequate for potential emergency supersessions.
- (8) Conducting annual reviews to confirm that there is a continuing requirement for the cryptonet keying material, including the quantity, quality, and operational effectiveness of that material. This review will normally be conducted as an annual update of the Keying material Support Plan (KMS²) described in paragraph 84.

b. Logistics:

(1) Notifying NSA (Y1) of any changes in the membership of the cryptonet and of any changes in the quantity of material each member is to receive.

(2) Notifying NSA (Y1) of any changes in the effective dates and key change times of cryptonet keying material.

c. Security (see also Section XVI, COMSEC Insecurity Reporting Requirements):

(1) Evaluating the security impact of reports of physical insecurities of superseded, effective, and future cryptonet keying materials; and making a determination as to whether or not a compromise of the material has occurred.

(2) Notifying appropriate Government authorities, cryptonet members, and NSA (S21) of the results of the evaluation.

(3) Directing emergency supersession of keying material; taking other appropriate actions in response to actual or suspected compromises (see Appendix 1 this Supplement).

(4) Ensuring that NSA (S21) and other appropriate Government authorities are notified of all incidents of suspected theft, subversion, espionage, defection, tampering, or sabotage affecting COMSEC materials.

(5) Directing emergency extensions of keying material cryptoperiods up to 24 hours (unless the specific cryptosystem doctrine prohibits such an extension or authorizes a longer period), and notifying NSA (S21) of this action.

83. Considerations in Establishing a Cryptonet. To fulfill its prescribed duties effectively, the controlling authority requires accurate information on all aspects of the cryptonet, and must have the capability to communicate with all cryptonet members. In particular, the controlling authority should be familiar with all aspects of the handling of keying material in his cryptonet, and with the most expeditious ways of promulgating supersession and other emergency information to all holders of the keying material. Some of the specific items to consider in establishing a cryptonet include the following:

a. The effective key change times should be as convenient as possible for all members of the cryptonet. A knowledge of the net operations at member locations, across different time zones, is helpful in picking an optimum key change time.

b. For security reasons, cryptonet size should be kept as small as possible. A goal should be to limit the number of people who have access to the key to the absolute minimum.

c. The date and time of key changes must be uniform throughout the cryptonet.

d. Cryptologistics should be carefully considered. How will the keying material get to each member of the cryptonet? Should new COMSEC accounts or subaccounts be established? Should existing accounts be closed down?

e. The availability of information for the controlling authority, and how it will reach the controlling authority are important points. In order to properly perform, the controlling authority must know the current status of the cryptonet.

f. Operational interoperability requirements may dictate cryptographic netting and subnetting schemes.

g. The quantity, sensitivity and classification (if applicable) of the information to be transmitted over the cryptonet must be considered in the determination of the classification of the keying material.

84. Keying Material Support Plan (KMSP). A primary responsibility of the controlling authority is the preparation of the "Keying Material Support Plan" or KMSP, which establishes how keying material will be provided to the cryptonet during its operational lifetime. Authorized vendors are required under their Memorandum of Agreement with NSA to offer assistance in the preparation of the KMSP, although the controlling authority may elect to prepare the KMSP unassisted, or use the COMSEC vendor's or the Government's assistance through the lead Contracting Officer.

If a Government entity is the controlling authority, it will prepare the KMSP in accordance with its department or agency procedures. The KMSP should be filed with NSA (Y1) to allow adequate lead time for the production and distribution of the right amounts of keying material. For planning purposes, a minimum of 120 days is required from the time NSA receives an order for keying material until it is produced and shipped from NSA. The KMSP will be submitted to NSA (Y1) for review and approval as follows:

a. If a contractor is the controlling authority and there is a lead service, department, or agency, the contractor will submit the KMSP through its appropriate contracting officer, who will forward the KMSP via department or agency channels or, if appropriate, directly to NSA (Y1).

b. If a Government entity is the controlling authority, it will submit the KMSP in accordance with department or agency procedures, and forward it to NSA (Y1).

c. If a contractor is the controlling authority and there is no lead service, department or agency, it will submit the KMSP directly to NSA (Y1).

85. Contents of the Keying material Support Plan. The KMSP must contain adequately detailed information about the cryptonet so that NSA can produce and provide the correct types and amounts of keying materials to the right place at the right time. There must also be enough information so that NSA can ensure that security concerns are addressed, e.g., making sure that no SECRET keying material is sent to an account authorized to hold only CONFIDENTIAL materials. The following are the specific topics which must be addressed in a KMSP:

a. The Operational Need: Brief statement of the need for the cryptonet, i.e., the Government contracts and types of information involved. Specify classification and/or sensitivity of the information.

b. The Operational Concept: Statement on the operational structure of the net; days/times of operation; identification of net control and alternates, as well as subnetting.

c. Controlling Authority: Identifying the cryptonet controlling authority, including names of points-of-contact, complete address information, and telephone numbers.

d. Contracting Office(s): Identity of the Government contracting office or offices served by or associated with the cryptonet; names, addresses and telephone numbers of contracting officers.

e. Keying Material Specification: The following information on the keying material which is needed for the operation of the cryptonet:

(1) Identity of cryptographic equipment (and fill devices) which will use the keying material.

(2) Use of keying material: operational; maintenance; training.

(3) Quantity required (copy counts). Also identify editions if there are special circumstances.

(4) Date required initial operational capability.

(5) Classification (or specify UNCLASSIFIED).

f. The Distribution Plan: Description of the keying materials to be shipped, identifying the originator (normally NSA) and the receiver. A block diagram of the shipping paths from NSA to the material's final destination should be included (it need only address the major points of accounting transfers). It must provide complete COMSEC account information for all major modes in the distribution plan. The distribution plan must identify any primary COMSEC accounts which will receive materials in bulk shipments from NSA, and identify any subaccounts which will not be serviced by their primary accounts. The distribution plan must also address how the keying materials will be distributed from the COMSEC accounts to the actual users.

g. Other Information: Any additional information which the controlling authority feels is significant, or is unique to his particular cryptonet or keying material.

86. Annual Reviews of Keying Material. The controlling authority is required to review the adequacy and currency of the KMSP annually, and provide any changes in writing to NSA (Y1) no later than 1 July of each year. Written negative reports (i.e., the review indicates that no changes are necessary to the current KMSP) are required. Particular points to be addressed in the annual KMSP review include the following:

- a. Changes in cryptonet membership.
- b. Changes in addresses, names of contacts, and telephone numbers.
- c. Changes in the classification or sensitivity of the information being communicated on the net.
- d. Any changes in the quantity of materials distributed. Controlling authorities must ensure that COMSEC accounts have enough material on hand for regular and emergency supersessions, but not too much material (which negatively affects security, storage, bookkeeping, etc.).
 - (1) User COMSEC account inventories should generally not exceed four months' total supply of monthly superseded material, including effective material.
 - (2) A minimum of one back-up edition of keying material must be held at the user COMSEC account regardless of the normal cryptoperiod length.
- e. Any planned changes or cancellations of requirements.

SECTION XI. PHYSICAL SECURITY

87. General. COMSEC material may require different levels of physical security under different conditions. TOP SECRET keying material is our nation's most sensitive keying material, since it is used to protect the most sensitive U.S. national security information and its loss to an adversary can subject to compromise all of the information protected by the key. For this reason, TOP SECRET keying material is afforded the special protection of two-person integrity (TPI)/no-lone zone (NLZ) controls. Any violation of the TPI/NLZ requirements specified herein is reportable as an insecurity in accordance with Section XVI., Paragraph 113.c. Waivers to the requirements for the control of TOP SECRET keying material may be requested; however, maintenance of a strong national COMSEC posture dictates that such waivers be granted on a case-by-case basis only when a genuine hardship exists. Where NSA is the COR, written requests for waivers should be directed through the Contracting Officer's Technical Representative (COTR) to Director, NSA, ATTN: S042. For contractors who are supported by another COR, requests for waivers should be directed through the appropriate COTR to the COMSEC authority of the user agency involved. The required physical controls pertinent to the specific circumstances are outlined in this Section.

88. Closed Area Designation and Access Controls.

a. A contractor must establish a Closed Area as prescribed in Section IV of the ISM, when the following conditions exist:

(1) There is a contractual requirement to design, analyze, fabricate, test or repair classified cryptographic systems; or to manufacture and/or work on keying materials designated CRYPTO. If the keying material is TOP SECRET, the required no-lone zone controls must also be instituted. These areas must be physically separated from other classified and unclassified project areas. 1/

(2) Open storage of classified COMSEC material is required due to its size or volume.

(3) Operational classified crypto-equipment is keyed and unattended.

(4) Operational CCI crypto-equipment is keyed with classified key and unattended.

NOTE: Where the operational classified or CCI equipment is contained within a special NSA-certified Class 5 security cabinet modified for such application (Such containers may be identified by labels placed in prominent positions inside the containers stating "Modified GSA-Approved Class 5 Security

1/ When it is essential in the performance of a contract to remove temporarily such material from a Closed Area, the material must be kept under the constant surveillance of an authorized person who is in a physical position to exercise direct security control over the material. The material must be returned to the controlled area prior to the close of business.

Container certified by NSA for the secure storage/closed-door operation of COMSEC equipment.") the unit need not be housed in a closed area, provided the supplemental controls specified in Section IV of the ISM are adhered to and the operational keying material in use is classified SECRET or below.

b. In addition to the above, the following requirements with respect to a Closed Area must be observed:

(1) The entrance must be arranged such that persons seeking entry can be identified and prevented from viewing the activities within the area before being permitted to enter.

(2) The door leading to the area must have a sign on the outside designating it a "Closed Area", but there shall be no indication that COMSEC activities are conducted therein. A security checklist will be placed on the inside of the door showing the date, time and name of the person who unlocked, locked and checked the area. During nonworking hours, the area must be protected as required in paragraph 34a(3) of the ISM.

(3) During working hours, entrance to the area must be controlled as prescribed in the ISM. When guards are used to control admittance, they must possess an appropriate security clearance and will be given a COMSEC briefing if access as set forth below is involved.

(4) An access list, authenticated by the Facility Security Officer, COMSEC Custodian or Alternate COMSEC Custodian must be prepared and conspicuously displayed within and near the entrance to the Closed Area. The list will indicate with an asterisk or other easily identifiable means, the names of the responsible persons designated to authorize escorted entry of other contractor personnel or authorized visitors. If guards are used during working hours to supervise admittance, the list may be held by the guard controlling entrance to the area.

(5) A visitor's register must be maintained inside the area. All persons other than those named on the access list will be required to identify themselves and register when entering and leaving the area. All classified COMSEC material will be concealed from view when visual access is a factor. Visitors permitted in the area will be escorted by an authorized and appropriately cleared person at all times while in the controlled area.

(6) The contractor must not permit the following devices within a Closed Area, unless the use of such devices is required in contract performance:

(a) Cameras, photographic devices/equipment capable of receiving and recording intelligible images.

(b) Sound recording devices/equipments, including magnetic tapes or magnetic wire.

(c) Amplifiers and speakers

(d) Radio transmitting and receiving equipment.

(e) Microphones.

(f) Television receivers.

89. CCI Access Controls.

a. CCI equipment is by definition unclassified, but controlled. Minimum controls for CCI equipment are prescribed under three different conditions: unkeyed, keyed with unclassified key, and keyed with classified key. The provisions apply to CCI equipment which is installed for operational use. Storage requirements for uninstalled CCI equipment are covered in paragraph 90.

(1) Installed and unkeyed: The CCI equipment must be treated as high value property. The contractor is responsible for providing procedural and/or physical controls adequate to prevent unauthorized removal of the CCI equipment or its CCI components. Where it is practical, rooms containing unkeyed CCI equipment should be locked at the end of the work day.

(2) Installed and keyed with unclassified key:

(a) Attended: The contractor is responsible for preventing access by unauthorized personnel through the use of physical controls and/or monitoring access with authorized personnel.

(b) Unattended: The contractor is responsible for preventing access by unauthorized personnel through the use of adequate physical controls (e.g., locked rooms, alarms, or random checks, etc.).

(3) Installed and keyed with classified key:

(a) Attended: CCI equipment must be under the continuous positive control of contractor personnel who possess a security clearance at least equal to the classification level of the keying material in use, and, if the keying material is TOP SECRET, the NLZ controls must be instituted. User locations where equipment holds TOP SECRET key in key-card form or has mechanical permuters will be operated as no-lone zones (i.e., space in which at least two appropriately cleared individuals must be present). However, NSA has approved a double-padlock hasp which can be installed on card readers or the KW-7 cabinet face to obviate NLZ manning for such locations. No-lone zones are not required when the key is resident in the crypto-equipment in electronic form, or where the crypto-equipment has been modified to preclude access by a lone individual to the hard copy key contained therein. However, two-person integrity controls shall always apply to initial keying and rekeying operations.

(b) Unattended: CCI equipment must be in a Closed Area (refer to paragraph 88, above).

90. STORAGE REQUIREMENTS: A contractor will not be eligible to receive or generate classified COMSEC information until adequate storage has been established at the facility. Storage of TOP SECRET key must meet the requirements of paragraph 90b(1), below.

