



**U.S. Government Contractors**  
**Controlled Cryptographic Item**  
**Manual**

2 February 1986

**FOR OFFICIAL USE ONLY**

## EXECUTIVE SUMMARY

### I. Purpose and Scope

A. The basic purpose of this U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual "Executive Summary" is twofold:

1. To act as an introduction and overview of the major features and requirements of the Manual.

2. To provide Government contractors who are potential purchasers or users of CCI equipment with:

a. A preliminary explanation of the procedures they must follow, and the requirements they must meet, to acquire, use, and dispose of communications security (COMSEC) equipment which has been designated as a Controlled Cryptographic Item (CCI).

b. The "Certificate Pertaining to Foreign Interests" questionnaire, which may need to be completed and sent to the National Security Agency (NSA) as a prerequisite for obtaining CCI equipment and obtaining a copy of the U.S. Government Contractors CCI Manual.

B. Because of these multiple purposes, and because the "Executive Summary" is primarily intended as an "Introduction to CCI" which vendors of CCI devices may send or give to prospective customers, the bulk of its information is organized under the specific questions (in section III below) which potential purchasers of CCI equipment are likely to ask. This summary does not ask, or answer, every question a user of CCI equipment will have, nor is it intended to do so. It has been designed primarily to give potential purchasers of CCI equipment a basic understanding of what "CCI" is, how it may be obtained, and how it must be controlled.

C. This "Executive Summary" is unclassified. It may be reproduced in whole or in part and provided to anyone interested in obtaining CCI equipment. No specific Government authorization is required. Vendors of CCI equipment are encouraged to provide copies of this summary to their potential customers as an official introduction to the Government requirements associated with that equipment. The U.S. Government Contractors CCI Manual itself, however, is administratively controlled by NSA. Distribution of the CCI Manual is made by NSA to U.S. Government contractors, upon request, after NSA has reviewed and approved the completed "Certificate Pertaining to Foreign Interests." The CCI Manual is also unclassified, except for one annex, which is separately distributed only to those contractors which have been identified by the Government as requiring it.

D. The CCI Manual was written for, and applies to U.S. Government contractors located in the United States, Puerto Rico, and U.S. possessions and trust territories, who are users or manufacturers of CCI equipment, as well as for use of CCI equipment, outside the U.S., Puerto Rico, or U.S. possessions or trust territories.

E. The CCI Manual contains the minimum U.S. Government requirements for the acquisition, use, and disposition of CCI equipment. Additional requirements may, for special reasons, be separately imposed by the contracting Government Department or Agency.

F. Vendors of CCI equipment are often able to answer many questions posed by potential purchasers. For additional information concerning CCI equipment, the CCI Manual, or any aspect of industrial communications security, write to:

Director  
National Security Agency  
Attention: S3  
9800 Savage Road  
Ft. George G. Meade, MD 20755-6000

or telephone the Office of COMSEC Industrial Relations (S3) on (301) 688-6581. For best service when calling, please identify yourself as a potential purchaser of CCI equipment, and state the nature of your question or comment, so the proper person may assist you.

G. The National Security Agency will provide holders of the CCI Manual with updates and changes as they may become necessary. Should you have a question to the currency of this "Executive Summary" you should contact a vendor of CCI equipment, or the NSA Office of COMSEC Industrial Relations (S3).

## **II. Background:**

A. National Security Decision Directive number 145 - "National Policy on Telecommunications and Automated Information Systems Security" - was signed by the President on 17 September 1984. One of the major features of this document was the establishment of national goals and responsibilities for securing classified information, and sensitive unclassified information, during automated processing and telecommunications. The Director, National Security Agency (NSA) was designated as the National Manager for Communications Security (COMSEC), and given a mandate to take necessary actions to protect the classified and sensitive communications not only of Government, but of American industry as well. Special emphasis was to be placed on the sensitive/classified communications of U.S. Government contractors.

B. In its effort to improve the COMSEC posture of Government contractors, the Director, NSA, issued a directive (NACSI 6002) which:

1. Requires all Government Departments and Agencies to identify the COMSEC requirements for all contract-related telecommunications.

2. Allows contractors' COMSEC costs to be charged to the contract in the same manner as other security costs.

C. With the issuance of NACSI 6002, and the increasing awareness on the part of industry and Government of the need for security in telecommunications, an increased demand for COMSEC equipment created the need for an increased supply. NSA responded to this need by creating several new Government-industry business relationships for the manufacture of COMSEC products, and by tailoring the control requirements for COMSEC equipments more closely to the needs of the user and his application.

1. With respect to the acquisition of COMSEC products, there are now several ways a Government contractor may obtain them:

a. As Government-owned, and Government-Furnished Property (GFP).

b. As Government-owned, and Contractor-Acquired Property (CAP).

c. As Contractor-Owned Property (COP).

2. In all three cases, the COMSEC equipment may be shipped directly from the manufacturer to the user.

3. With respect to the tailoring of the control requirements for COMSEC equipment, the most important features have been:

a. The declassification of formerly classified COMSEC equipments.

b. The creation of a new "Unclassified, but Controlled" category, called Controlled Cryptographic Item, or CCI. COMSEC equipments designated as CCI may be used, with appropriately classified keying material, to secure classified and unclassified telecommunications. They may also be used, with unclassified keying material, to protect unclassified telecommunications.

D. With these changes, it became clear that a single document was needed which would bring together all of the procedures, doctrine, and requirements pertaining to the acquisition and ownership, transportation, physical security and access control, accounting, TEMPEST countermeasures, insecurity reporting, keying, and disposition of CCI equipments in the Government contractor environment. The result was the February 1986 publication by NSA of the U.S. Government Contractors CCI Manual.

1. The CCI Manual addresses all appropriate aspects of contractor use of CCI equipment in both the unclassified and classified applications.

2. Its provisions apply to all U.S. Government contractors who use or otherwise handle CCI equipment. Because CCI equipment - although it is itself unclassified - can process either classified or unclassified communications, the CCI Manual incorporates many of the existing rules for protecting classified information. The requirements for contractor protection of classified information and materials are administered under the Industrial Security Program, and the provisions of:

a. DoD 5220.22-M, the "Industrial Security Manual for Safeguarding Classified Information," dated December 1985, and;

b. DoD 5220.22-S-1, the "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information," dated 12 August 1983.

3. U.S. Government contractors who do not have classified information, and who will be using CCI equipment to secure only unclassified telecommunications, are not subject to the "Industrial Security Manual for Safeguarding Classified Information" and its COMSEC Supplement.

### III. Questions Concerning CCI Equipment:

A. The following questions address those aspects of the acquisition and use of CCI equipment of which a potential purchaser or user should be aware.

Q. "Is CCI the right level of equipment for my application?"

A. There are three general "levels" of cryptographic equipments which employ Government cryptography.

1. There are some COMSEC equipments which are classified. These equipments are authorized for the protection of both classified and unclassified communications. They are not available for contractor ownership,

and generally are not available for direct acquisition as Contractor-Acquired Property. They are normally obtained as Government-Furnished Property. Contractors must meet all the requirements of the Industrial Security Program to obtain and operate classified equipments. If you think that a classified COMSEC equipment may meet your particular application, check with your Government contracting office for additional information.

2. Other COMSEC equipments are designated as CCI. CCI equipments may be used to protect classified or unclassified telecommunications, and are generally available for direct acquisition from the manufacturer as GFP, CAP, or COP. Although CCI equipments are unclassified, there are significant Government requirements for their control, of which the potential user should be aware. If your application involves the protection of classified information, or may involve a future need to protect classified information, CCI equipment may be appropriate.

3. A third category of equipments is limited to the protection of unclassified telecommunications. If your application is strictly limited to the protection of unclassified information, you may want to investigate the availability of appropriate equipments in this category. The only control on these equipments is that they may not be exported.

Q. "What do I have to do to qualify to purchase and use CCI equipment?"

A. There are three general requirements.

1. In order to obtain and use CCI equipment, the contractor must have or establish a COMSEC Account, accountable to an appropriate Government Central Office of Record (COR), which is normally NSA. Before a COMSEC account can be formally established, if the contractor has a facility clearance issued by the Defense Investigative Service (DIS), he must forward a copy of his most recently completed Form 441s (together with any updates or changes) to NSA. If the contractor does not have a facility clearance issued by DIS, then he must complete the attached "Certificate Pertaining to Foreign Interests" and have it reviewed and approved by NSA.

2. Second, the contractor must also have at least one current U.S. Government contract at the time the CCI equipment is acquired.

3. A third requirement is that the contractor must have executed a "CCI Control Agreement" with NSA. The "CCI Control Agreement" is a legally binding agreement in which the contractor agrees to comply with all the requirements of the CCI Manual for as long as the contractor has use of CCI equipment. Vendors of CCI equipment are required to verify with NSA that a potential purchaser is qualified to receive the equipment before it may be shipped. To illustrate the process, there are seven basic steps involved in a contractor's purchase of CCI equipment:

a. Send the most recent Form 441s or the completed "Certificate Pertaining to Foreign Interests" (attached to this Executive Summary) to NSA, attention Y13.

b. After NSA review, NSA/Y13 will send a copy of the CCI Manual to the buyer with a request for return of the Manual should the transaction not be completed. The CCI Manual contains a copy of the "CCI Control Agreement," which may be duplicated by the buyer.

c. The buyer then submits a package to NSA/Y13 containing:

(1) A certification and reference of his U.S. Government contract number.

(2) A request for establishment of a COMSEC account (if one doesn't already exist).

(3) A completed "CCI Control Agreement."

(4) A copy of the contractor's Government Contracting Office authorization to purchase the CCI equipment, if the purchase is to be Contractor-Acquired Property.

d. NSA (Y13) then supplies a COMSEC account number and appropriate account information to the buyer.

e. The buyer certifies to the CCI vendor that he has a COMSEC account (providing the vendor with account number and shipping address), and that he has executed a "CCI Control Agreement" with NSA.

f. The vendor then verifies with NSA that the purchaser is authorized to receive CCI equipment, and that the COMSEC account information is correct. (NSA checks the purchaser's COMSEC account, CCI Control Agreement status, contract status, and category of purchase, i.e., as contractor owned, or acquired property).

g. After NSA verification, the vendor ships the CCI equipment to the purchaser.

Q. "Can I own CCI equipment, or is ownership retained by the Government?"

A. Either situation or combination of the two is possible, depending on the circumstances.

1. A qualified contractor (as defined in the answers to the previous question) may purchase CCI equipment with his own funds as contractor-owned property (COP) plant equipment, as defined in Federal Acquisition Regulation (FAR) 45.101(a). The only additional restriction is that contractors organized and existing under the laws of a U.S. possession or trust territory may not own CCI equipment, except under special circumstances and with specific authorization from NSA.

2. Government ownership of CCI equipment is retained if it is provided to the contractor by the Government as Government-Furnished Property (GFP), as defined in FAR, 45.101(a). The contractor's Government contracting office may have CCI COMSEC requirements for the contract. In this case, where the contractor is otherwise qualified to obtain CCI equipment as GFP, the contractor may arrange purchase of additional CCI equipment to meet other COMSEC needs.

3. CCI equipment purchased by contractor and charged to a Government contract(s) is Contractor-Acquired Property (CAP) as defined in FAR 45.101(a). In this case, ownership remains with the Government. As in the case of GFP above, otherwise qualified contractors may purchase additional CCI equipment as Contractor-Owned Property (COP).

Q. "What information is contained in the Government Contractor CCI Manual?"

A. The CCI Manual is a large document, of approximately 200 pages, organized with a brief introductory section followed by ten annexes. The information covered includes:

Annex A - Acquisition:

This annex and its appendices describe the criteria for owning CCI equipment, and the procedures and requirements to be followed in acquiring CCI equipment.

Annex B - COMSEC Accounts:

This annex describes the procedures and requirements for establishing, operating, and closing formal COMSEC accounts and sub-accounts. It addresses both classified and unclassified accounts, as well as the responsibilities of personnel involved (e.g., COMSEC custodian).



#### Annex C - Accounting Procedures:

This annex and its appendix provide detailed accounting procedures for COMSEC accounts and sub-accounts. Sample forms are contained in an appendix to this annex.

#### Annex D - Physical Security:

This annex and its appendices contain the minimum physical security and access controls required for CCI equipment, keying materials, and other related materials. Its appendices contain a cryptographic access briefing, information on destruction devices, copies of public laws relating to CCI and classified information, and guidance on the items to be included in a local facility Standard Practice Procedure (SPP).

#### Annex E - TEMPEST:

This annex describes the Government requirements for protecting against classified information compromise due to system electrical emanations. It is classified CONFIDENTIAL.

#### Annex F - Keying Material Management:

This annex discusses key management, with emphasis on the procedures for acquiring keying materials, the establishment of cryptonets, responsibilities of a controlling authority, and specific requirements for a Keying Materials Support Plan (KMSP).