AD-A270 027

COSMEC SUPPLEMENT TO INDUSTRIAL SECURITY MANUAL FOR
SAFEGUARDING CLASSIFIED INFORMATION(U) DEPARTMENT OF
DEFENSE WASHINGTON DC 17 MAR 88 DODD-5220.22-5

2/2

UNCLASSIFIED

XD-WHS/DD

NL

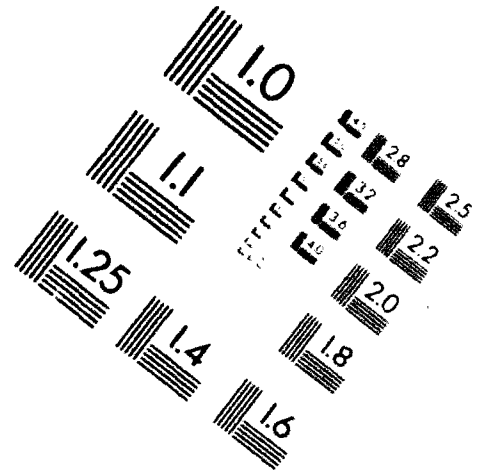
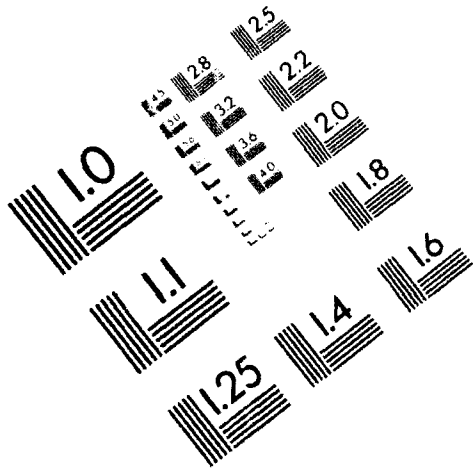
END FILMED DTIC



AIM

Association for Information and Image Management

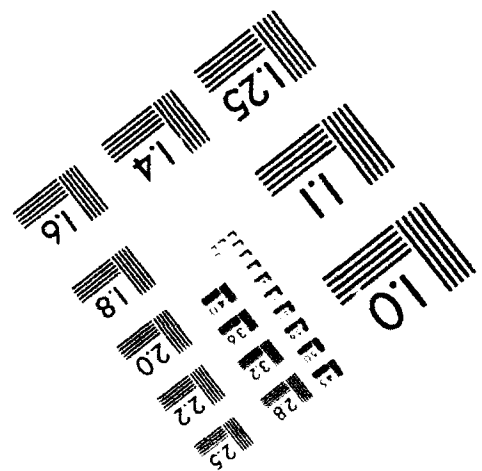
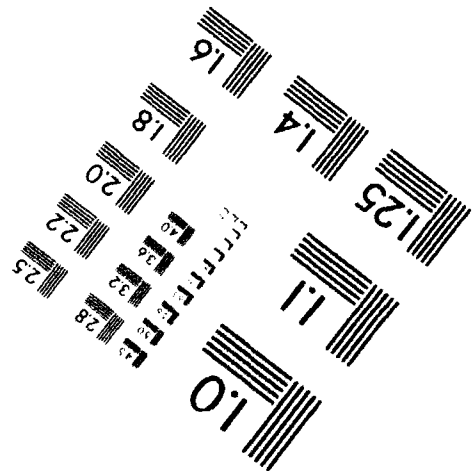
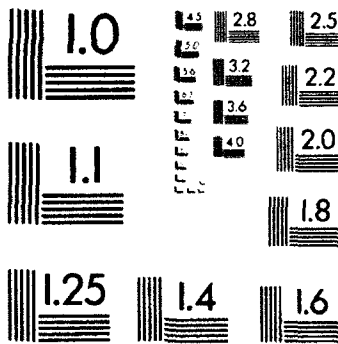
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202



Centimeter



Inches



MANUFACTURED TO AIM STANDARDS
BY APPLIED IMAGE, INC.

a. Classified COMSEC Equipment and Information. Classified COMSEC equipment and information other than keying material marked CRYPTO must be stored as prescribed in the ISM for other classified material at the same classification level.

b. Keying Material Marked CRYPTO. Secure storage for keying material marked CRYPTO must be as follows:

(1) TOP SECRET keying material must be stored under two-person (TPI) controls employing two different approved combination locks, with no one person authorized access to both combinations. Storage can be in a special access control container(s) (SACC) which is secured inside a GSA-Approved security container; in a GSA-Approved security container within a Class A vault as prescribed in the ISM or a modular vault composed of panels constructed and certified in accordance with UL standard 608 (M rating or higher); or in a GSA-Approved security container with two built-in combination locks on the master drawer. At least one of the combination locks must be built-in, as in a vault door or in a security container drawer. In addition, supplemental controls as outlined in paragraph 14a(2), ISM, are required.

(2) SECRET keying material may be stored in the same manner as TOP SECRET keying material; or in a steel security file cabinet originally procured from the GSA Federal Supply Schedule; or a Class B vault as prescribed in the ISM. In addition, supplemental controls as outlined in paragraph 14a(4), ISM, are required.

(3) CONFIDENTIAL keying material may be stored in the same manner as TOP SECRET or SECRET keying material; or in a file cabinet having an integral automatic locking mechanism and a built-in, three position, dial type, changeable combination lock; or in a Class C vault as prescribed in the ISM. However, CONFIDENTIAL keying material may be stored in a steel file cabinet equipped with a steel bar and a three-position, dial-type, changeable combination padlock provided the supplemental controls as outlined in paragraph 14a(4), ISM, are in effect.

(4) UNCLASSIFIED keying material may be stored in the same manner as TOP SECRET, SECRET, or CONFIDENTIAL keying material; or in the most secure manner available to the user.

In those exceptional cases when the nature, size, or unique characteristics of the material make it impractical to store as above, the contractor shall safeguard it by control of the area as outlined in paragraph 88, above.

c. CCI Equipment. CCI equipment must never be stored in a keyed condition. Prior to placing CCI equipment in storage, all keying material must be removed, and internal key storage registers zeroized. When unkeyed, CCI equipment must be protected against unauthorized removal or theft during storage (e.g., placed in a locked room, or a room with an adequate alarm system).

91. Record of Individuals Having Knowledge of the Combinations to Containers Storing Classified COMSEC Material. A record must be maintained of the names, addresses, and home telephone numbers of persons having knowledge of

the combination to containers in which classified COMSEC material is stored. In the event of an emergency; e.g., the container or vault is found open after normal working hours, the container must be kept under surveillance and at least one of these individuals will be notified immediately. Normally these containers are under the direct control of the COMSEC Custodian and Alternate COMSEC Custodian; however, where operational need necessitates, classified COMSEC material - to include one edition of current keying material marked CRYPTO - may be issued to a user. Under these circumstances, the notified individual must also contact either the COMSEC Custodian or Alternate COMSEC Custodian. Upon arrival of the summoned individual(s), an inventory of the contents of the container will be immediately undertaken. Upon completion of the inventory, the container combination must be changed and the container locked. The COMSEC Custodian/Alternate COMSEC Custodian will then compare the results of the inventory against the account's COMSEC Register File and, if any material is determined to be missing, this information will be included in the report made in accordance with the provisions of Section XVI.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION XII. PROTECTION OF LOCK COMBINATIONS FOR VAULTS AND
CONTAINERS UNDER THE DIRECT CONTROL OF THE
COMSEC CUSTODIAN/ALTERNATE COMSEC CUSTODIAN

92. General. The provisions of this Section apply to combination locks for containers and vaults under the direct control of the COMSEC Custodian and Alternate COMSEC Custodian. It is not intended to apply to combination locks for containers storing classified COMSEC material issued to a user. Once COMSEC material is issued on hand receipt to a user, the user becomes responsible for the material and the container storing such material is considered to be under the user's direct control.

a. Selection of Combinations. Each lock must have a combination composed of randomly selected numbers. This combination will not deliberately duplicate a combination selected for another lock within the facility and not be composed of successive numbers in a systematic sequence, nor predictable sequence (e.g., birthdates, social security numbers, and phone numbers).

b. Changing Combinations. Lock combinations as outlined above will only be changed by the COMSEC Custodian or Alternate COMSEC Custodian. Combinations must be changed:

(1) When the lock is initially placed in use. (The manufacturer's preset combination must not be used.)

(2) When any person having authorized knowledge of the combination no longer requires such knowledge (e.g., through transfer or loss of clearance).

(3) When the possibility exists that the combination has been subjected to compromise.

(4) At least annually, except for those containers storing keying material marked CRYPTO, the combination to which shall be changed once each six months.

(NOTE: It is specifically prohibited for individuals to record and carry, or store insecurely for personal convenience, the combination to areas or containers in which COMSEC material is stored. Also, records of such combinations may not be stored in electronic form in a computer).

c. Classification of Combinations. Lock combinations must be classified the same as the highest classification of the information protected by the locks. For a security container, this is the highest classification of the information held in the container; for a vault door, it is the highest classification of the information held in the vault, including that information stored in containers.

d. Record of Combinations. Each combination must be recorded on a separate record card and each card then placed in a separate envelope, properly marked as described below and sealed. The face of the envelope must be stamped with the highest classification of the information protected

by the combination and annotated with the identification number of the container to which it applies. The date of the combination change will also be recorded on the envelope. Each lock combination used to protect TOP SECRET keying material must be recorded separately and protectively packaged to prevent undetected, unauthorized access to the combination (refer to Paragraph 93, below). Each records-of-combination envelope will be identified by the nomenclature COMBO-1 and will be controlled in the CMCS by quantity (ALC-2). For instance, if there is only one container under the direct control of the COMSEC Custodian, then a quantity of one COMBO-1 will be entered into the COMSEC account; however, if there are six different containers under the COMSEC Custodian's direct control, and, therefore, six different record-of-combination envelopes, then a quantity of six COMBO-1s will be entered into the COMSEC account. Once the COMSEC Custodian has recorded the appropriate number of COMBO-1s, he/she will submit a possession report to the COR, identifying the quantity of COMBO-1s entered into the COMSEC Account. When a combination is changed, the record card must be updated and the date of the change annotated on the record-of-combination envelope, but the nomenclature identification will remain unchanged. The record-of-combination envelopes must be secured in a container approved for storage at the level of the information protected by the locks and such container must be under the direct control of the COMSEC Custodian and Alternate Custodian. The combination to this central container will be committed to memory by the COMSEC Custodian and Alternate Custodian.

93. Protective Packaging of Lock Combinations. To provide for ready access to secured material in emergencies, the lock combination of the central container will be recorded on a separate record card, placed in a separate envelope, properly identified and appropriately classified, sealed and protectively packaged. This record-of-combination card will be hand-receipted to the FSO, who will store it in a container approved for the classification level identified on the envelope. The container must be under the direct control of the FSO. Guidance for one method of protective packaging is provided, as follows:

a. Protective Packaging Techniques. Lock combination record cards may be protectively packaged by covering the record card front and back with aluminum foil, placing it in the record-of-combination envelope (refer to paragraph 92), sealing the envelope, then heat sealing the envelope between two sheets of plastic laminating material.

(1) Materials Required. Protective packaging as set forth above requires the following material:

(a) A standard opaque envelope with a gummed flap and of a suitable size to accommodate the record card.

(b) Aluminum foil (the standard household type is adequate).

(c) Transparent plastic laminating material. This material should be specifically imprinted with a distinctive design, lettering, or logo type to deter attempted penetration. (If stock laminating material is used, it may be possible for an unauthorized person to penetrate the plastic laminate, gain access to the combination, then relaminate the envelope,

possibly without detection.) The special, imprinted plastic material should be carefully controlled during production, distribution, storage, and use to prevent pilfering or duplication by persons seeking to penetrate the protective packaging.

(d) Standard heat-sealing equipment for laminating the plastic.

(2) Packaging procedures.

(a) Cover the record card front and back with aluminum foil. This will lessen the possibility of sophisticated optical penetration.

(b) Place the aluminum-covered record card in the opaque envelope and seal the envelope. Enter on the face of the envelope the information specified in paragraph 92. These entries must be made in ink to lessen the possibility of alteration.

(c) Heat seal the envelope between two sheets of plastic laminating material. Where special imprinted laminating material is used, any scraps bearing the special imprint should be treated as classified waste.

94. Periodic Inspection and Superseded Combination.

a. The protective packaging described in this section provides an added degree of protection, but is not penetration proof. It is recommended, therefore, that the package be inspected monthly. This inspection should include a close visual examination of the entries on the face of the envelope to ensure that they are authentic, and an inspection of all plastic surfaces, including the four edges of the package. This may reveal actual or attempted penetration of the protective packaging.

b. When a protectively packaged combination has been superseded, the package will be opened and inspected on the inside. This is accomplished by making two diagonal cuts, forming an "X" from corner to corner, through the plastic and front of the envelope with an X-Acto knife or similar cutting tool. This allows the package to be opened completely, exposing all inside surfaces for inspection. If a penetration of the package occurred, it will be revealed under close inspection at this time.

THIS PAGE INTENTIONALLY LEFT BLANK

Section XIII. Displays, Demonstrations, and Marketing of CCI Equipment

95. General. The open or public display of CCI equipment (keyed or unkeyed) at conferences, symposia, meetings, open houses, etc., outside the United States is forbidden. This prohibition includes discussion, publication, or presentation of information concerning equipment.

96. Requirements. CCI equipment which is demonstrated at conferences, symposia, meetings, open houses, etc., or publicly marketed within the United States must be provided physical controls adequate to limit viewing and demonstration to U.S. citizens only.

a. When possible, the clearance or registration procedures for the conference will be used to determine U.S. citizenship prior to providing visual access to or demonstrations of CCI equipment.

b. Where it is impossible to verify U.S. citizenship using regular conference procedures, the following will apply:

(1) Access to the demonstration of CCI equipment will be limited to those individuals who state that they are U.S. citizens by completing and signing a form that indicates country of citizenship, full name, social security number, and the name, address and telephone number of the company or agency the individual represents. This form will also contain a Privacy Act Statement to be read and signed by the individual. In addition, the individual must present identification which verifies his name and signature. Subsequent to the demonstration, but within 30 days, the vendor must verify the information provided on citizenship, etc., with the company represented by the individual who filled out the form. Any discrepancies which are detected will be reported immediately to NSA, ATTN: S213.

(2) Visual access and demonstrations of the equipment will be conducted in a room separate from the general conference area, and which has a controlled entrance to ensure that unauthorized individuals do not hear or see the demonstration. The demonstration will be conducted at the unclassified level.

(3) Vendors must not disclose any classified characteristics of the CCI equipment, nor provide photographs, diagrams, or schematics of the inside of the equipment.

c. Recognizing that certain information needs to be available to potential purchasers of CCI equipment early in the vendor's marketing program (i.e., before the purchaser's U.S. citizenship and Government contract status have been established, as for example, at a large convention or exposition), the following information may be provided to the two groups indicated below, but only under the following circumstances:

(1) Group 1: Potential purchasers of CCI equipment who have not been established as U.S. citizens (e.g., persons attending technical conventions, telephone inquiries, etc.):

- (a) Identification of the basic purpose of the equipment (e.g., encryption of serial data).
- (b) Availability for purchase and delivery.
- (c) Size, weight, and power consumption.
- (d) Data rates, or required bandwidths and carrier service (e.g., conditioned telephone lines).
- (e) Basic front-panel operations/controls.
- (f) Maintenance options or other service packages offered by the vendor.
- (g) The fact that the equipment is a Controlled Cryptographic Item (CCI), and that this means there are certain Government-required controls the purchaser must agree to follow.
- (h) The fact that the equipment meets TEMPEST specifications.
- (i) The fact that the equipment requires a changing key (called "keying material").
- (j) The fact that the CCI equipment is endorsed by NSA for securing classified information.
- (k) The statement that a contract or Memorandum of Understanding/Agreement (MOU/MOA) has been executed between the vendor and NSA.

NOTE: Under no circumstances will classified information be discussed with Group 1 personnel, nor will any discussion of keying materials, cryptoperiods, etc., beyond that specified above take place. Although still photographs may be displayed, no actual or videotaped demonstrations of the CCI equipment will be provided for Group 1 personnel.

(2) Group 2: Potential purchasers of CCI equipment who have been identified as U.S. citizens, and as representing a company, corporation, firm or government agency located in the United States. Citizenship will be determined using the procedures identified in subparagraph a, above.

- (a) All information approved for Group 1 disclosure.
- (b) Information on keying fill interfaces and devices.
- (c) Information on net structuring.
- (d) Key variable update capabilities.
- (e) Key management issues (e.g., how to order, distribute, and control keying materials).

(f) Information on the equipment installation security certification process.

(g) Shipping and delivery procedures.

(h) CCI access and physical control requirements.

(i) Classification level to which the equipment is endorsed.

NOTE: Under no circumstances will classified information be discussed or disclosed to Group 2 personnel who have not clearly established both their appropriate security clearance and need-to-know. In addition, no Program Manager, or other specific NSA point-of-contact will be identified, by name, by the vendor to purchasers of CCI equipment. As a general rule, no discussions will be held with any purchasers of CCI equipment concerning the cryptographic algorithm, to include its identification and any details of its operation.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION XIV. ROUTINE DESTRUCTION OF COMSEC MATERIAL

97. General. The security achieved through the proper use of contemporary U.S. cryptosystems is heavily dependent upon the physical protection which is afforded the associated keying material. Current and superseded keying material is extremely sensitive, since its compromise potentially exposes to compromise all traffic encrypted with it. For this reason, keying material (other than defective or faulty key) 1/ must be destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. Destruction of superseded or obsolete crypto-equipment and supporting documentation is also essential to the maintenance of a satisfactory national COMSEC posture, since these materials may be of significant long-term benefit to hostile interests desiring to exploit U.S. communications for intelligence purposes.

98. Training of Destruction Personnel. Contractors must ensure that destruction personnel have been properly trained prior to performing destruction. The personnel involved must be instructed on the proper use/handling of the destruction devices and the proper destruction procedures.

99. Procedures for Routine Destruction of COMSEC Material. Routine destruction should normally be done by the COMSEC Custodian and the Alternate COMSEC Custodian. However, this restriction should not be enforced at the cost of delaying destruction. Granting the authority to destroy superseded material to additional appropriately cleared 2/ people, who then certify this destruction to the COMSEC Custodian, is preferable to delaying destruction, even for short time. The following paragraphs indicate various types of procedures which might be followed in representative situations, with emphasis on keying material.

a. In a large facility, cleared users may be granted authority to destroy keying material they use, in the presence of cleared witnesses, as soon as the material is superseded.

b. In a small facility with only a few COMSEC equipments, the COMSEC Custodian may personally collect superseded keying material, replace it with new material, and effect timely destruction of superseded material in the presence of a cleared witness.

1/ DO NOT DESTROY defective or faulty keying material. Such material should be reported to DIRNSA, ATTN: S042, and held for disposition instructions.

2/ The term "appropriately cleared" and "cleared" means possession of a final security clearance equal to the highest classification of the material to be destroyed.

c. In mobile situations, routine destruction may be accomplished by the user and an appropriately cleared witness. The issuing COMSEC Custodian must be advised by the user, either verbally or in writing, that the user has destroyed the material. Verbal notification must be followed up with written confirmation of destruction as soon as possible. For accounting purposes, the COMSEC Custodian will then consider the material destroyed. In such cases, the COMSEC Custodian must brief the user on the necessity for prompt and complete destruction of superseded keying material, and for prompt reporting of any loss of control of material before destruction could be accomplished.

d. Scheduling Routine Destruction.

(1) Keying material designated CRYPTO which has been issued for use must be destroyed as soon as possible after supersession, and may not be held longer than 12 hours following supersession. However, where special circumstances prevent compliance with the 12-hour standard (e.g., facility unmanned over weekend or holiday period), the FSO may authorize an extension to a maximum of 72 hours. Keying material designated CRYPTO which has been issued for use must be destroyed as soon as possible after supersession, and may not be held longer than 12 hours following supersession. However, where special circumstances prevent compliance with the 12-hour standard (e.g., facility unmanned over weekend or holiday period), the FSO may authorize an extension to a maximum of 72 hours. Where communications activity is suspended for extended periods (e.g., plant-wide holidays), unused keying material need not be destroyed as it is superseded, but may be retained in the COMSEC account until communications activity resumes, at which time superseded key must be expeditiously destroyed. For circumstances not covered above, contact your COR for instructions.

(2) Complete editions of superseded keying material designated CRYPTO which are held by a user COMSEC account must be destroyed within 5 days after supersession.

(3) Maintenance and sample keying material not designated CRYPTO is not regularly superseded and need only be destroyed when physically unserviceable.

(4) Superseded classified COMSEC publications which are held by a user COMSEC account must be destroyed within 15 days after supersession.

(5) The residue of entered amendments to classified COMSEC publications must be destroyed within 5 days after entry of the amendment.

100. Routine Destruction Methods. The authorized methods for routinely destroying paper COMSEC material are burning, pulverizing or chopping, crosscut shredding, and pulping. Nonpaper COMSEC material authorized for routine destruction must be destroyed by burning, chopping or pulverizing, or chemical alteration.

a. Paper COMSEC Material. The criteria given below apply to classified COMSEC keying material and media which embody, describe, or implement a classified cryptographic logic. Such media include full maintenance manuals,

cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic software. Other paper COMSEC material may be destroyed by any means that are approved for the destruction of other paper material of equal classification or sensitivity.

(1) When destroying paper COMSEC material by burning, the combustion must be complete so that all material is reduced to white ash, and contained so that no unburned pieces escape. Ashes must be inspected and, if necessary, broken up or reduced to sludge.

(2) When pulping, pulverizing, or chopping devices are used to destroy paper COMSEC material, they must reduce the material to bits no larger than five millimeters in any dimension.

NOTE: DO NOT PULP paper-mylar-paper key tape or high wet strength paper (map stock) and durable-medium paper substitute (e.g., TYVEC olefin, polyethylene fiber). These materials will not reduce to pulp, and must be destroyed by burning, pulverizing or chopping, or crosscut shredding.

(3) When crosscut (double cut) shredders are used to destroy paper COMSEC material, they must reduce the material to shreds not more than 3/64-inch (1.2 mm) in width and not more than 1/2-inch (13 mm) in length, or not more than 1/35-inch (0.73 mm) in width and not more than 7/8-inch (22.2 mm) in length.

b. Nonpaper COMSEC Material. The authorized methods for routinely destroying nonpaper COMSEC material are burning, melting, chopping, pulverizing, and chemical alteration. The material must be destroyed to the extent that there is no possibility of reconstructing classified information by physical, chemical, electrical, optical, or other means.

(1) Microforms (microfilm, microfiche, or other reduced-image photo negatives) may be destroyed by burning or by chemical means, such as emersion in household bleach (for silver film masters), or acetone or methylene chloride (for diazo reproductions) for approximately five minutes. When destroying by chemical means, film sheets must be separated and roll film must be unrolled. NOTE: Caution should be exercised to prevent potential hazards when using chemical means for destruction. Contractors are also responsible for ensuring that OSHA standards are met.

(2) Magnetic or electronic storage or recording media are handled on an individual basis. Magnetic tapes may be destroyed by disintegration or incineration. Magnetic cores may be destroyed by incineration or smelting. Magnetic discs, disc packs, and drums may be destroyed by removal of the entire recording surface by means of an emery wheel, disc sander, or by incineration.

WARNING

DO NOT INCINERATE MAGNETIC TAPE ON ALUMINUM REELS, AS THIS MAY CAUSE
AN EXPLOSION

(3) Hardware keying material (i.e., USKAU (Proms), USKAW (permuting plugs)) and associated manufacturing aids will not be destroyed without the approval of NSA.

(4) Plastic canisters. The objective in destroying plastic canisters is to disfigure the two large flat surfaces (sides) of the canister. This can be accomplished by inserting the canister in a zip-lock bag and either puncturing or smashing the empty canister. An empty canister will shatter. Do not attempt to destroy an empty canister without following the safety precautions noted in the handling instructions that accompany canisterized key tape.

c. COMSEC Equipment and Components. Routine destruction of COMSEC equipment and components by users is NOT AUTHORIZED. Disposition instructions for equipment held by contractors which is unserviceable and cannot be repaired, or which is no longer required, must be obtained from the cognizant contracting officer.

101. NSA-Approved Routine Destruction Devices. Contractors may use any destruction devices which satisfy the destruction criteria set forth in this section for the routine destruction of COMSEC material. Information concerning routine destruction devices which have been tested and approved by NSA may be obtained from NSA, ATTN: S042.

102. Reporting Routine Destruction. The routine destruction of all ALC-1 and ALC-2 COMSEC aids must be reported to the COR. Specific reporting requirements for keying material are as follows:

a. When all key settings contained within a particular type of keying material are used or superseded and have been destroyed, the COMSEC Custodian or Alternate COMSEC Custodian must prepare a destruction report and submit it to the COR. The COMSEC Custodian may elect to submit a destruction report as soon as destruction is accomplished or consolidate the destruction information and submit it on a monthly basis. Each COMSEC Custodian who is provided operational keying material for use must ensure that this monthly destruction report is submitted to the COR no later than the 16th day of each month following supersession. No exceptions are authorized; however, negative reports are not required if for any reason no keying material is held that was authorized for destruction during the preceding month.

b. The completed "USAGE RECORD" on the inner front covers of key card books and the "DISPOSITION RECORD" of key lists/key tape segment cards must be reviewed to ensure that all settings were used and properly recorded on the card. The Custodian will then prepare the destruction report and forward one copy to the COR.

c. When destruction reports are prepared by the COMSEC Custodian for keying material actually destroyed by other properly authorized individuals, the appropriate records substantiating the destruction must be retained by the COMSEC Custodian for a period of three years and protected in the same manner as other comparable classified COMSEC material. Additionally, the following remark will be typed below the NOTHING FOLLOWS line on the SF-153 destruction report: "The official records in my possession indicate that the above-listed item(s) has/have been properly destroyed by duly authorized individuals."

SECTION XV. COMSEC EMERGENCY ACTION PROCEDURES

103. Emergency Protection Planning. All facilities which hold classified or CCI COMSEC material must maintain a current, written emergency plan for the protection of such material during emergencies. For locations in CONUS, planning need consider only natural disasters (such as fire, flood, tornado, and earthquake). For locations outside of CONUS, planning must consider both natural disasters and hostile actions (such as enemy attack, mob action, civil uprising). For natural disasters, planning should be directed toward maintaining security control over the material until order is restored. By contrast, planning for hostile actions must concentrate on actions to safely evacuate or securely destroy the COMSEC material. Normal operating routines must be structured so as to minimize the number and complexity of actions which must be taken during emergencies to protect COMSEC material. For example:

a. Only the minimum amount of COMSEC material will be held at any time; i.e., routine destruction should be conducted frequently and excess COMSEC material disposed of in accordance with the disposition instructions obtained from the cognizant contracting officer.

b. COMSEC material should be stored in ways which will facilitate emergency evacuation or destruction.

104. Preparedness Planning for Disasters. Planning for disasters must provide for:

a. Fire reporting and initial fire fighting by assigned personnel.

b. Assignment of on-the-scene responsibility for ensuring protection of the COMSEC material held.

c. Securing or removal of classified COMSEC material and evacuation of the area(s).

d. Protection of material when admission of outside fire fighters into the secure area(s) is necessary.

e. Assessment and reporting of probable exposure of classified COMSEC material to unauthorized persons during the emergency.

f. Post-emergency inventory of classified and CCI COMSEC material and the reporting of any losses or unauthorized exposures to appropriate authority.

105. Preparedness Planning for Hostile Actions. Planning for hostile actions must take into account the possible types of situations which may occur; e.g., an ordered withdrawal over a specified period of time, a hostile environment situation where destruction must be carried out in a discrete manner to avoid triggering hostile actions, or fully hostile imminent overrun situations. Such planning must provided for:

a. Assessing the threat of occurrence of various types of hostile actions at the particular activity and the threat which these potential emergencies pose to the COMSEC material held.

b. Availability and adequacy of physical security protection capabilities; e.g., perimeter controls, guard forces, and physical defenses at the individual buildings and other locations in which COMSEC material is held.

c. Facilities for effecting emergency evacuation of COMSEC material under emergency conditions, including an assessment of the probable risks associated with evacuation. 1/

d. Facilities and procedures for effective secure emergency destruction of COMSEC material held, including adequate supplies of destruction devices, availability of electrical power, secure nearby storage facilities, adequately protected destruction areas, personnel assignments, and responsibilities for implementing emergency destruction.

e. Precautionary destruction of COMSEC material, particularly maintenance manuals and keying material, which is not operationally required to ensure continuity of operations during the emergency. In a deteriorating situation all "full" maintenance manuals (i.e., those containing cryptographic logic information) which are not absolutely essential to continued mission accomplishment should be destroyed. When there is insufficient time under emergency conditions to completely destroy such manuals, every reasonable effort must be made to remove and destroy their sensitive pages (i.e., those containing cryptographic logic). Sensitive pages in U.S.-produced KAMs are listed on fold-out Lists of Effective Pages at the rear of other textual portions and, in addition, some KAMs further identify their sensitive pages by means of gray or black diagonal or rectangular markings at the upper portion of the binding edge.

(1) To prepare for possible emergency destruction sensitive pages from COMSEC maintenance manuals in areas or situations where capture by hostile forces is possible, the following is suggested:

(a) Apply distinctive markings (e.g., red stripes) to the binder edge and covers of all KAMs containing identified sensitive pages.

(b) Remove the screw posts or binder rings, or open the multiring binder, whichever is applicable.

(c) Remove each sensitive page from the KAM and cut off the upper left-hand corner of the page so that the first binder hole is removed. Care must be taken not to delete any text or diagram.

1/ Except under extraordinary conditions (e.g., an urgent need to restore secure communications after relocation), COMSEC keying material should be destroyed rather than evacuated.

(d) Reassemble the document and conduct a page check.

(2) Should it become necessary to implement emergency destruction, the sensitive KAM pages may be removed as follows:

(a) Remove the screw posts or binder rings, or open the multiring binder and remove all pages from the KAM.

(b) Insert a thin metal rod (e.g., wire or screwdriver) through the remaining top left-hand hole of the document.

(c) Grasp the rod in both hands and shake the document vigorously; the sensitive pages should fall out freely.

f. External communications during emergency situations should be limited to contact with a single remote point. This point will act as a distribution center for outgoing message traffic, and as a filter for incoming queries and guidance, thus relieving site personnel and facilities from multiple actions during emergency situations. When there is warning of hostile intent and physical security protection is inadequate to prevent overrun of the facility, secure communications should be discontinued in time to allow for thorough destruction all classified and CCI COMSEC material, including classified and CCI elements of COMSEC equipment.