#### Annex G - Insecurity Reporting:

This annex and its appendix address the reporting of insecurities associated with CCI equipments, keying materials, and related materials.

#### Annex H - System Certification and Configuration Control:

This annex describes the requirements for system certification and configuration control. It addresses the responsibilities and procedures for pre-installation site surveys, site preparation, site inspection, installation, installation inspection, certification, and continuing systems configuration control.

#### Annex I - Authorized Vendor Equipment:

This annex and its appendices describe the particular CCI equipment available from authorized vendors. Included are a brief description of the

equipment; the vendor names, addresses, and points of contact; and any additional, system-specific requirements for control or operation, e.g., unique procedures for obtaining keying materials.

#### Annex J - Glossary:

This annex lists definitions of terms and acronyms used in the CCI Manual, as well as other frequently used COMSEC terms.

Q. "Where can I find out about current vendors of CCI equipment?"

A. If you have a copy of the CCI Manual, they are listed in Annex I. They are frequently listed in other NSA publications, e.g., the Industrial Telecommunications Protection Bulletin. Otherwise, you should call or write to the NSA Office of COMSEC Industrial Relations (S3) at the address/phone number listed in section I of this summary.

Q. "What are my responsibilities for physically controlling CCI equipment?"

A. This depends on several factors, such as whether or not the CCI equipment is keyed, what type of key (classified or unclassified) is installed in it, whether it is attended by persons who are authorized access, etc.

1. The contractor's fundamental responsibility for CCI equipment is that he treat it as high-value equipment, prevent its loss or theft, and provide additional protection as the sensitivity/classification level of the keying material may dictate.

2. The CCI Manual defines "access" to CCI equipment as "installing, troubleshooting, maintaining, and keying" the equipment. For contractor personnel to have this access, they must meet the following requirements:

a. Be a U.S. citizen whose duties specifically require access.

b. Be indoctrinated on the importance of safeguarding CCI equipment and keying materials. The contractor is responsible for ensuring that all personnel who have access to CCI equipment have been given the briefing contained in the CCI Manual.

c. Be familiar with the contents of the contractor's Standard Practice Procedure (SPP), which will contain the information called for in the CCI Manual.

d. If classified keying material is used, possess a security clearance at least equal to the keying material used by the CCI equipment during a period of access.

3. Unescorted users of keyed CCI equipment or its connected telecommunications systems who do not require "access" as defined above must:

- a. Be familiar with the CCI sections of the contractor's SPP.
- b. Have an appropriate security clearance, if the CCI equipment is keyed with classified keying material.

4. Unkeyed CCI equipment is treated as high-value equipment, and the contractor is responsible for preventing loss, theft, or unauthorized removal.

5. Keyed CCI equipment is protected according to the requirements of the installed key. If the key is classified, then the equipment must either be under the positive control of personnel who have the appropriate security clearance, or it must be physically secured at a level commensurate with the key. These physical requirements are detailed in the CCI Manual. If the installed key is unclassified, the contractor is responsible for preventing access by unauthorized personnel through the use of physical controls adequate to the local facility (e.g., locked rooms, alarms, random checks, etc.), or monitoring and positive control by authorized personnel.

Q. "How can I transport CCI equipment?"

A. First you make sure the equipment is unkeyed. If the move is local (e.g., within a building), then the move may be performed by any contractor personnel who are U.S. citizens, have been given the COMSEC briefing contained in the CCI Manual, and who are completely familiar with the local SPP for CCI equipment.

1. If the move is to another building, or to another COMSEC account or sub-account, then the CCI equipment will be transported by:

a. Authorized Government courier service (e.g., ARFCOS, Diplomatic Courier Service); or

b. NSA-approved commercial carriers; or

c. Authorized contractor/company couriers (couriers must be authorized access to CCI equipment, and be specifically designated by the Government Contracting Office, or by the local Facility Security Supervisor. There are several other administrative requirements for company couriers detailed in the CCI Manual); or

d. U.S. Registered Mail

Q. "What are the requirements for destruction of CCI equipments?"

A. Government contractors will not destroy any CCI equipment without the specific written approval of NSA. In cases where destruction is authorized, it will be performed only in accordance with NSA-prescribed procedures. CCI equipments may be returned to the Government for destruction. Contractors should require destruction (or return) approval through their Government contracting office. If there is no appropriate Government contracting office, the contractor should address his request for destruction instructions to NSA, attention Y13.

Q. "What are my responsibilities in accounting for CCI equipment?"

A. Government contractors holding CCI equipment must maintain an active formal COMSEC account, responsible to a Government Central Office of Record (COR), and continuously account for each CCI equipment by serial number. The COR for contractor accounts will normally be NSA. The contractor is also responsible for ensuring that CCI equipments are accounted for, by serial number, when they are transferred to another COMSEC account. Accounts can be established which handle only unclassified equipment and materials. If a COMSEC account already exists to account for classified equipment and materials, it can also be used to account for CCI equipment, all of which are unclassified.

1. The detailed procedures for establishing COMSEC accounts and sub-accounts, and for designating a COMSEC Custodian, are contained in Annex B of the CCI Manual.

2. The COMSEC account Custodian is required to perform an annual physical-sight inventory of all CCI equipments charged to the account against the COR's inventory listing for that account.

3. Special inventories may be required of the COMSEC Custodian when directed by the account's COR, the U.S. Government Contracting Officer (if applicable), or the local Facility Security Supervisor, for reasons of suspected loss of CCI equipment or other accountable COMSEC material, or for frequent deviation from normal accounting procedures.

4. COMSEC accounts will be audited at least once annually by the appropriate COR. This audit includes verification of the completeness and accuracy of the account's reports and files, physical sighting of all accountable equipment and materials, and compliance with standard packing, marking, and related procedures.

Q. "Are there any additional requirements associated with using CCI equipment?"

A. In all cases there are some system/installation certification requirements, and depending on the sensitivity of the application (particularly if classified information is to be processed), there may be additional requirements for systems configuration control, system certification and recertification, and special restrictions required by the Government Contracting Office. Briefly, these may include the following:

1. When CCI equipment is initially placed into a new installation (in contrast to one which already has CCI equipment installed), the user is responsible for ensuring that the site meets all the physical security requirements of the CCI Manual.