106. Preparing the Emergency Plan. Preparation of the emergency plan is the responsibility of the FSO. If the plan calls for destroying the COMSEC material, all destruction material, devices, and facilities must be readily available and in good working order. The plan must be realistic; it must be workable, and it must accomplish the goals for which it is prepared. Factors which will contribute to this are:

a. All duties under the plan must be clearly and concisely described.

b. All authorized personnel at the facility should be aware of the existence of the plan. Each individual who has duties assigned under the plan should receive detailed instructions on how to carry out these duties when the plan becomes effective. All personnel should be familiar with all duties so that changes in assignment may be made, if necessary. This may be accomplished by periodically rotating the emergency duties of all personnel.

c. Training exercise should be conducted periodically (quarterly exercises are recommended) to ensure that everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties. If necessary, the plan should be changed based on the experience of the training exercises.

d. The three options available in a hostile-action emergency are securing the material, removing it from the scene of the emergency, or destroying it. Planners must consider which of these may be applicable to their facilities, either singly or in a combination. Which one to choose in various situations should be clearly stated in the plan. For example, if it appears that a civil uprising is to be short lived, and the COMSEC facility is to be only temporarily abandoned, the actions to take could be:

- (1) Ensure that all superseded keying material has been destroyed.
- (2) Gather up the current and future keying material and take it along.
- (3) Remove all classified and CCI elements from crypto-equipment and lock them, along with other classified COMSEC material, in approved storage containers.
- (4) Secure the facility door(s), and leave.
- (5) Upon return, conduct a careful and complete inventory.

Or, if it appears that the facility is likely to be overrun, the emergency destruction plan should be put into effect.

107. Emergency Destruction Priorities. Three broad categories of COMSEC material which may require destruction in hostile-action emergencies are keying material; other COMSEC aids (e.g., maintenance manuals, operating instructions, and general doctrinal publications); and equipment. Depending upon the availability of sufficient personnel and destruction facilities, the priorities set forth under subparagraphs a. or b., below, must be followed.

a. Destruction Priorities within Categories COMSEC Material. When sufficient personnel and destruction facilities are available, different individuals should be made responsible for destroying the material in each category, by means of separate destruction facilities, as set forth in the following subparagraphs:

(1) Keying Material. Emergency destruction priorities for keying material are as follows:

- (a) Superseded keying material designated CRYPTO.
- (b) Currently effective keying material designated CRYPTO (to include zeroization of keying variables stored electrically in crypto-equipment and fill devices).
- (c) Card Reader Insert Boards (CRIBs).
- (d) Future editions of TOP SECRET keying material designated CRYPTO.
- (e) Future editions of SECRET and CONFIDENTIAL keying material designated CRYPTO.
- (f) Training, maintenance, and sample key.

(2) Other COMSEC Aids. Emergency destruction priorities for classified COMSEC Aids other than keying material are as follows:

- (a) Complete cryptomaintenance manuals or sensitive pages, thereof.

(b) Status documents showing the effective dates for COMSEC keying material.

(c) Keying material holder lists and directories.

(d) Remaining classified pages of cryptomaintenance manuals.

(e) Classified cryptographic and noncryptographic operational general publications (KAGs and NAGs).

(f) Cryptographic Operating Instructions.

(g) Remaining classified COMSEC documents

(h) National, department, agency, and service general doctrinal guidance publications.

(3) COMSEC Equipment. Reasonable efforts should be made under deteriorating situations to evacuate COMSEC equipment. In an actual emergency, the immediate goal is to render COMSEC equipment unusable and irreparable. ^{2/} When there is warning of hostile intent, secure communications should be discontinued in advance to allow for thorough destruction of COMSEC equipment. Emergency destruction priorities for COMSEC equipment are as follows:

(a) Zeroize the equipment if the keying element (e.g., key card, permuter plug) cannot be physically withdrawn.

(b) Remove and destroy removable classified and CCI elements (e.g., printed-circuit boards).

(c) Destroy remaining classified and CCI elements.

NOTE: Hulks of equipments and unclassified elements not marked CCI, need not be destroyed. Maintenance manuals for COMSEC equipment contain component listings which identify classified and CCI elements.

b. Destruction Priorities for Combined Categories of COMSEC Material. When personnel and/or destruction facilities are limited, the three categories of COMSEC material will be combined, and destruction will be carried out in accordance with the following priority listing:

(1) All keying material designated CRYPTO, in the following order: superseded key, currently effective key, future key.

(2) Sensitive pages from classified maintenance manuals, or the entire manual (if sensitive pages are not separately identified).

(3) Classified and CCI elements of classified and CCI COMSEC equipment.

^{2/} Although it is desirable to destroy jeopardized crypto-equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most field environments.

(4) Any remaining classified COMSEC or related material.

NOTE: Hulks of equipment, unclassified elements not marked CCI, and unclassified portions of maintenance manuals, operating instructions, etc., need not be destroyed.

108. Emergency Destruction Tools. Basic hand tools should be readily available for emergency destruction of COMSEC equipment at all facilities holding such equipment. These tools will be useful, and in some cases required, for removing classified and CCI elements from equipment, for removing certain components from classified and CCI elements prior to disintegrator destruction and, in worst-case situations, to actually accomplish destruction. The following is a list of suggested tools which should be kept in a designated area reserved exclusively for emergency destruction of COMSEC equipment:

- ° Hammer, 3-lb, ball or cross peen
- ° Cold chisel, 5-3/4-inches long, 1/2-inch wide tip
- ° Stubby screwdriver, 1-inch blade, 7/32-inch wide tip
- ° Screwdriver, 1-1/2-inch blade, 5/32-inch wide tip
- ° Screwdriver, 6-inch blade, 5/16-inch wide tip
- ° Phillips screwdriver, number 0
- ° Phillips screwdriver, number 2
- ° Wrench, 5/16, box- and open-end combination
- ° Pliers, 5-inch, diagonal cutting
- ° Pliers, heavy duty, linemans
- ° Crowbar
- ° Fire ax or sledge hammer

In addition to the above hand tools, facilities which maintain an incinerator for emergency destruction should also have tongs and asbestos gloves readily available.

109. Emergency Destruction Methods. Any of the methods approved for routine destruction of classified COMSEC material may be used for emergency destruction. Additionally, incendiary destruction devices may be available for emergency destruction at certain locations outside of CONUS. Information concerning these devices is contained in NTISSI No. 4004, "Routine Destruction and Emergency Protection of COMSEC Material."

110. Reporting Emergency Destruction. Accurate information relative to the extent of an emergency destruction is absolutely essential to the effective

evaluation of the COMSEC impact of the occurrence, and is second in importance only to the conduct of thorough destruction. Reports must be submitted by the most expeditious means available and shall clearly indicate the material destroyed, the method(s) of destruction, and the extent of destruction. The report must also identify any items which were not thoroughly destroyed and which may be presumed to be compromised. In such cases, an insecurity report must be submitted as prescribed in Section XVI.

111. Review of Emergency Action Procedures. COMSEC emergency procedures developed under these guidelines will be made available for review upon the request of NSA.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION XVI. COMSEC INSECURITY REPORTING REQUIREMENTS

112. General. To be successful, the National COMSEC Insecurity Reporting System must receive an uninhibited flow of information relating to a clear understanding of the circumstances surrounding an insecurity. Thus, users of COMSEC material must be encouraged to report COMSEC insecurities promptly. Adherence to the following guidelines will ensure the success of the system.

a. Every person who will deal in any way with COMSEC material must understand his or her responsibilities for immediately reporting insecurities to the FSO or his designated representative. These officials must report COMSEC insecurities as prescribed in this Section. Insecurity reports must be submitted promptly and not be delayed in administrative channels.

b. Individuals will not be disciplined for reporting a COMSEC insecurity. Corrective measures are most productive when aimed at the national doctrine or the organizational policy or procedure which allowed or contributed to the insecurity. Disciplinary action should normally be taken only against the perpetrator or perpetrators of grossly negligent or willful acts which jeopardize the security of COMSEC material.

113. Types of COMSEC Insecurities. COMSEC insecurities fall into three categories, as noted below. Included under each category are representative types of reportable insecurities. Additional reportable insecurities which are peculiar to a given cryptosystem are normally listed in the operating instructions, and maintenance manual(s) for that cryptosystem.

a. Cryptographic Insecurities.

(1) Use of COMSEC key which is compromised, superseded, defective, previously used and not authorized for reuse, or in any way incorrect for the cryptoperiod or application in which it is used; e.g.:

(a) Unauthorized use of any key for other than its intended purpose.

(b) Use of key which was produced locally without the authorization of the Director, NSA. 1/

(c) Unauthorized extension of a cryptoperiod.

(d) Premature use of key.

NOTE: Failure to zeroize a common-fill device within the required time must be reported as a physical insecurity.

(2) Use of a cryptosystem or a cryptosystem operating practice or maintenance practice which is not approved by NSA; e.g.,

1/ DIRNSA AUTHORIZATION TO GENERATE KEY IN THE FIELD IS IMPLICIT IN THE PUBLICATION OF OPERATING INSTRUCTIONS FOR CRYPTOSYSTEMS WHICH POSSESS THAT CAPABILITY.

(a) Operational use of a COMSEC equipment without completion of a required alarm-check test or after failure of a required alarm-check test.

(b) Actual or attempted maintenance of a COMSEC equipment by unqualified personnel.

(3) Use of COMSEC equipment having defective cryptographic logic circuitry; e.g.:

(a) Plaintext transmission resulting from a COMSEC equipment failure or malfunction.

(b) Any transmission during or after an uncorrected failure, that may cause improper operation of a COMSEC equipment.

(4) Discussions via nonsecured telecommunications of the details of a crypto-equipment failure or malfunction.

(5) Tampering with, or unauthorized modifications of, a COMSEC equipment or system.

(6) Compromising emanations from a COMSEC equipment.

(7) Any other occurrence which may have resulted in a cryptographic insecurity.

b. Personnel Insecurities.

(1) Known or suspected defection, espionage, hostile cognizant agent activity, treason, sabotage, or capture by an enemy of persons who have detailed knowledge of cryptographic logic or uncontrolled access to keying material.

(2) Theft of COMSEC material.

(3) Deliberate falsification of COMSEC records.

(4) Unauthorized disclosure of information concerning COMSEC material or attempts by unauthorized persons to effect such disclosure.

c. Physical Insecurities.

(1) The physical loss of COMSEC material, including a portion(s) thereof (e.g., a CCI equipment or a classified page from a crypto-equipment maintenance manual).

(2) COMSEC material discovered outside of required COMSEC accountability or physical control; e.g.:

(a) COMSEC material reflected on a destruction report as having been properly destroyed and witnessed, but found not to have been destroyed.

(b) COMSEC material left unsecured and unattended where unauthorized persons could have had access.

(3) COMSEC material improperly packaged, shipped, or destroyed;
e.g.:

(a) COMSEC material received in a damaged package.

(b) Destruction of COMSEC material by other than authorized means or COMSEC material not completely destroyed and left unattended.

(4) COMSEC material received in a package which shows evidence of tampering, or known or suspected tampering with COMSEC material at any time.

(5) Unauthorized access to COMSEC material.

(6) Failure to zeroize a common fill device within the required time.

(7) Premature opening of a sealed package of keying material.

(8) Unexplained loose keycards in a package having a wide-band seal.

(9) Unauthorized copying, reproducing, or photographing of COMSEC material.

(10) A clandestine intercept or recording device discovered in or near a COMSEC facility.

(11) Any other incident which jeopardizes the physical security of COMSEC material.

114. Reporting Insecurities. When reporting insecurities, the contractor must make an immediate telephonic notification to the DIS CSO and NSA of any incident or violation of the security requirements specified in this Supplement irrespective of the contractor's judgement as to whether or not an insecurity or possible insecurity occurred. Where secure means of transmission are available, the initial report will provide all the details known at that time. Where the notification is made over an unsecure-mode, the insecurity report should be limited to minimum essential information. During normal duty hours (0730-1730 EST), notification to NSA will be made to the COMSEC Insecurity Branch (S213) on (301) 688-6010 or 6948. After normal duty hours and on weekends and holidays, the notification will be made to the Senior Information Security Coordinator on (301) 688-7003. The initial telephonic report must be followed up with a letter report, classified according to its contents, and securely forwarded. Unclassified reports will be marked For Official Use Only.

115. Types of Reports.

a. Initial Report. An initial written report is required for each detected COMSEC insecurity. If all of the facts regarding the incident are included in the initial report, it may also serve as the final report,

provided it contains all information required by paragraph 115d, below. In such cases, paragraph 6 of the initial report will include a request that the report be accepted as a final report.

b. Amplifying Report. Whenever significant, new information concerning a reported incident is discovered, an amplifying report is required. An amplifying report may also serve as the final report, provided it contains all information required by paragraph 115d, below. In such cases, paragraph 6 of the amplifying report must include a request that the report be accepted as a final report.

c. Interim Report. If a final report is not submitted within 30 days after the initial report or the last amplifying report, an interim report will be submitted every 30 days until the final report is submitted. The interim report will advise of the status of an inquiry or investigation, or other reason for delay of the final report.

d. Final Report. A final report is required for each reported COMSEC insecurity unless the initial or an amplifying report also served as the final report. The final report must include a summary of the results of all inquiries and investigations, and it will identify corrective measures taken or planned to minimize the possibility of recurrence.

116. Format and Content of Insecurity Letter Reports. Format and content requirements for insecurity letter reports are set forth below. Where subsequent reports would merely duplicate information previously reported, the information need not be repeated. Instead, reference will be made to the previous report which contains the information.

a. Subject. The subject of the report will consist only the words "COMSEC Insecurity."

b. References. The report must include reference(s), as applicable, to:

(1) The paragraph number of the operating, maintenance, or Agency or Department instruction or this supplement in which the reported insecurity is listed, or the statement: "Formal reporting requirements cannot be identified at this time."

(2) Previously forwarded, related insecurity reports and other correspondence identified sufficiently to permit location (e.g., date, time, office symbol, etc.).

c. Material Involved. Paragraph 1 of the report must identify the COMSEC material involved. Include the short title (including edition designator, modification suffix letter, and MATSYM or system designator, if applicable); register, accounting and serial number (as applicable) of Accounting Legend Code 1 and 3 material (all other material by quantity); specific cards, tape segments, tables, and days if not a complete document; a description of the material or equipment involved; and whether equipment was keyed or unkeyed. Where the insecurity involves keying material, identify the controlling authority for each short title.

d. Personnel Involved. For personnel insecurities only, paragraph 2 of the report must identify the individual(s) who caused, or was otherwise responsible for, the insecurity. Include for each individual: name, citizenship, duty position, and level of security clearance held. For all other COMSEC insecurities, provide only the duty position, the level of security clearance, if known, and the nationality of the individual(s) involved.

e. Location of Incident. Paragraph 3 of the report must identify the location of the incident, the responsible facility, and its COMSEC account number.

f. Circumstances of Incident. Paragraph 4 of the report must identify the circumstances surrounding the insecurity. Give a chronological account of the events which led to the discovery of the insecurity and, when known, sufficient details to give a clear picture of how the insecurity occurred. The chronology must include all relevant dates, times of day, frequencies of events, etc. Include a description of the security measures in effect at the location, and estimate the possibility of unauthorized personnel having access to the COMSEC material involved. Paragraph 4 of amplifying report may also be used to report significant new information not included in other paragraphs of the report.

g. Additional Reporting Requirements. Paragraph 5 of the report will include any additional reporting that may be required. The following subparagraphs list the reporting requirements for specific incidents or items.

(1) Improper use of Keying Material or Use of Improper Operating Procedures.

(a) A description of the associated communications activity (e.g., online/offline, simplex/half-duplex/full-duplex, point-to-point/netted operations).

(b) The operating mode of the crypto-equipment (e.g., clock start, message indicator, traffic flow security).

(c) The general type of traffic involved, if any (SI/SAO, voice, data).

(2) Operational Use of Malfunctioning COMSEC Equipment.

(a) The symptoms of the malfunction.

(b) The likelihood that the malfunction was deliberately induced. If so, see subparagraph (8), below.

(c) The amount and type of traffic involved, if any.

(3) Known or Suspected Defection, Espionage, Hostile Cognizant Agent Activity, Treason, Sabotage, or Capture.

(a) The individual's general background in COMSEC and the extent of his/her knowledge of crypto-principles.

(b) List the cryptosystems to which the individual had current access and state whether the access was to cryptographic logic and/or key. (For logic, state whether access was to full or limited maintenance manuals, and for key state the short titles and edition identifiers involved.)

(4) Loss of COMSEC Material.

(a) The actions being taken to locate the material.

(b) The possibility of access by unauthorized persons.

(c) The possibility of removal of material by authorized or unauthorized persons.

(d) The methods of disposal of all classified and unclassified waste and the possibility of loss by those methods.

(5) COMSEC Material Discovered Outside of Required COMSEC Accountability or Physical Control.

(a) The action which caused accountability or physical control to be restored.

(b) The possibility of access, surreptitious or otherwise, by unauthorized persons.

(c) The estimated length of time the material was unsecured.

(6) COMSEC Material Received in a Damaged Package.

(a) The means of transmittal (when the damage occurred in transit).

(b) A description of how the material was stored (when the damage occurred in storage).

NOTE: Ensure all packaging containers, wrappers, etc., are retained until destruction is authorized or directed.

(7) COMSEC Material Received in a Package that Shows Evidence of Tampering, or known or Suspected Tampering at Any Time.

(a) A description of the evidence of known or suspected tampering.

(b) The means of transmittal (when the suspected tampering occurred in transit).

(c) A description of how the material was stored (when the suspected tampering occurred in storage).

NOTE: When tampering is known or suspected, immediately seal the package and/or material in a plastic (or any other) wrapper and place it in the most

secure, limited-access storage available. Handle the package and/or material as little as possible until instructions are received from NSA. Take no action that would jeopardize potential evidence.

(8) Unauthorized Copying, Reproduction, or Photographing.

(a) A complete identification of the equipment or material copied or photographed.

(b) The reason for reproduction and how the reproduced material was controlled.

(c) Whether espionage is indicated or suspected. If so, see subparagraph (3), above.

(d) The degree to which details of equipment internals, keying material, or documents were copied or photographed.

NOTE: A copy of each photograph or other reproduction must be included with the insecurity letter report.

(9) Unauthorized Modification or Maintenance of a COMSEC Equipment, or Discovery of a Clandestine Intercept or Recording Device in or Near a COMSEC Facility.

(a) A description of the modification, or device; its installation and symptoms; and the host equipment involved.

(b) An estimate of how long the item may have been in place.

(c) An estimate of the classified information/traffic jeopardized.

NOTE: Hold information concerning these types of insecurities on a strict need-to-know basis. The equipment or devices should not be used or otherwise disturbed until further instructions are received from NSA. Where a clandestine intercept or recording device is suspected, do not speak about it in the area of the device. Nothing should be done that would possibly alert the COMSEC exploiter, except on instructions from NSA.

h. Possibility of Compromise. Paragraph 6 of the report must state which of the following opinions is applicable: compromise certain, compromise possible, compromise improbable; and will include the basis for the opinion. Where an initial or amplifying report is to also serve as the final report, paragraph 6 must include a request that the report be accepted as a final report.

i. Point of Contact. Paragraph 7 of the report will include the name, commercial telephone number, and, if available, secure telephone number of an individual who is prepared to respond to questions from the evaluating authority.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION XVII. INSPECTION/AUDIT OF COMSEC ACCOUNTS

117. Notification. Prior notice may or may not be provided to the contractor when a COMSEC account has been selected for audit/inspection.

118. Access. The auditor/inspector must present proper identification prior to gaining access to the COMSEC account.

119. DIS Inspection Criteria. DIS may inspect COMSEC accounts as part of its regular industrial security inspections. Prior to each COMSEC inspection, the DIS representative will review the most current COR report or letter provided to the contractor as a result of the last COR audit of the account. The purpose for this review of COR audit reports by the DIS representative is to preclude duplication of inspection effort by DIS and NSA.

120. Report of Inspection. When deficiencies are noted that require formal corrective action by the contractor, DIS will forward to the COR a copy of the COMSEC inspection report, along with a copy of its letter to management.

121. COR Audit Criteria.

a. Primary COMSEC Accounts. The COR will audit primary COMSEC Accounts annually or as deemed necessary. The audit will include:

(1) Verification of the completeness and accuracy of COMSEC accounting reports and files.

(2) Determination of the COMSEC Custodian and Alternate COMSEC Custodian's knowledge of and adherence to the provisions of this Supplement.

(3) Normally, physically sighting all COMSEC material held by the account.

(4) Verification of compliance with packaging, marking and shipping procedures.

(5) Solicitation of any problems encountered by the COMSEC Custodian in maintaining the account.

(6) Recommendations for the improvement of local COMSEC accounting and control procedures.

b. COMSEC Subaccounts. The COR will conduct audits of COMSEC Subaccounts on a random, unannounced basis and in the same manner as for Primary COMSEC Accounts. Prior to the audit, the Primary COMSEC Account will be requested to provide the NSA COR a pre-printed listing of the COMSEC subaccount's holdings.

122. Primary COMSEC Account Audit Criteria. COMSEC Custodians of primary COMSEC Accounts must conduct audits of their Subaccount(s) at least annually and in the same manner as that specified in paragraph 121, above.

123. Report of COR Audit of Primary COMSEC Accounts. Immediately upon completion of the audit, the Auditor will notify the COMSEC Custodian of any situation requiring immediate action, and will conduct an exit interview with the FSO and, if deemed necessary, with management. A formal report of audit outlining any discrepancies noted during the audit, the condition of the COMSEC account, and recommendations for improvements will be forwarded to the contractor. A copy of the Audit Report will also be provided to the appropriate DIS CSO. When the Audit Report outlines actions required of the COMSEC Custodian, the FSO, or others concerned, a Certificate of Action Statement will accompany the Audit Report. The letter forwarding the Audit Report will normally specify that all actions required in the report be completed within ten working days following receipt of the letter. A special effort must be placed on returning the Certificate of Action Statement within the specified time.

124. Report of COR Audit of COMSEC Subaccounts. The COR's formal report of the audit will be forwarded to the COMSEC Custodian of the primary account, with a copy furnished to the subaccount COMSEC Custodian. If the audit report outlines corrective actions to be taken, a Certificate of Action Statement will also be included with the letter forwarding the report. It will be the responsibility of the COMSEC Custodian of the primary COMSEC account to ensure that required corrective actions are accomplished by the subaccount COMSEC Custodian within the specified period of time. Once the required actions have been completed, the subaccount COMSEC Custodian must return a signed copy of the Certificate of Action Statement to the COMSEC Custodian of the primary COMSEC account, who will then countersign it and return it to the COR, retaining a copy for file.

125. Report of Primary COMSEC Account Audit of Its COMSEC Subaccount. The report of the auditing COMSEC Custodian's findings must be submitted to the subaccount COMSEC Custodian and a copy retained by the primary account COMSEC Custodian to be made available to the COR at the time of the primary COMSEC Account's annual audit or upon request. When the Audit Report outlines actions required of the subaccount COMSEC Custodian, a Certificate of Action Statement must accompany the report. The required actions must be completed by the subaccount COMSEC Custodian within ten working days following receipt of the report. Upon completion of the actions, the Subaccount COMSEC Custodian shall sign the Certificate of Action Statement and return it to the Primary COMSEC Account for retention.

APPENDICES

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I

CONTROLLING AUTHORITY INSECURITY EVALUATION GUIDANCE

1. The purpose of this Appendix is to provide guidance to personnel and organizations for making evaluations of reported insecurities. Each insecurity incident is different from every other insecurity, so that each case must be independently reviewed and evaluated. The key elements in performing an insecurity evaluation are as follows:

a. Get the facts.

b. Determine the probability of compromise, loss, etc., of the cryptographic system, keying material, etc.

c. Determine the type and amount of information which may have been compromised due to the COMSEC insecurity, and ensure that appropriate officials are notified, so that they can take necessary actions to limit the damage caused by actual or potential loss of the information.

d. Consider the various options for actions to avoid or reduce damage caused by the COMSEC insecurity (e.g., superseding keying material).

e. Direct implementation of corrective actions.

2. When an insecurity report is received for evaluation, if the facts reported are not adequate for the evaluation, additional information should be requested from the organization reporting the insecurity. It is often useful to specify the exact information which is needed.

3. Cryptographic equipments are designed so that their security depends primarily upon the changing mathematical variables used to key them. What this means for evaluations of insecurities is that corrective actions fall into different categories for equipments and non-changing materials (e.g., maintenance manuals) on the one hand, and keying materials on the other hand.

a. For cryptographic equipments and related materials other than keying materials, the options for corrective actions after an insecurity has been reported center on preventing a recurrence of the insecurity. Certain special cases, such as the suspected tampering of a cryptographic device, may merit special actions (e.g., notifying NSA so that a technical inspection can be made), but in general, the evaluation response must focus on correcting the problem which allowed or caused the insecurity to happen.

b. For keying materials, however, the evaluation process is much different.

(1) If it is determined that superseded or effective keying material has been compromised, then by extension, it must be assumed that all information encrypted using that keying material has been compromised. In this case it is especially important to notify appropriate officials so that actions can be taken to minimize the damage caused by the actual or possible disclosure of the information.

(2) If it is determined that future keying material (not yet used) has been compromised, then every step should be taken to avoid its use, and replace it with keying material which has not been subjected to compromise.

(3) If it is determined that currently effective keying material has been compromised, then the evaluation should focus on the potential impacts of compromising the secured information as well as the prospects for emergency supersession of keying materials which have not been subjected to compromise.

4. Lost keying material and materials which are temporarily out of prescribed control, or are found in an unauthorized location, should be considered compromised. An example would be keying material which was temporarily lost but then later discovered in circumstances under which continuous secure handling cannot be verified.

a. Casual viewing of keying material by unauthorized U.S. personnel under circumstances in which copying, photographing, or memorizing would be difficult should be considered as no compromise.

b. Access to keying material by unauthorized U.S. personnel under circumstances in which any reasonable opportunity existed to copy, photograph, or memorize key should be considered a compromise.

c. Any viewing of keying material by unauthorized foreign personnel should be considered a compromise unless there is substantial evidence that no compromise has occurred, i.e., the circumstances of the incident effectively precluded the possibility of copying, photographing, or memorizing the keying material.

d. The unauthorized absence of personnel who are authorized access to keying material should be considered as no compromise, unless there is evidence of defection, theft, or loss of keying material. When a person who has had access to keying material is officially reported as an unauthorized absentee, however, all cryptographic equipment, key, and other materials to which he/she could have had access must be inventoried.

e. If a controlling authority experiences difficulty in evaluating insecurities of a technical nature, or any other difficulty in making an evaluation, assistance may be obtained from NSA (ATTN: S21).

f. With respect to the security of keying material, it should always be kept in mind that the key may be stolen, copied, photographed, changed or substituted during a very brief period when the material is not under proper control. Controlling authorities are urged to be both cautious and conservative when making evaluations of insecurity reports involving keying material.

5. Once the determination has been made that there is any degree of possibility that equipment has been lost, keying material has been compromised, etc., the organization doing the evaluation must direct appropriate actions to be taken. As noted above, for those cases in which keying material is not involved, the primary task is to inform appropriate organizations (e.g., for a lost CCI equipment, ensure that the accountability

requirements to a COR are addressed). To ensure that effective actions are taken to prevent a recurrence of an insecurity involving keying material is usually more complex, and there are a number of options available to a controlling authority.

a. Direct implementation of emergency or spare key setting for keying materials which provide for such spare settings.

b. Direct the early implementation of uncompromised future editions of keying material. This action must be reported immediately to NSA (ATTN: S21 and Y1) so that resupply action may be taken and replacement materials may be produced and shipped.

c. Direct the early implementation of uncompromised future editions by those cryptonet members who hold those future editions, or who can be supplied with them in time; and exclude from cryptonet operations those members who do not hold or who cannot be supplied with the replacement keying material. This action must also be reported to NSA (S21 and Y1).

d. If the options above are not feasible, the following actions should be considered for implementation:

(1) Extend the cryptoperiod of uncompromised keying material, up to 24 hours (unless specified cryptosystem doctrine prohibits such an extension or authorizes a longer period), until replacement keying material can be supplied to cryptonet members.

(2) Transmit by secure electrical means, which provides end-to-end encryption, replacement key settings to cryptonet members. The replacement key settings must be encrypted by means of machine keying material which has not been subject to compromise.

(3) Suspend cryptonet operations until resupply can be accomplished.

(4) Continue to use the compromised key. This action should be considered only as a last resort and used when:

(a) Normal supersession of the compromised material will take place before an emergency supersession can be accomplished.

(b) Keying material changes would have a seriously detrimental effect on significant operations.

(c) When there is no replacement keying material available by any means.

(5) In cases such as (4) above, where the compromised keying material continues to be used, the controlling authority should alert all cryptonet members, preferably by other secure means, that a possible compromise of the keying material has occurred, and that transmissions in the compromised key may themselves be compromised and should be minimized.

e. Consideration of superseding a current or future edition of keying material in an emergency is contingent upon several factors, including the number of editions held at cryptonet member COMSEC accounts, and the capability of NSA or others to supply replacement editions. Any decisions to supersede must take into consideration the time required for advance notification to all cryptonet members and for them to implement the new keying materials. All emergency supersessions should be coordinated with the regular supplier of the keying material (normally NSA, ATTN: S21 and Y1).

APPENDIX II
COMSEC BRIEFING

A. You have been selected to perform duties which will require access to sensitive COMSEC information. It is, therefore, essential that you are made fully aware of certain facts relative to the protection of this information before access is granted. This briefing will provide you with a description of the types of COMSEC information you may have access to, the reasons why special safeguards are necessary for protecting this information, the directives and rules which prescribe those safeguards, and the penalties which you will incur for willful disclosure of this information to unauthorized persons.

B. COMSEC equipment and keying material are especially sensitive because they are used to protect other sensitive information against unauthorized access during the process of communicating that information from one point to another. Any particular piece of COMSEC equipment, keying material, or other cryptographic material may be the critical element which protects large amounts of sensitive information from interception, analysis, and exploitation. If the integrity of the COMSEC system is weakened at any point, all the sensitive information protected by that system may be compromised; even more damaging, this loss of sensitive information may never be detected. The procedural safeguards placed on COMSEC equipment and materials, covering every phase of their existence from creation through disposition, are designed to reduce or eliminate the possibility of such compromise.