2. Before the CCI equipment may be used with operational keying materials, the installation must be inspected and approved for operation.

a. If classified keying material is to be used, the Facility Security Supervisor (FSS) must inspect and approve that the area(s) which will contain the CCI equipment, the classified key, and other classified material, meet the applicable physical security requirements of the CCI Manual. The FSS is required to provide written certification of the approval to appropriate Government officer.

b. If only unclassified keying material is to be used with the CCI equipment, the local COMSEC Custodian will perform the inspection, and prepare a written approval. This document will be retained by the COMSEC Custodian.

3. If changes are made to the installation which could affect security, a recertification must be made.

4. In certain uses of CCI equipment to secure classified information, the Government may require selected TEMPEST countermeasures.

5. For applications in which classified keying material is used with the CCI equipment, there are additional system configuration control requirements. Essentially these involve requiring the FSS to keep accurate records of the system configuration (e.g., equipment model numbers) so that changes to certified systems may be easily tracked by the user and by Government auditors.

6. As noted in the response to an earlier question, the particular Government contracting Department or Agency may have special requirements unique to its application of CCI equipment.

Q. "What if I already have a COMSEC account, or a Cleared Facility, or both?"

A. Then you will have less processing to do to obtain the use of CCI equipment. You will not be required to establish a separate "unclassified COMSEC account" solely to handle CCI equipment; you may use your existing account. You will, however, still need to send in a Form 441s, or fill out a "Certificate Pertaining to Foreign Interests." You must also sign a "CCI Control Agreement." These are necessary to establish the status of foreign ownership, control, or interest in the contractor, and to legally bind the contractor to the requirements of the CCI Manual.

Q. "Where and how do I obtain keying material for CCI equipment?"

A. 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 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." The controlling authority may be a Government office or member of the cryptonet, or it may be a contractor office associated with the cryptonet. Usually the Controlling Authority is the member of the cryptonet in the best position to manage the security and logistical needs of the cryptonet, which includes managing the supply of keying material to all net members. 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. The KMSP is prepared by the Controlling Authority, often with the assistance of the CCI vendor, and provided to NSA so that the right types and amounts of keying material can be produced and distributed through the COMSEC material control system. A KMSP is only required for new cryptonets; if you are obtaining CCI equipment in order to join an existing cryptonet, a keying material management plan will already be in effect. The KMSP is a comprehensive document with respect to keying the cryptonet. It includes such information as:

1. The need for the cryptonet, and its operational concept.
2. The identities of the Controlling Authority and all associated Government contracting offices.
3. The keying material specification:
  - a. Format
  - b. Use and identity of cryptographic equipment
  - c. Quantities required
  - d. Dates required
  - e. Classification (if classified)
4. Distribution plan
5. Proposed carriers

Q. "Am I required to report problems, such as insecurities, to the Government?"

A. Yes. Insecurities involving cryptographic equipments, keying material, and related materials may have severely adverse effects on the security of the information which is being protected by the cryptographic system. If an insecurity exists which remains undetected or unreported, its damage may be multiplied by users of the same cryptographic system who believe that their communications are still secure. It is critically important, therefore, that potential and actual cryptographic, physical or personnel insecurities be promptly reported to proper authorities. Detailed guidance on what to report, and how to report it, is contained in the CCI Manual. An important point all users of CCI equipment should be aware of, however, is that the purpose of reporting insecurities is not to discipline, prosecute, or otherwise punish those involved. On the contrary, it is the Government's stated policy that Government and contractor personnel will not be disciplined in any way for honest security mistakes, oversights, etc. The Government's requirement for insecurity reporting exists so that appropriate measures can be taken in a timely manner to restore confidence in the security of the cryptonet. It is the Government's policy that disciplinary measures will be taken only in those cases of gross negligence or to willfully jeopardize the security of cryptographic equipment or associated materials.

Q. "Where do I obtain support services for CCI equipment, such as for maintenance and repair?"

A. Because maintenance of CCI equipment requires the use of technically qualified personnel who have granted access to CCI equipment, support services such as maintenance will normally be provided by either the CCI vendor, or arranged through your Government contracting office. Many if not all CCI vendors offer equipment support contracts as part of their marketing package. Several Government Departments and Agencies have qualified personnel available to provide similar services. Additionally, the Government may have purchased an equipment support package from the CCI vendor when it purchased CCI equipment which may have been provided to you as GFP. Your particular approach to maintenance and equipment support should be discussed and completely understood with your CCI vendor, or Government contracting office - whichever is appropriate - before you begin to operate CCI equipment.

Q. "What happens to the CCI equipment when my Government contract expires, or is terminated?"

A. The answer largely depends upon the ownership of the equipment.

1. If the CCI equipment was acquired as Contractor-Acquired Property (CAP), or Government-Furnished Property (GFP), in which case the Government retains ownership, then disposition of the equipment is at the direction of the Government contracting office. Possible disposition decisions include:

a. Direction to the contractor to return the CCI equipment to the Government for future use or for destruction.

b. Direction to the contractor to destroy the CCI equipment.

c. Direction to the contractor to retain the equipment for use on a different Government contract.

d. A purchase offer to the contractor. In this case, a contractor qualified for CCI equipment ownership would have the CCI equipment offered for his purchase and future retention.

2. If the contractor already owns the equipment as Contractor-Owned Property (COP), he would, of course, retain the equipment after the Government contract has been terminated. Under the CCI Control Agreement between the contractor and the Government, however, the contractor is still



responsible for all the control and accounting requirements contained in the CCI Manual. CCI equipment which is COP may be sold to another qualified contractor, sold back to the Government, or destroyed in accordance with the procedures contained in the CCI manual, and outlined in the response to a prior question. If you have any questions concerning the disposition of CCI equipment which is Contractor-Owned Property, you should contact NSA, attention Y13.

IV. Summary:

A. It is the Government's goal to make high-quality cryptographic equipment available for every application in which the security of classified or sensitive communications of American Government or Industry is at stake. To assist in meeting this goal, the Government has created a category of cryptographic equipments which are unclassified but controlled, and has published a U.S. Government Contractor CCI Manual to govern the use of this CCI equipment by U.S. Government contractors.

B. As the National Manager for Communications Security (COMSEC), the National Security Agency (NSA) has established an Office of COMSEC Industrial Relations (S3) to manage the overall program of Government-Industry cooperation on matters of COMSEC. That office has led the effort to produce the CCI Manual, and along with the Office of Cryptomaterial Production (Y1), stands ready to assist the users of CCI equipment in any way possible. Contractor comments on the contents of the CCI Manual, or this "Executive Summary" are welcome, and should be addressed to NSA (S3).