C. Communications Security (COMSEC) is the general term used for all steps taken to protect information of value when it is being communicated. COMSEC is usually considered to have four main components: Transmission security, physical security, emission security, and cryptographic security. Transmission security is that component of COMSEC which is designed to protect transmissions from unauthorized intercept, traffic analysis, imitative deception and disruption. Physical security is that component of COMSEC which results from all physical measures to safeguard cryptographic materials, information, documents, and equipment from access by unauthorized persons. Emission security is that component of COMSEC which results from all measures taken to prevent compromising emanations from cryptographic equipments or telecommunications systems. Finally, cryptographic security is that component of COMSEC which results from the use of technically sound cryptosystems, and from their proper use. To ensure that telecommunications are secure, all four of these components must be considered.

D. Part of the physical security protection given to COMSEC equipment and materials is afforded by the special handling it receives for distribution and accounting. There are two separate channels used for the handling of such equipment and materials: "COMSEC channels" and "administrative channels." The COMSEC channel, called the COMSEC Material Control System (CMCS) is used to distribute accountable COMSEC items such as keying material, maintenance manuals, and classified and CCI equipment. (EXCEPTION: Some Military Departments have been authorized to distribute CCI equipment through their standard logistics system.) The CMCS channel is composed of a series of COMSEC accounts, each of which has an appointed COMSEC Custodian who is personally responsible and accountable for all COMSEC materials charged to the account. The COMSEC Custodian assumes responsibility

for the material upon receipt, and then controls its dissemination to authorized individuals on a need-to-know basis. The administrative channel is used to distribute COMSEC information and materials other than that which is accountable in the COMSEC Material Control System.

E. Particularly important to the protection of COMSEC equipment and materials is an understanding of all security regulations and the timely reporting of any compromise, suspected compromise, or other security problem involving these materials. If a COMSEC system is compromised but the compromise is not reported, the continued use of the system, under the incorrect assumption that it is secure, can result in the loss of all information that was ever protected by that system. If the compromise is reported, steps can be taken to change the system, replace the keying material, etc., to reduce the damage done. In short, it is your individual responsibility to know and to put into practice all the provisions of the appropriate publications which relate to the protection of the COMSEC equipment and materials to which you will have access.

F. Public disclosure of any COMSEC information is not permitted without the specific approval of your Government contracting office representative or the National Security Agency (NSA). This applies to both classified and unclassified COMSEC information, and means that you may not prepare newspaper articles, speeches, technical papers, or make any other "release" of COMSEC information without specific Government approval. The best personal policy is to avoid any discussions which reveal your knowledge of or access to COMSEC information and thus avoid making yourself of interest to those who would seek the information you possess.

G. Finally, you must know that should you willfully disclose or give to any unauthorized persons any of the classified or CCI COMSEC equipment, associated keying materials, or other classified COMSEC information to which you have access, you will be subject to prosecution under the criminal laws of the United States. The laws which apply are contained in Title 18, United States Code, sections 641, 793, 794, 798, and 952.

H. If your duties include access to classified COMSEC information, in addition to the above, you should avoid travel to any countries which are adversaries of the United States, or to their establishments/facilities within the U.S. Should such travel become necessary, however, your security office must be notified sufficiently in advance so that you may receive a defensive security briefing. Any attempt to elicit the classified COMSEC information you have, either through friendship, favors, or coercion must be reported immediately to your security office.

APPENDIX III

National Security Agency
Deputy Directorate for Information Security
Controlled Cryptographic Item (CCI)
Control Agreement

This CCI Control Agreement (called the "Agreement") is entered into this _____ day of _____, 19____, by and between the United States of America, acting through the National Security Agency, Deputy Directorate for Information Security (hereinafter called the Agency) and _____

(i) a corporation organized and existing under the laws of the state of _____

(ii) a partnership consisting of _____

(iii) an individual doing business as _____ with its principal office and place of business at _____ in the city of _____ state of _____ zip code _____

(hereinafter called the "User")

Witnesseth that:

Whereas the User is now in a contractual relationship with the Government, or a participant in the Commercial COMSEC Endorsement Program (CCEP), which may require the exchange of classified and/or sensitive Government information; and

Whereas the User requires CCI to secure its telecommunications involving classified or sensitive Government information; and

Whereas, the parties desire to define and set forth the precautions and specific safeguards to be taken by the User and the Government in order to preserve and maintain the national security of the United States through the prevention of improper disclosure and/or transfer of CCI, i.e., technical data, software, equipment, associated manuals and documents, and any other CCI material, the transfer or disclosure of which may be detrimental to the national security of the United States; and

Whereas, the Agency would not make CCI equipment and associated materials available to the User if this Agreement were not entered into;

Now, therefore, in consideration of the foregoing and the promises and agreements set forth in this document, and with specific recognition that the User's access to and use of CCI and associated materials involves special trust and confidence involving the national security, the User agrees:

Section I - CONTROLS AND PROCEDURES FOR ACCOUNTABILITY

(A) The User agrees to provide for and maintain, in accordance with the requirements of the COMSEC Supplement to the Industrial Security Manual (CSISM) and the applicable systems Doctrine, attached hereto and made part of this Agreement, a system of controls and procedures for accountability of CCI within the User's organization, subject, (i) to any revisions of the CSISM required by the demands of national security, as determined by the Agency, notice of which shall be provided to the User, and (ii) to mutual, written agreements entered into by the parties in order to adapt the CSISM to the User's business and necessary procedures. In order to place in effect such control and procedures, the User further agrees to prepare Standard Practice Procedures for its own internal use, such procedures to be consistent with the CSISM.

(B) The User understands that upon Agency approval of the User's written application, the Agency will open and administer a COMSEC account for the User. The Government will provide COMSEC Briefings to User personnel who are required, by the terms of the CSISM, to be so briefed.

(C) The User agrees that during the term of the Agreement he will not (i) sell, lease, alienate, transfer, or otherwise divest himself of title (in any manner, whether voluntarily or involuntarily, in whole or in part) to any CCI equipment or associated material owned, held or controlled by the user, except in accordance with the requirements of the CSISM, (ii) pledge, mortgage, hypothecate or grant a security interest in any CCI equipment or associated material owned, held or controlled by the User; or (iii) suffer or permit to exist any lien or security interest in any CCI equipment or associated material owned, held or controlled by the User.

(D) The User agrees that he may not assign this Agreement nor any rights or obligations hereunder.

Section II - INSPECTION AND AUDIT

The user acknowledges that designated representatives of the U.S. Government responsible for inspection pertaining to the maintenance of proper controls and audit of COMSEC accounts to ensure the completeness and accuracy of

accounting and reporting shall have the right to inspect, at reasonable intervals, the procedures, methods and facilities utilized by the User to comply with the requirements of the CSISM and the terms of this Agreement. Should the Government determine that the User's control and accounting procedures, methods and facilities do not comply with such requirements, it shall submit a written report to the User advising of the deficiencies, and specify a reasonable time for cure and re-inspection. Failure to correct deficiencies may result in the termination of this Agreement.

Section III - MODIFICATION

Modification of this Agreement may be made only by written agreement of the parties. The CSISM may be modified in accordance with Section I of this Agreement.

Section IV - TERMINATION

This Agreement shall remain in effect until terminated by providing 30 days written notice. If the Government gives notice of intent to terminate for reasons as specified in Section II of the Agreement, the User shall either (i) dispose of his CCI inventory in accordance with the requirements of the Manual, or (ii) collect, properly package and deliver all such CCI equipment to the Agency or a receiver designated by the Agency at a place or places to be designated by the Agency. Such disposition shall be completed within 30 days of receipt of the notice of intent to terminate, or as soon after as is reasonably practicable. Notwithstanding any such termination, the terms and conditions of this Agreement shall remain in effect for so long as the User is in possession of CCI equipment or associated materials. In the event that the User is the owner of all or a part of the CCI inventory, the Government shall receive CCI equipment and material which have not been otherwise properly disposed by the User (as specified above) and make arrangements to sell them to purchaser(s) authorized to hold such CCI under an agreement similar to this agreement. The proceeds of such sale shall be remitted to the User.

Section V

The User agrees that he will report to the Agency if his facility clearance is revoked because of factors related to foreign ownership, control or influence (FOCI) or for any other reasons, so that the Agency can determine the User's continued eligibility to purchase, own or use CCI equipment. If the Agency determines that the User is no longer authorized because of FOCI, to purchase, own and/or use CCI equipment and associated materials, this Agreement shall be terminated as set forth in Section IV.

The User further agrees that he will immediately notify the Agency in the event any petition under the federal Bankruptcy Act, or any other federal or state law for the relief of debtors, is filed for or against the User.

Section VI - NOTICE

All notices provided for in this Agreement shall be in writing and shall be personally delivered to the party to whom notice is to be given, or mailed through the U.S. Postal Service, First Class, with postage affixed. Notice to the User shall be made at the address given on the first page of this Agreement, or such other address as the User shall hereafter designate in writing. Notice to the Government shall be given to the Deputy Director for Information Security, National Security Agency, Fort George G. Meade, Maryland 20755-6000.

Section VII - PENALTIES

By entering into this agreement the User acknowledges that its failure to adhere to the terms and conditions of the agreement may result in Government instituted civil, criminal, or administrative actions including, but not limited to, contract claims, breach of trust actions, actions to debar or suspend the User as a Government contractor, and criminal prosecution for violations constituting offenses punishable pursuant to the provisions of the United States Code.

Section VIII - WAIVER AND SEVERABILITY OF AGREEMENT PROVISIONS

Waiver by the Government of one breach or default under this Agreement shall not be deemed a waiver of any subsequent breach or default. The Government shall have sole discretion to waive or compromise any provision in this Agreement. Furthermore, any such action taken upon one occurrence shall not be deemed to be binding upon the Government upon a subsequent occurrence of the same or similar event.

Section IX - OTHER AGREEMENTS

This Agreement shall not be construed to pertain to, nor to modify or replace any other agreements or contractual arrangements which were previously entered into between the User and the U.S. Government.

Section X - COSTS

The User acknowledges that this Agreement does not obligate Agency funds, and the Agency shall not be liable for any costs or claims of the User arising out of this Agreement or instructions issued hereunder. The parties may, however, enter into agreements or contractual arrangements to provide for secure telecommunications to the User which may be properly chargeable to the Agency or the U.S. Government.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year written above:

THE UNITED STATES OF AMERICA

BY _____

(Authorized Representative of
the Government)

(User)

WITNESS

By _____

(Firm)

NOTE: In case of a corporation witnesses are not required, but the certificate must be completed. Type or print names under all signatures.

(Title)

(Address)

NOTE: The User, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, (name) _____ certify that I am the (title of certifier) _____ of the corporation named as User herein; that (name of signatory) _____ who signed this agreement on behalf of the User, was then (title of signatory) _____ of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

(Signature)

Appendix IV.

CONTRACTING OFFICER AUTHORIZATION TO PURCHASE
CCI EQUIPMENT AS CONTRACTOR ACQUIRED PROPERTY

1. _____ (Company Name), _____ (Address) has a requirement based upon a U.S. Government contract(s) or subcontract(s) to purchase CCI equipment.

2. The appropriate Government Contracting Officer(s) has authorized the purchase of the following equipment in the quantities specified:

3. The CCI equipment specified in paragraph 2 (above) will be Contractor Acquired Property, as defined at FAR 45.101(a), and be charged to the following U.S. Government contracts:

Prime Contract No.
Subcontract No. (if applicable)

Government Contracting Officer
Name Telephone

Typed or Printed Name

Authorized Signature

Position/Title

Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX V

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

TSEC Nomenclature

TABLE OF DESIGNATORS—COMSEC EQUIPMENT

I FUNCTION	II TYPE	III ASSEMBLIES	IV HOW TO COMPARE
C—COMSEC Equipment System K—Cryptographic H—Crypto-Ancillary M—Manufacturing N—Noncryptographic S—Special Purpose	G—Key Generation I—Data Transmission L—Literal Conversion N—Signal Conversion O—Multi-Purpose P—Materials Production S—Special Purpose T—Testing, Checking U—Television W—Teletypewriter X—Facsimile Y—Speech	A—Advancing B—Base or Cabinet C—Combining D—Drawer, Panel E—Strip, Chassis F—Frame, Rack G—Key Generator H—Keyboard I—Translator, Reader J—Speech Processing K—Keying, Permuting L—Repeater M—Memory or Storage O—Observation P—Power Supply, Converter R—Receiver S—Synchronizing T—Transmitter U—Printer V—Removable Communications Security Component W—Logic Programmer/Programming X—Special Purpose	<p>1 <i>Equipment</i> The nomenclature designator "TSEC" followed by a slant (/), and a digraph formed with letters selected from Columns I and II, thus TSEC/KG-Item Number for Cryptographic Key Generator</p> <p>2 <i>Equipment System</i> The nomenclature designator "TSEC" followed by a slant (/) and digraph formed with the letter "C" from Column I and an appropriate letter from Column II, thus TSEC/CY-Item Number for COMSEC Equipment System, Speech, or TSEC/CU-Item Number for COMSEC Equipment System, Television</p> <p>3 <i>Equipment Assembly</i> The nomenclature designator "TSEC" preceded by a slant (/) and a trigraph formed with letters selected from Columns I, II, and III, thus KGP-Item Number/TSEC is a Power Supply used with a Cryptographic Key Generator Also, Integrated COMSEC Device designators are selected from these columns, i.e., KGV-Item Number/TSEC is a removable key generator integrated into a particular communications system</p>

TABLE OF DESIGNATORS—COMSEC AIDS (U)

RELEASE	FUNCTIONAL RELATIONSHIP	PURPOSE	TYPE AID	MANUFACTURING AIDS
US—Identifies the item as NOFORN A—Identifies the item as authorized for release to specified allies	C—Two-Man Control K—Cryptographic H—Ancillary M—Manufacturing N—Noncryptographic S—Special Purpose	A—Operational B—Compatible Multiple Keying Variable L—Logistics Combinations M—Maintenance R—Reference S—Sample T—Training V—Developmental X—Exercise Z—"On the Air" Testing	A—Authenticator B—Diagnostic Test Program C—Code/Cipher D—Obsolete E—Special Purpose Aperture Card F—Cryptographic Program G—General Publication H—Call Sign and/or Freq. Chng System I—Recognition and/or Identification Sys J—Indicator List K—Key List L—Miscellaneous M—Maintenance Manual N—Computer Keying Material O—Operating Manual P—One-Time Pad Q—Engineering Document R—Rotor S—Sealed Authentication System T—Tape U—PROMs/ROMs/LSI Devices V—Communications Electronics Operations Instructions W—CRIB X—Fanfold Pad Y—Key Card Z—Permuting Plug	B—Blue Line C—Contour Notch Pattern F—Checking Aid G—Generation Program K—Keying Specification L—Miscellaneous M—Manuscript N—Negative P—Page Proof R—Repro Page S—Sample T—Tape (magnetic or punched) W—Wiring Diagram

** FORM

A—PUNCHED CARDS
 D—MAGNETIC CARDS
 E—MAGNETIC TAPE
 F—MICROFICHE
 V—VIDEO CASSETTES

**Examples Form KAMF-XXX a maintenance manual in microfiche form, KAGD-XXX, a general document in mag card form *Note* This column should only be used when a COMSEC aid is being produced in some form other than paper.