# CERTIFICATE PERTAINING TO FOREIGN INTERESTS

## PENALTY NOTICE

PENALTY - Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of eligibility either to participate in the Commercial COMSEC Endorsement Program (CCEP) as a vendor or to acquire CCI equipment. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$10,000 fine, or both, knowingly to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.

---

## PROVISIONS

1. This report is authorized by the Director, National Security Agency, pursuant to authority granted him by NSDD 145. While you are not required to respond, your eligibility to participate in the CCEP as a vendor or for acquisition of CCI equipment and associated materials cannot be determined if you do not complete this report. The retention of eligibility as described above is contingent upon your notifying NSA (Y13) immediately of any situation which would cause a change to the answer to any question in this report.
2. These reports are subject to the provisions of the Freedom of Information Act (FOIA), Section 552, Title 5, United States Code. Information considered proprietary information by company submitters should be so marked. Where information so marked is requested under the FOIA, the Agency will consult with the submitter company in the course of reaching its determination regarding the releasability of the information and to protect such information against disclosure as authorized by law.
3. Complete all questions on this report. Answer each question in either the "Yes" or "No" column. If your answer is "Yes" furnish in full the complete information under "Remarks".

## DIRECTIONS

**Question 1:** Identify the percentage of any class of shares or other securities issued, that is owned by foreign interests, broken down by country. If the answer is "Yes" and a copy of Schedule 13D and/or Schedule 13G filed by the investor with the Securities and Exchange Commission (SEC), has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 2:** Furnish the name, address by country, and the percentage owned. Include name and title of officials of the facility who occupy positions with the foreign entity, if any.

**Question 3:** Furnish full information concerning the identity of the foreign interest, and the position he or she holds in the organization.

**Question 4:** Identify the foreign interests(s) and furnish full details concerning the control or influence.

**Question 5:** Furnish name of foreign interest, country, and nature of agreement or involvement. Agreements include licensing, sales, patent exchange, trade secrets, agency, cartel, partnership, joint venture, and proxy. If the answer is "Yes" and copy of Schedule 13D and/or Schedule 13G filed by the investor with the SEC has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 6:** Furnish the amount of indebtedness and by whom furnished as related to the current assets of the organization. Include specifics as to the type of indebtedness and what, if any collateral, including voting stock, has been furnished or pledged. If any debentures are convertible, specifics are to be furnished.

**Question 7:** State full particulars with respect to any income from Communist countries, including percentage from each such country, as related to total income, and the type of services or products involved. If income is from non-Communist countries, give overall percentage as related to total income and type of services or products in general terms. If income is from a number of foreign countries, identify countries and include percentage of income by each country.

**Question 8:** Identify each foreign institutional investor holding 5 percent or more of the voting stock. Identification should include the name and address of the investor and percentage of stock held. State whether the investor has attempted to, or has in fact, exerted any management control or influence over the appointment of directors, officers, or other key management personnel, and whether such investors have attempted to

influence the policies of the corporation. If a copy of Schedule 13D and/or Schedule 13G filed by the investor with the SEC has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 9:** Include identifying data on all such directors. If they have a security clearance, state so. Also, the name and address of all other corporations with which they serve in any capacity.

**Question 10:** Provide complete information by identifying the individuals and the country of which they are a citizen.

**Question 11:** Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

---

## QUESTIONS

---

1. Do foreign interests own or have beneficial ownership in 5% of your organization's securities? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, to what extent? Please describe.
2. Does your organization own any foreign interest in whole or in part? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
3. Do any foreign interests have positions, such as directors, officers, or executive personnel in your organization? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
4. Does any foreign interest control or influence, or is any foreign interest in a position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel? Yes \_\_\_\_\_ No \_\_\_\_\_
5. Does your organization have any contracts, agreements, understandings, or arrangements with a foreign interest(s)? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
6. Is your organization indebted to foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
7. Does your organization derive any income from foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
8. Is 5% or more of any class of your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose the beneficial owner of equitable title? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
9. Does your organization have interlocking directors with foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ Please describe.
10. Are there any citizens of foreign countries employed by or who may visit your facility (or facilities) in a capacity which may permit them to have access to U.S. cryptographic information, or CCI equipment and related materials (exclude cleared immigrant aliens in answering this question)? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.

11. Does your organization have any foreign involvement not otherwise stated in your answers to the above questions? Yes \_\_\_\_\_ No \_\_\_\_\_ .If so, please describe.

REMARKS (Attach additional sheets, if necessary)

---

## CERTIFICATION

I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge are made in good faith.

WITNESS:

\_\_\_\_\_

\_\_\_\_\_ Date Certified

\_\_\_\_\_

BY \_\_\_\_\_

\_\_\_\_\_ Company

\_\_\_\_\_ Title

\_\_\_\_\_ Address

**NOTE:** For corporations, witnesses are not required, but the following certificate must be completed. The corporation, should execute the following certificate under its corporate seal, provided that the same officer shall not execute both the certification and the certificate. Type or print names under all signatures.

---

## CERTIFICATE

I, (name) \_\_\_\_\_ certify that I am the (title of certifier) \_\_\_\_\_ of the corporation named as Contractor herein; that (name of signatory) \_\_\_\_\_ who signed this certificate on behalf of the Contractor, was then (name of signatory) \_\_\_\_\_ of said corporation; that said certificate 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.

\_\_\_\_\_ Signature and Date



## NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MARYLAND 20758-6000

4 February 1986

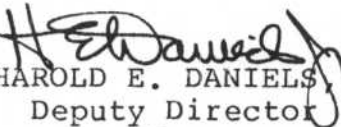
### FOREWORD

This is the first publication of the U.S. Government Contractor Controlled Cryptographic Item (CCI) Manual. Its primary objective is to describe the procedures for implementing CCI equipment and key material at U.S. Government contractor locations. Specifically, this Manual outlines the process for acquiring CCI equipment and keying material, and establishes the requirements for controlling these items.

The communications security problem in this nation is greater now than ever and it is essential that Government and Industry join in its solution. As a Government contractor your communications are vulnerable to exploitation and you must play an integral part in implementing protection to classified and sensitive information. This Manual should serve as a valuable aid to you in achieving this goal.

The individual(s) designated within your company to perform the duties outlined in this Manual are responsible for ensuring that all procedures are correctly followed and properly executed. With this in mind, U.S. Government contract classified and sensitive information will be afforded the very best communications security available.

Should you need further guidance concerning any aspect of this Manual, please contact the Office of Industrial Relations (S3), telephone (301) 688-6581. For additional copies of this Manual, please contact Y13, telephone (301) 688-8110.

  
HAROLD E. DANIELS, JR.  
Deputy Director  
for  
Information Security



**U.S. Government Contractors**

**Controlled Cryptographic Item**

**Manual**

2 February 1986

This Manual will be periodically updated and/or amended. Updates and amendments will automatically be provided in numbers equal to the number of copies of Manuals originally provided you. Although this Manual is unclassified (excluding Annex E), the information contained herein should not be locally reproduced or disseminated outside your company. Should you no longer have a need for the Manual please return it to Director, National Security Agency, ATTN: Y131, Fort Meade, Maryland 20755-6000. Use the form below as a record of changes made to the Manual.

**U.S. GOVERNMENT CONTRACTORS**

**CONTROLLED CRYPTOGRAPHIC ITEM MANUAL**

**RECORD OF CHANGES**

CHANGE NO.	AUTHORITY AND DATE OF CHANGE	DATE	SIGNATURE OF PERSON ENTERING CHANGE

**FOR OFFICIAL USE ONLY**

## TABLE OF CONTENTS

	<u>PAGE</u>
<b>INTRODUCTION</b>	
I. Purpose and Scope	1
II. Applicability	1
III. Authority	1
IV. Background	4
V. Program Description	4
VI. Organization	5
VII. Additional Information	7
<b>Annex A – Acquisition</b>	A-1
I. Introduction	A-1
II. Ownership	A-1
III. Requirements and Procedures for Acquisition of CCI Equipment	A-2
IV. Appendix 1 – CCI Control Agreement	A-1-1
V. Appendix 2 – Sample FOCI Form	A-2-1
VI. Appendix 3 – Contracting Officer's Authorization to Purchase Form	A-3-1
<b>Annex B – COMSEC Accounts</b>	B-1
I. General	B-1
II. Procedures for Establishing a Primary COMSEC Account at a Contractor Facility with the NSA as COR	B-3
III. Personnel Selection Criteria (for classified accounts)	B-4

<b>Annex B – COMSEC Accounts (Cont'd)</b>		<u>PAGE</u>
IV.	Indoctrination and Guidance for COMSEC Custodians	B-5
V.	Duties of the COMSEC Custodian, Alternate Custodian, and Facility Security Supervisor	B-6
VI.	Sub-accounts	B-10
VII.	Closing COMSEC Accounts	B-13
<b>Annex C – Accounting Procedures</b>		C-1
I.	General	C-1
II.	Receipt of Accountable COMSEC Material	C-1
III.	Transfer of COMSEC Material	C-3
IV.	CCI and COMSEC Material Inventory Reporting	C-7
V.	Destruction Reports	C-9
VI.	Audit of COMSEC Accounts	C-10
VII.	Change of COMSEC Custodian	C-12
VIII.	CCI Equipment Distribution	C-14
IX.	Forms, Reports, and Files	C-15
X.	Vendor Accounting Responsibilities	C-20
XI.	Appendix 1 – Miscellaneous Accounting Forms	C-1-1
XII.	Appendix 2 – Map of ARFCOS Stations	C-2-1
XIII.	Appendix 3 – Certificate of Action Statement	C-3-1

	<u>PAGE</u>
<b>Annex D – Physical Security</b>	D-1
I. General	D-1
II. CCI Equipment	D-2
III. Fill Devices for Loading Key	D-8
IV. Keying Material	D-8
V. Other Related Materials	D-18
VI. Transportation	D-19
VII. Displays, Demonstrations, and Marketing	D-22
VIII. Appendix 1 – Cryptographic Briefing	D-1-1
IX. Appendix 2 – Material Destruction Guidelines	D-2-1
X. Appendix 3 – NSA-Approved Paper Destruction Devices	D-3-1
XI. Appendix 4 – Reference Materials	D-4-1
XII. Appendix 5 – Facility Standard Practice Procedure	D-5-1
XIII. Appendix 6 – Company Information Form	D-6-1
<b>Annex E – TEMPEST Requirements</b>	E-1
I. General	E-1
II. Countermeasures Determination	E-2
III. Countermeasures Requirements	E-4
IV. TEMPEST Personnel Certification	E-7
V. Industrial TEMPEST Program	E-9
VI. Appendix 1 – TEMPEST Security Evaluation Form	E-1-1

	<u>PAGE</u>
VII. Appendix 2 – TEMPEST Countermeasures Determination Procedures	E-2-1
<b>Annex F – Keying Material Management</b>	F-1
I. Introduction	F-1
II. Responsibilities of a Controlling Authority	F-4
III. Considerations in Establishing a Cryptonet	F-6
IV. Keying Material Support Plan	F-7
<b>Annex G – Insecurity Reporting</b>	G-1
I. General	G-1
II. Reportable COMSEC Insecurities	G-2
III. Basic Requirements for Reporting Insecurities	G-5
IV. Types of Insecurity Reports	G-11
V. Appendix 1 – Insecurity Evaluation Guidance	G-1-1
<b>Annex H – System Certification and             Configuration Control</b>	H-1
I. Introduction	H-1
II. Certification	H-1
III. Configuration Control	H-4

	<u>PAGE</u>
<b>Annex I - Authorized Vendor Equipment</b>	I-1
I. Appendix 1 - KY-71/71A	I-1-1
II. Appendix 2 - Key Ordering Form	I-2-1
III. Appendix 3 - KG-84A	I-3-1
IV. Appendix 4 - KOI-18, KYK-13, and KYX-15 Fill Devices	I-4-1
<b>Annex J - Glossary</b>	J-1

# INTRODUCTION

## I. Purpose and Scope

A. The manual provides the minimum requirements for the acquisition and ownership, transportation, certified installation, physical security and access control, key accounting, determination of TEMPEST countermeasures, insecurity reporting, and disposition of CCI equipment and associated keying and other support materials at contractor facilities. Clarification on specific issues will be provided upon request.

B. This manual has been prepared to guide users, vendors, contract officers, program managers, cryptologic support elements and other entities involved in the implementation of Controlled Cryptographic Item (CCI) COMSEC equipment in support of U.S. Government contracts.

## II. Applicability

The provisions of this manual apply to all U.S. Government contractors implementing CCI equipment, whether the information which is being processed by that equipment is classified, other sensitive Government-derived information, or the contractor's corporate communications. For classified information and materials, the provisions of DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," dated December 1985, and DoD 5220.22-S-1, "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information," dated 12 August 1983, apply.

## III. Authority

A. This manual derives its authority from national policy, national directives and national instructions. The following paragraphs summarize the pertinent portions of these national documents.