Figure 1. Table of Designators
 AV-3

<input checked="" type="checkbox"/> TRANSFER	<input type="checkbox"/> INVENTORY	<input type="checkbox"/> DESTRUCTION	<input type="checkbox"/> HAND RECEIPT	<input type="checkbox"/> OTHER (Specify)	
2 Director National Security Agency FR112 R Room 9E456, FANX III O Fort George G. Meade, MD M 20755-6000		ACCT NO 880999	4 DATE OF REPORT (YR. MO., DA) 871001	5 OUTGOING NUMBER 999025	
		DATE REPORT IS PREPARED	6 DATE OF TRANSAC- TION (YR. MO., DA) LEAVE BLANK	7 INCOMING NUMBER LEAVE BLANK	
3 Commander 10th Signal Group T ATTN: Account 505106 O Fort Hood, TX 10623-5000		ACCT NO. 505106	8. *ACCOUNTING LEGEND CODES 1. ACCOUNTABILITY BY SERIAL NO IN CMCS 2. ACCOUNTABILITY BY QUANTITY IN CMCS 3. ACCOUNTABLE BY SERIAL NUMBER IAW SERVICE/AGENCY DIRECTIVES 4. INITIAL RECEIPT CONTROL IAW SERVICE/ AGENCY DIRECTIVES		
SHORT TITLE	10 QUANTITY	11. ACCOUNTING NUMBERS		12 * ALC	13 REMARKS
		BEGINNING	ENDING		
1 KAM-297 A	2	766	767	1	
2 KAM-331 A	2	101	102	1	
3 KG-13 3	2	642	643	1	
-----NOTHING FOLLOWS-----					
9 Custodian: Sign all copies and distribute as prescribed 10 by the accounting instructions of your Service. ← Required Notations 11 12 13 14 This shipment consists of 3 containers. ← Required Notations 15 16 The material above is NSA property being 17 loaned to the Army for one year. ← Required Notations 18 19 20 21 22 23 24 DCS Control No., Registered Mail No., 25 GBL No., or other Control No. as 26 Appropriate. 27 28 29 30 31 32 33 34					
14 THE MATERIAL HEREON HAS BEEN <input type="checkbox"/> RECEIVED <input type="checkbox"/> INVENTORIED <input type="checkbox"/> DESTROYED					
15 SIGNATURE OF COMSEC CUSTODIAN			17 SIGNATURE OF <input type="checkbox"/> WITNESS <input type="checkbox"/> OTHER (Specify)		
16 TYPED OR STAMPED NAME, GRADE SERVICE			18 TYPED OR STAMPED NAME, GRADE, SERVICE		
19 FOR DEPARTMENT OR AGENCY USE DCS No./15089			20 PAGE 1 OF 1 PAGES		

Figure 2. Transfer Report of COMSEC Material to a Military Service (SF-153)

<input checked="" type="checkbox"/> TRANSFER	<input type="checkbox"/> INVENTORY	<input type="checkbox"/> DESTRUCTION	<input type="checkbox"/> RECEIPT	<input type="checkbox"/> OTHER (Specify)
1 EAST COAST ELECTRONICS 2 830 WASHINGTON AVENUE 3 BALTIMORE, MARYLAND 4 ROBERT L. SHEA		ACCT NO 870399	REPORT U. DA) J31	5 OUTGOING NUMBER 399008
		DATE REPORT IS PREPARED	6 DATE OF TRANSAC TION (YR. MO. DA) LEAVE BLANK	7 INCOMING NUMBER LEAVE BLANK
8 BOSTON COMPUTER CORP. 9 6366 ATLANTIC AVENUE 10 CAMBRIDGE, MASSACHUSETTS 11 ATTN: COMSEC CUSTODIAN		ACCT NO 870344	8 *ACCOUNTING LEGEND CODES 1 ACCOUNTABILITY BY SERIAL NO IN CMCS 2 ACCOUNTABILITY BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4 INITIAL RECEIPT CONTROL LAW SERVICE/ AGENCY DIRECTIVES	
SHORT TITLE	10 QUANTITY	11 ACCOUNTING NUMBERS		12 * ALC
		BEGINNING	ENDING	13 REMARKS
1 KW-62	1	-	4	1 New Material
2 KW-40	1	-	11	4 " "
3 KW-40	2	21	22	4 " "
4 E-ABC	5	N/N	-	2 " "
6 // NOTHING FOLLOWS //				
7 CUSTODIAN SIGN ALL COPIES.				
8 RETURN ORIGINAL COPY TO: ←				
9 DIRECTOR				
10 NATIONAL SECURITY AGENCY				
11 OPERATIONS BUILDING NO. 3 (Y13)				
12 ROOM 1B51				
13 FORT GEORGE G MEADE, MARYLAND 20755-6000				
14				
15				
16 DISPOSE OF REMAINING COPIES IN ACCORDANCE WITH				
17 INSTRUCTIONS OF YOUR ORGANIZATION.				
18				
19				
20 THIS SHIPMENT CONSISTS OF 4 CONTAINERS ←				
21 EXAMPLE OF A TRANSFER REPORT OF COMSEC				
22 MATERIAL TO AN ACCOUNT OTHER THAN A				
23 MILITARY SERVICE.				
24				
25				
26				
27				
28				
29				
30 DCS CONTROL NO., REGISTERED MAIL NO.,				
31 GEL NO., OR OTHER CONTROL NO. AS				
32 APPROPRIATE.				
33				
34				
14 THE MATERIAL HEREON HAS BEEN				
<input type="checkbox"/> RECEIVED		<input type="checkbox"/> INVENTORIED		<input type="checkbox"/> DESTROYED
15 SIGNATURE OF COMSEC CUSTODIAN			17 SIGNATURE OF	
			<input type="checkbox"/> WITNESS	
			<input type="checkbox"/> OTHER (Specify)	
16 TYPED OR STAMPED NAME, GRADE, SERVICE			18 TYPED OR STAMPED NAME, GRADE, SERVICE	
19 FOR DEPARTMENT OR AGENCY USE			DD-250 PARTIAL NO./4	
DCS NO./15091 CONTRACT NO./DA18-119-AMC-17777(Y)			20 PAGE 1 OF 1 PAGES	

Figure 3. Transfer Report of COMSEC Material to an Account Other Than a Military Service (SF-153)

	<input type="checkbox"/> TRANSFER	<input type="checkbox"/> INVENTORY	<input checked="" type="checkbox"/> DESTRUCTION	<input type="checkbox"/> HAND RECEIPT	<input type="checkbox"/> OTHER (Specify)
2 F R O M	EAST COAST ELECTRONICS 830 WASHINGTON AVENUE BALTIMORE, MARYLAND ROBERT L. SHEA		ACCT NO 870399	4 DATE OF REPORT (YR. MO. DA) 871031	5 OUTGOING NUMBER 399004
			DATE REPORT IS PREPARED	6 DATE OF TRANSACTION (YR. MO. DA) LEAVE BLANK	7 INCOMING NUMBER LEAVE BLANK
3 T O	DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM 11B51 FORT GEORGE G MEADE, MARYLAND 20755-6000		ACCT NO	8 *ACCOUNTING LEGEND CODES 1 ACCOUNTABILITY BY SERIAL NO IN CMCS 2 ACCOUNTABILITY BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER 4 INITIAL RECEIPT CONTROL LAW SERVICE AGENCY DIRECTIVES	
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34	SHORT TITLE	10 QUANTITY	11. ACCOUNTING NUMBERS		12 A/C
			BEGINNING	ENDING	REMARKS
	KAM-109 A	2	1125	1126	1
	KAM-114 C	1	-	965	1
	AMEND 1 to KAM-140 A	1	-	169	4 RESIDUE
	AMEND 2 to KAM-140 A	1	-	185	4 RESIDUE
	//////////////////////NOTHING FOLLOWS////////////////////////////////////				
	AUTHORITY FOR DESTRUCTION: HANDLING INSTRUCTIONS OF SUPERSEDING EDITIONS.				
	EXAMPLE OF A DESTRUCTION REPORT OF COMSEC MATERIAL.				
	ACCOUNTING LEGEND				
14 THE MATERIAL HEREON HAS BEEN					
<input type="checkbox"/> RECEIVED <input type="checkbox"/> INVENTORIED <input checked="" type="checkbox"/> DESTROYED					
15 SIGNATURE OF COMSEC CUSTODIAN			17 SIGNATURE OF		
<i>Robert L. Shea</i>			<input checked="" type="checkbox"/> WITNESS		
			<input type="checkbox"/> OTHER (Specify) <i>Walter J. Hoffman</i>		
16 TYPED OR STAMPED NAME, GRADE, SERVICE			18 TYPED OR STAMPED NAME, GRADE, SERVICE		
ROBERT L. SHEA			WALTER J. HOFFMAN, ALTERNATE CUSTODIAN		
19 FOR DEPARTMENT OR AGENCY USE					
20 PAGE OF					

Figure 4. Destruction Report (SF-153)

CLASSIFICATION

DATE 06 AUG 87

EXAMPLE OF COMSEC MATERIAL INVENTORY

OUTGOING TN 396008

TO BE PLACED ON THE INVENTORY BY THE COMSEC CUSTODIAN

ACCOUNT 870396 INVENTORY

SHORT TITLE	START EDIT	ENDING EDIT	TOTAL EDIT	START COPY #	ENDING COPY #	TOTAL COPIES	TRANS NUMBER	TRANSACTION DATE	PREV ACCT	ACCT LGND	STATE OWN REMARKS
KAM-342	A	A	1	1	1	1	111117	12 DEC 86	880092	1	<div style="border: 1px solid black; padding: 5px;"> TRANSFERRED TO NSA ACCT 880641 TN NO. 396074 DATED 4AUG84 </div>
KAM-143	A	A	1	540	540	106001	12 DEC 86	880099	1		
KG-10	--	--	--	1070	1070	166809	16 DEC 86	880099	1		
KG-10(V-1)	--	--	--	34	34	111105	20 DEC 86	880091	1		
ST-26	--	--	--	30	30	100000	31 DEC 86	880099	1		

////////////////////////////////////NOTHING FOLLOWS////////////////////////////////////

I CERTIFY THAT I HAVE PHYSICALLY INVENTORIED THE MATERIAL LISTED HEREON. I FURTHER CERTIFY THAT COGNIZANT PERSONNEL HAVE REVIEWED THE MATERIAL LISTED, AND THAT ALL MATERIAL EXCEPT AS NOTED IN THE "REMARKS" COLUMN, IS CURRENTLY NEEDED BY THIS ACTIVITY. THIS REPORT, AS AMENDED, INCLUDING None PAGE(S) OF SUPPLEMENTAL SF-153, CONSTITUTES A COMPLETE INVENTORY OF ACCOUNTABLE COMSEC MATERIAL IN MY POSSESSION AS OF THE DATE OF THIS REPORT.

I CERTIFY THAT I HAVE WITNESSED THE PHYSICAL INVENTORY OF THE MATERIAL LISTED ON THIS REPORT AS SUPPLEMENTED AND/OR AMENDED.

SIGNATURE (CUSTODIAN)
Jack A. Jones

DATE OF INVENTORY
 16 Aug 1987

SIGNATURE (WITNESS)
 - *Robert Elliott*

DATE OF INVENTORY
 16 Aug 1987

CLASSIFICATION

Figure 5. Preprinted Inventory

CLASSIFICATION
DATE 25 JAN 87

EXAMPLE OF COMSEC
MATERIAL INVENTORY

OUTGOING TN
395008

TO BE PLACED
ON THE INVENTORY
BY THE COMSEC CUSTODIAN

ACCOUNT 870395 INVENTORY

SHORT TITLE	START EDIT	ENDING EDIT	TOTAL EDIT	START COPY #	ENDING COPY #	TOTAL COPIES	TRANS NUMBER	TRANSACTION DATE	PREV ACCT	ACCT LGND	STATE OWN	REMARKS
KAM-342	A	A	1	1	1	1	111117	12 DEC 86	880092	1		<div style="border: 1px solid black; padding: 5px;"> TRANSFERRED TO NSA ACCT 880641 TN NO. 396074 DATED 4JAN84 </div>
KAM-143	A	A	1	540	540	106001	12 DEC 86	880099	1			
KG-10	--	--	--	1070	1070	166809	16 DEC 86	880099	1			
KG-10(V-1)	--	--	--	34	34	111105	20 DEC 86	880091	1			
ST-26	--	--	--	30	30	100000	31 DEC 86	880099	1			

////////////////////////////////////NOTHING FOLLOWS////////////////////////////////////

I CERTIFY THAT I HAVE PHYSICALLY INVENTORIED THE MATERIAL LISTED HEREON. I FURTHER CERTIFY THAT COGNIZANT PERSONNEL HAVE REVIEWED THE MATERIAL LISTED, AND THAT ALL MATERIAL EXCEPT AS NOTED IN THE "REMARKS" COLUMN, IS CURRENTLY NEEDED BY THIS ACTIVITY. THIS REPORT, AS AMENDED, INCLUDING / PAGE(S) OF SUPPLEMENTAL SF-153, CONSTITUTES A COMPLETE INVENTORY OF ACCOUNTABLE COMSEC MATERIAL IN MY POSSESSION AS OF THE DATE OF THIS REPORT.

I CERTIFY THAT I HAVE WITNESSED THE PHYSICAL INVENTORY OF THE MATERIAL LISTED ON THIS REPORT AS SUPPLEMENTED AND/OR AMENDED.