### B. NSDD 145

1. National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," dated 17 September 1984, establishes as a national responsibility the securing of telecommunications and automated information systems which process and communicate classified national security information or other sensitive government-derived information, and the offering of assistance in the protection of certain private sector information.

2. NSDD 145 designated the Director, National Security Agency (DIRNSA) as the National Manager for Telecommunications and Automated Information Systems Security whose responsibilities include:



a. Acting as the government focal point for cryptography, telecommunications systems security and automated information security;

b. Prescribing the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques and information;

c. Entering into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including Government contractors and foreign governments.

C. NCSC-11

1. National COMSEC Committee (NCSC)-11, "National Policy for Protection of Telecommunications Systems Handling Unclassified National Security-related Information", dated 3 May 1982, establishes national policy for the protection of telecommunications systems handling unclassified national security-related information.

D. NACSI 6002

1. National COMSEC Instruction No. 6002, "Protection of Government Contractor Telecommunications," dated 4 June 1984, provides for the implementation of national policy which requires the protection of national security (classified) and national security-related (unclassified) telecommunications associated with U.S. Government contracts.

2. NACSI 6002 directs that:

a. Contract-related telecommunications which require communications security be identified during the contracting process and specific implementation provisions be made for such communications security.

b. Contractor's communications security costs be allowable in the same manner as they would charge other contract security costs.

c. Mechanisms must be identified by which communications security equipment can be made directly available to qualified Government contractors.

d. DIRNSA recommend alternative mechanisms by which communications security equipment can be made more readily available to qualified Government contractors.

e. Implementation planning commence immediately and should be designed to provide protection of contractor circuits within two years from the date of the Instruction (June 1984).

F. NTISSI 4001

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items" dated 25 March 1985, establishes a new category of secure telecommunications and information handling equipment, and associated cryptographic components, which are unclassified (when unkeyed) but controlled. The intent of this new category is to promote the broad use of secure telecommunications for the protection of national security (classified) and national security-related (unclassified) and other sensitive information which should be protected in the national interest while protecting against loss of this equipment to adversaries of the United States. This instruction applies to all departments and agencies of the U.S. Government, and their contractors who handle, distribute, account for, store, or use CCI equipment and associated components.

2. NTISSI 4001 assigns to the Director, National Security Agency (DIRNSA), the responsibility for establishing requirements for controlling CCI equipments and components and for issuing new or revised system doctrine for equipment designated CCI.

G. NACSI 4005

National COMSEC Instruction (NACSI) No. 4005, dated 12 October 1979, "Safeguarding and Control of Communications Security Material", prescribes the minimum standards for safeguarding and control of communications security material. NACSI 4005, Annex C., "Safeguarding COMSEC Equipment", states that additional or different controls may be prescribed by the DIRNSA for specific applications and that these take precedence over NACSI 4005. This manual provides additional and different controls for the application of CCI equipment and related materials in support of Government contract communications.

H. DoDI 5210.74

Department of Defense Instruction 5210.74, "Security of Defense Contractor Telecommunications," implements guidance to expedite securing and protecting telecommunications between and among DoD components, their contractors and subcontractors. It provides a new method for direct acquisition of COMSEC for contractor installation and maintenance of service, and for recovery of costs through the contract. Policy, procedures, and responsibilities for securing DoD contractor telecommunications are also outlined in DoDI 5210.74.

#### **IV. Background**

A. Our adversaries' attention to national security or sensitive information transmitted between and among the government and its contractors is well documented and the threat to our national interests is all too clear. Communications security is a vital element of the operational effectiveness of the national security activities of the U.S. Government and its contractors. Ensuring the security of telecommunications which process classified and sensitive information and offering assistance in the protection of private sector information are national responsibilities.

B. In the past, limited quantities of COMSEC equipment have been provided to contractors as Government Furnished Property. The Government's ability to satisfy its own need for COMSEC within currently available inventories tends to place contractors at a disadvantage in competing for these scarce resources.

#### **V. Program Description**

A. Acting on its responsibility to secure contract related communications, the NSA, in conjunction with other government elements, has taken a number of initiatives to make secure telecommunications products much more readily available for government contractors. These initiatives include:

1. Authorizing certain COMSEC contractors to market their COMSEC products and offer support services directly to government contractors;
2. Encouraging and assisting the commercial telecommunications industry in the integration of COMSEC functions into their products;
3. Tailoring, and in the process relaxing, the physical security and access controls on COMSEC equipment and on TEMPEST requirements in the United States;
4. Declassifying certain COMSEC equipment;
5. Assisting industry in becoming aware of the need for and implementing secure telecommunications.

B. A large scale implementation of secure communications equipment can take place only by making some significant changes in the way this equipment is acquired and controlled.

1. Vendors have been authorized to directly market and sell CCI equipment and offer support services (e.g., installation and maintenance) to

permit a more readily available source of high-grade COMSEC for the protection of classified as well as sensitive unclassified information. This essentially makes high-grade cryptography for the securing of classified and sensitive unclassified communications as available to authorized users as other protection equipment which is limited in application to unclassified communications.

2. The CCI equipment category, and its associated relaxed physical security requirements, has been created to facilitate the implementation of this high-grade COMSEC. However, to ensure the security integrity of the system within which the CCI equipment is used and to protect our national cryptographic interests, there must be certain requirements for controlling the CCI equipment. These requirements include:

a. Limiting the ownership of CCI equipment to U.S. Government elements or eligible U.S. Government contractors. This requirement is implemented for Government contractors by executing a CCI Control Agreement between the NSA and the contractor. This agreement binds the contractor to the requirements of this manual and prescribes conditions for the resale and/or other disposition of the CCI equipment.

b. Limiting access to U.S. citizens and requiring a cryptographic access briefing for all who need access;

c. Accounting of the CCI equipment by serial number via a formal accounting system with an annual inventory requirement. This will include the establishment of a COMSEC account under a Central Office of Record (COR), where one does not already exist, in accordance with the procedures of this manual.

d. Protecting the CCI equipment as other high value property.

e. Controlling keying materials in a manner commensurate with their sensitivity and/or classification.

f. Implementing TEMPEST countermeasures only when the information being processed is at the SECRET or higher classification level, and then only when in accordance with Annex E of this Manual.

g. Certifying that CCI equipment installations are in accordance with the requirements of this manual.

## **VI. Organization**

This manual is divided into a number of annexes with supporting appendices as necessary. Each of these annexes addresses a major element necessary for the implementation of CCI equipment in support of securing

contract related communications. The following provides a brief summary of the contents of the various annexes.