SIGNATURE (CUSTODIAN) *Jack Q. Jones* DATE OF INVENTORY *2 Feb 1987*

CLASSIFICATION

SIGNATURE (WITNESS) *Robert Elliott* DATE OF INVENTORY *2 Feb 1987*

Figure 6. Preprinted Inventory With Supplement

COMSEC
MATERIAL REPORT

OMB
APPROVAL NO 22-R0164

<input type="checkbox"/>	TRANSFER	<input type="checkbox"/>	INVENTORY	<input type="checkbox"/>	DESTRUCTION	<input type="checkbox"/>	HAND RECEIPT	<input checked="" type="checkbox"/>	Supplement to OTHER (Specify) Inv.	
FROM	2 JONES ASSOCIATES 5959 COMSEC WAY NOWHERE, MT 12345			ACCT NO 870395		4 DATE OF REPORT (YR. MO. DA) 870202		5 OUTGOING NUMBER 395008		
						6 DATE OF TRANSACTION (YR. MO. DA)		7 INCOMING NUMBER		
ROOM	3 DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MD 20755-6000			ACCT NO		8 *ACCOUNTING LEGEND CODES 1 ACCOUNTABILITY BY SERIAL NO IN CMCS 2 ACCOUNTABILITY BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER IAW SERVICE/AGENCY DIRECTIVES 4 INITIAL RECEIPT CONTROL IAW SERVICE/ AGENCY DIRECTIVES				
SHORT TITLE			10	11 ACCOUNTING NUMBERS		12*	13			
			QUANTITY	BEGINNING	ENDING	ALC	REMARKS			
1	KAG-48			1	445	445	1			
2	////////////////////			NOTHING FOLLOWS		////////////////////				
3										
4										
5	NOTE: ABOVE RECEIVED FROM 880099 ON TN395004 ON 13 JANUARY 1987.									
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
14 THE MATERIAL HEREON HAS BEEN				<input type="checkbox"/>	RECEIVED	<input checked="" type="checkbox"/>	INVENTORIED	<input type="checkbox"/>	DESTROYED	
15 SIGNATURE OF COMSEC CUSTODIAN					17 SIGNATURE OF					
<i>Jack A. Jones</i>					<input checked="" type="checkbox"/> WITNESS <i>Robert Elliott</i>					
<input type="checkbox"/> OTHER (Specify)										
16 TYPED OR STAMPED NAME, GRADE SERVICE					18 TYPED OR STAMPED NAME, GRADE SERVICE					
JACK A. JONES					ROBERT ELLIOTT					
19 FOR DEPARTMENT OR AGENCY USE						20 PAGE 1 OF 1 PAGES				

NSN 7540-00-935-5861

DOD KAG-1 153-121

STANDARD FORM 153 (Rev. 9/79)

FOR OFFICIAL USE ONLY

PRESCRIBED BY DOD

Figure 6A. Supplement to Preprinted Inventory (Continued)

COMSEC
MATERIAL REPORT

OMB
APPROVAL NO 22-R0164

<input type="checkbox"/>	TRANSFER	<input type="checkbox"/>	INVENTORY	<input type="checkbox"/>	DESTRUCTION	<input type="checkbox"/>	HAND RECEIPT	<input checked="" type="checkbox"/>	CHANGE-OF-CUST. OTHER (Specify)
F R O M	2. JONES ASSOCIATES 5959 COMSEC WAY NOWHERE, MT 12345			ACCT NO 870999		4. DATE OF REPORT (YR. MO. DA) 871228		5. OUTGOING NUMBER 999001	
	3. DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MD 20755-6000			ACCT NO		8. *ACCOUNTING LEGEND CODES 1. ACCOUNTABILITY BY SERIAL NO IN CMCS 2. ACCOUNTABILITY BY QUANTITY IN CMCS 3. ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4. INITIAL RECEIPT CONTROL (LAW SERVICE) AGENCY DIRECTIVES			
SHORT TITLE				10 QUANTITY	11. ACCOUNTING NUMBERS		12 ALC	13 REMARKS	
					BEGINNING	ENDING			
1.	KAM 240 C			1	-	421	1		
2.	KAM 240 D			1	-	321	1		
3.	KAO 137 RP 1 D			1	-	125	1		
4.	KGB 36			1	-	600	1		
5.	KGD 36			1	-	600	1		
6.	KOK 1			1	-	13100	1		
7.									
8.									
9.	////////////////////							NOTHING FOLLOWS	
10.									
11.									
12.									
13.									
14.									
15.									
16.									
17.									
18.									
19.									
20.									
21.									
22.									
23.									
24.									
25.									
26.									
27.									
28.									
29.									
30.									
31.									
32.									
33.									
34.									

14. THE MATERIAL HEREON HAS BEEN				<input checked="" type="checkbox"/> RECEIVED	<input type="checkbox"/> INVENTORIED	<input type="checkbox"/> DESTROYED
15. SIGNATURE OF COMSEC CUSTODIAN <i>Robert J. Lewis</i>			17. SIGNATURE OF: <input checked="" type="checkbox"/> WITNESS <i>Robert G. Hall</i> <input type="checkbox"/> OTHER (Specify)			
16. TYPED OR STAMPED NAME, GRADE SERVICE ROBERT J. LEWIS (INCOMING COMSEC CUSTODIAN)			18. TYPED OR STAMPED NAME, GRADE SERVICE ROBERT G. HALL (OUTGOING COMSEC CUSTODIAN)			
19. FOR DEPARTMENT OR AGENCY USE				20. PAGE 1 OF 1 PAGES		

NSN 7540-00-935-5861

DDO KAG-1 153-121

STANDARD FORM 153 (Rev. 9/79)

FOR OFFICIAL USE ONLY

PRESCRIBED BY 101

Figure 8. Change-of-COMSEC-Custodian Inventory Completed on an SF-153

COMSEC
MATERIAL REPORT

OMB
APPROVAL NO 22-R0164

<input type="checkbox"/>	TRANSFER	<input type="checkbox"/>	INVENTORY	<input type="checkbox"/>	DESTRUCTION	<input checked="" type="checkbox"/>	HAND RECEIPT	<input type="checkbox"/>	OTHER (Specify)			
FROM	2. COMSEC CUSTODIAN Thomas Smith				ACCT. NO. 870999		4. DATE OF REPORT (YR., MO., DA.) 871228		5. OUTGOING NUMBER			
	3. William Grace Engineering Department				ACCT. NO.		8. *ACCOUNTING LEGEND CODES 1. ACCOUNTABILITY BY SERIAL NO IN CMCS 2. ACCOUNTABILITY BY QUANTITY IN CMCS 3. ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4. INITIAL RECEIPT CONTROL LAW SERVICE/ AGENCY DIRECTIVES					
6. DATE OF TRANSAC- TION (YR., MO., DA.)							7. INCOMING NUMBER					
TO	SHORT TITLE				10. QUANTITY		11. ACCOUNTING NUMBERS		12. ALC		13. REMARKS	
							BEGINNING		ENDING			
1.	KAO 199				1		-		42		1	
2.	//////////				1		NOTHING FOLLOWS		//////////		//////////	
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												
17.												
18.												
19.												
20.												
21.												
22.												
23.												
24.												
25.												
26.												
27.												
28.												
29.												
30.												
31.												
32.												
33.												
34.												

14. THE MATERIAL HEREON HAS BEEN RECEIVED INVENTORIED DESTROYED

15. SIGNATURE OF COMSEC CUSTODIAN	17. SIGNATURE OF <input type="checkbox"/> WITNESS <input checked="" type="checkbox"/> OTHER (Specify) <i>William Grace</i> HAND RECEIPT
16. TYPED OR STAMPED NAME, GRADE SERVICE	18. TYPED OR STAMPED NAME, GRADE, SERVICE WILLIAM GRACE

19. FOR DEPARTMENT OR AGENCY USE

20. PAGE OF PAGES

NSN 7540-00-935-5061

DDO KAG-1 153-121

STANDARD FORM 153 (Rev. 9-79)
PRESCRIBED BY DDO

FOR OFFICIAL USE ONLY

Figure 9. COMSEC Material Hand Receipt Utilizing an SF-153

COMSEC MATERIAL HAND RECEIPT			
IDENTIFICATION		QUANTITY	ACCOUNTING NUMBERS
KW-49		1	67
COMSEC material issued on a hand receipt will never be reissued by a user. If the material is needed by another individual outside the immediate control of the original recipient, it must be returned to the COMSEC custodian for reuse. Signature signifies understanding.			
RECIPIENT	PRINTED NAME	JACK E. JONES	ORGANIZATION ENG LAB
	SIGNATURE	<i>Jack Jones</i>	PHONE
DATE	RECEIVED	1 Jul 87	
	DUE	3 Jul 87	
	RETURNED	1 Jul 87	
REMOVAL AUTHORIZED BY		BILL SMITH, COMSEC CUSTODIAN	
RETURNED TO		Bill Smith	
FORM A 1721 REV MAR 82 (Supersedes A1721 REV MAR 71 which is obsolete)			

Figure 10. COMSEC Material Hand Receipt Utilizing an A-1721

FRONT SIDE OF FORM L6061

SHOW FINAL DISPOSITION ON THIS SIDE AND SUPPORTING ADDRESSES, TRANSACTION NOS AND DATES AS APPROPRIATE

SHORT TITLE				KW-49			
NO (S)		QUANTITY		ACCOUNTING LEGEND		CLASSIFICATION	
67		1		1		SECRET	
INITIAL RECEIPT				FINAL DISPOSITION			
REC'D FROM		DATE OF RECEIPT		TYPE		DATE	
NSA ACCT 880666		1 JUL 87					
		VOUCHER NO				VOUCHER NO	
		395061		BASIC EQUIPMENT		KW-49	
				CONTRACT NO.		DA18-119-AMC-44X	
FORM L6061 REV JUL 67				(over)		COMSEC MATERIAL RECORD	

REVERSE SIDE OF FORM L6061

INITIAL AND DATE WHEN MATERIAL IS RETURNED BY USER.

(continued)						LOCATION/HAND RECEIPT	
NO(S)	LOCATION	HAND RECEIPT		RETURNED			
		SIGNATURE	DATE	INITIALS	DATE		
67	ENG LAB	Jack Jones	1 Oct 87	BS	1 Oct 87		

Figure 11. COMSEC Material Record (L6061)

SAMPLE COMSEC MATERIAL IDENTIFICATION MARKINGS
TSEC/KY 99

SAMPLE
PACKAGE MARKINGS

1. EQUIPMENT PACKAGE

- a. Short Title of Equipment
- b. Assemblies Contained in Equipment
- c. Accounting Numbers

KY-99 CONSISTING OF:
KYB-95/100
KYK-90/88

2. ASSEMBLY PACKAGE

- a. Short Title of Equipment
- b. Assembly Short Titles
- c. Accounting Numbers

KY-99 ASSEMBLIES:
KYG-96/106
KYL-88/110
HYP-66/109

3. ELEMENT PACKAGE

- a. Short Title of Equipment
- b. Element Short Titles
(classified elements only)

KY-99 ELEMENTS:
E-ANG 1 ea.
E-ANJ 1 ea.
E-ABR 1 ea.
E-BRG 1 ea.

Figure 12: Sample COMSEC Material Identification Markings

SHORT TITLE

ACCOUNTING NO.



LONG TITLE:

CONTROLLED MANUSCRIPT

PAGES _____ THRU _____ COPY _____ OF _____ COPIES
PAGES _____ THRU _____
PAGES _____ THRU _____

RECORD OF PAGE CHECKS		RECORD OF PAGES ADDED, REMOVED OR DESTROYED				
DATE CHECKED	BY WHOM (SIGNATURE)	DATE ADDED	DATE REMOVED	DATE DESTROYED	PAGES ADDED, REMOVED OR DESTROYED	BY WHOM ADDED REMOVED OR DESTROYED (SIGNATURE)

WARNING: THE ATTACHED DOCUMENT HAS BEEN ENTERED INTO THE NSA COMSEC MATERIAL CONTROL SYSTEM AND WILL BE HANDLED AND ACCOUNTED FOR IN ACCORDANCE WITH THE PROVISIONS OF DOD 5220.22-S-1 OR NSAM 90-2 OR CSCM-1, AS APPLICABLE



Figure 15. Sample of Controlled Manuscript Cover

SHORT TITLE

ACCOUNTING NO.



LONG TITLE:

**IN-PROCESS
CONTROLLED MANUSCRIPT**

PAGES _____ THRU _____ COPY _____ OF _____ COPIES
PAGES _____ THRU _____
PAGES _____ THRU _____

RECORD OF PAGE CHECKS		RECORD OF PAGES ADDED, REMOVED OR DESTROYED				
DATE CHECKED	BY WHOM (SIGNATURE)	DATE ADDED	DATE REMOVED	DATE DESTROYED	PAGES ADDED, REMOVED OR DESTROYED	BY WHOM ADDED REMOVED OR DESTROYED (SIGNATURE)

WARNING: THE ATTACHED DOCUMENT HAS BEEN ENTERED INTO THE NSA COMSEC MATERIAL CONTROL SYSTEM AND WILL BE HANDLED AND ACCOUNTED FOR IN ACCORDANCE WITH THE PROVISIONS OF DOD 5220.22-S-1 OR NSAM 90-2 OR CSCM-1, AS APPLICABLE



Figure 15A. Sample of IN-PROCESS Controlled Manuscript Cover

DEFENSE COURIER SERVICE STATIONS

- | | | |
|---|---|---|
| 1. ANCHORAGE
Building 31-260
Elmendorf AFB, Alaska | 7. JACKSONVILLE
Building 934
Naval Air Station
Jacksonville, FL
Comm: (904)772-2784 | 12. NORFOLK
Building LP-82
Naval Air Station
Norfolk, VA
Comm: (804)444-3471/
3472/3473 |
| 2. BOSTON
Building 225
Naval Air Station
South Weymouth, MA
Comm: (617)786-2780/
2781/2857/2958/2558 | 8. KELLY
Building 1470
Kelly AFB, TX
Comm: (512)925-3704 | 13. OFFUTT
MOD "B"
Offutt AFB, NE
Comm: (402)294-5354/
5355/5356 |
| 3. CHARLESTON
Air Freight Bldg(S-178)
Charleston AFB, SC
Comm: (803)554-2191/
3603/2401 | 9. LOS ANGELES
Building 205
Los Angeles AF Station
El Segundo, CA
Comm: (213)643-1878/
1879 | 14. SAN DIEGO
Building 1
937 North Harbor Drive
San Diego, CA
Comm: (714)235-3381/3382 |
| 4. DENVER
Building 612
Rocky Mountain Arsenal
Commerce City, CO
Comm: (303)289-0289/
0294 | 10. MCCORD
Building 1410
McCord AFB
Tacoma, WA
Comm: (206)984-5908
2426 | 15. TRAVIS
Building 934
Travis AFB
Fairfield, CA
Comm: (707)438-2641/2642 |
| 5. DOVER
Building 506
Dover AFB, DE
Comm: (302)678-6063/
6064 | 11. MCGUIRE
Building 17-02
Air Freight Warehouse
McGuire AFB, NJ
FTS: 484-4534
Comm: (609)723-7937 | 16. WASHINGTON
7455"A" New Ridge Road
Linthicum, MD 21090
Comm: (301)677-2144/2145 |
| 6. HONOLULU
Building 4069
Air Freight Building
Hickam AFB, HI
Comm: (808)449-1130
1171 | | 17. WRIGHT-PATTERSON
Building 829, Area "A"
Wright-Patterson
AFB, OH 45437
Comm: (513)257-3121/
6130 |

Figure 16. DCS Station Addresses
AV-20

**END
FILMED**

DATE:

10-93

DTIC