A. Annex A - Acquisition

This annex and its appendices describe the criteria for owning CCI equipment, the eligibility requirements to acquire this equipment and procedures to be followed for acquiring CCI equipment.

B. Annex B - COMSEC Accounts

All CCI equipment, keying material and certain support materials (e.g., CCI equipment depot repair manuals) are to be accounted for in a formal COMSEC accounting system. This annex describes the procedures for establishing and closing classified and unclassified COMSEC accounts and sub-accounts. It includes the criteria for selecting the account custodian, his alternate, as well as a description of their duties and, when applicable, the duties of the Facility Security Supervisor.

C. Annex C - Accounting Procedures

This annex and its appendices complement Annex B by describing in detail the various procedures for operating COMSEC accounts and sub-accounts. Topics which are addressed include receipting for accountable material, transferring material, inventory reporting (e.g., CCI equipment requires an annual inventory), auditing the accounts, and CCI equipment shipment. The annex also provides sample forms used in the accounting system and a description of the files that are to be maintained in support of an account.

D. Annex D - Physical Security

This annex and its appendices describe the minimum physical security and access controls required for the implementation and support for CCI equipment, keying material and other related items, such as manuals. It addresses the requirements for access and physical security for keyed and unkeyed equipment, protected distribution systems, storage, maintenance personnel, transportation, disposition and destruction, and displays and demonstrations.

E. Annex E - TEMPEST

This annex and its appendices describe the requirements for complying with current national TEMPEST policy. It includes a summary of current national policy, a description of the basic TEMPEST countermeasures that can be implemented and the requirements for each, a procedure for determining which countermeasures to select and description of the qualifications for TEMPEST certified personnel. This annex is classified

CONFIDENTIAL and will not be included in the manual. It will, however, be provided to selected recipients when needed.

F. Annex F - Keying Material Management

This annex addresses the subject of keying material management. It includes a description of the responsibilities of a cryptographic network controlling authority, procedures for the selection of a controlling authority, the steps involved in the establishment of a cryptographic network, the procedure for acquiring key and the requirements for a Keying Material Support Plan and the procedures for its periodic review.

G. Annex G - Insecurity Reporting

This annex and appendix address the reporting of any insecurities associated with CCI equipment, keying material, and related materials. It addresses the categories of insecurities (i.e. cryptographic, personnel, physical), the basic requirements for reporting, reporting procedures, the responsibilities for report preparation and evaluation, and the types of reports. It also provides guidance for making evaluations of reported insecurities.

H. Annex H - System Certification and Configuration Control

This annex describes the requirements for system certification and configuration control. It addresses the responsibilities and procedures for pre-installation site surveys, site preparation, site inspection, installation, installation inspection, certification, and continuing system configuration control.

I. Annex I - Authorized Vendor Equipment

This annex and its appendices describe the equipment available from authorized vendors for securing contract related communications. It includes a brief description of the equipment capabilities; the vendor(s) name, address and point of contact; any unique access and physical security requirements in addition to those addressed in Annex D; and, as applicable, any other special requirements, such as unique procedures for obtaining key material.

J. Annex J - Glossary

The glossary lists descriptions and definitions of terms and acronyms used in this manual, plus other frequently used COMSEC terms.

**VII. Additional Information**

A. The NSA Office of Industrial Relations (S3) is responsible for providing assistance to U.S. industry in the application of secure

communications systems for the protection of classified and unclassified national security communications.

B. For additional information or questions concerning any aspects of this effort to secure industrial communications, or the contents of this manual, write to Director NSA, ATTN: S3, 9800 Savage Road, Ft. George G. Meade, Maryland, 20755-6000 or phone the S3 office on (301) 688-6581.

## **ANNEX A**

### **OWNERSHIP AND ACQUISITION**

#### **I. Introduction**

This annex describes the criteria for CCI equipment ownership and the requirements and procedures for acquiring CCI equipment directly from NSA authorized vendors in support of U.S. Government contractor secure communications requirements. It is recognized that there may be a distinction between the owner and the actual user of the CCI equipment. Specific references are made to each as appropriate.

#### **II. Ownership**

A. The currently available Government-Furnished Property mechanism does not alone provide enough flexibility to satisfy the requirement to provide secure communications for U.S. Government contractors as directed in the provisions of NACSI 6002. This necessitates that there be new options for acquiring and owning CCI equipment. These options include contractor acquisition and ownership of the CCI equipment. The ownership categories are:

##### **1. Government owned**

a. CCI equipment purchased by a U.S. Government department or agency and furnished to a contractor as Government-Furnished Property (GFP), as defined in Federal Acquisition Regulation (FAR), 45.101(a).

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

2. Contractor-Owned -- CCI equipment purchased by a contractor as plant equipment, as defined in FAR 45.101(a).

B. 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 to U.S. Government departments and agencies and their contractors as follows:

1. Any U.S. Government department or agency may purchase and own CCI equipment.

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

a. 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. in accordance with applicable U.S. export regulations.

b. 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 a plant equipment, except with the prior approval of the National Security Agency, Deputy Director for Information Security (NSA/DDI) based on a case-by-case review in accordance with applicable guidelines.

c. 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 interest of the U.S.

### **III. Requirements and Procedures for Acquisition of CCI Equipment**

This section addresses the requirements and procedures for the acquisition and use of CCI equipment by U.S. Government contractors by each of the following methods: Government-Furnished Property (purchased by a Government department or agency and provided to the contractor); Contractor-Acquired Property (CAP) (purchased by a contractor and charged directly to the government contract for which it was acquired); and Contractor-Owned Property (plant equipment). A chart depicting the CCI direct sales process is provided at Figure A.1.

#### **A. Government-Furnished Property**

When the purchaser is a U.S. Government department or agency and the CCI equipment is to be provided as GFP to a U.S. Government contractor, these requirements and procedures shall be followed:

1. Contractors to whom the CCI equipment will be furnished as Government Furnished Property must provide the following information to NSA:

a. Copy of the most recently completed Form DD 441s, Certificate Pertaining to Foreign Interests and any amendments thereto, if the contractor has a facility clearance (Step 3, Figure A.1.);

b. Completed Certificate Pertaining to Foreign Interests (form provided in Executive Summary to this Manual and in Appendix 2 to this Annex), if the contractor does not have a facility clearance (Step 3, Figure A.1.);

c. Executed CCI Control Agreement (Appendix 1 of this Annex) (Step 5, Figure A.1) and;

d. Request for the establishment of a COMSEC account in accordance with the requirements of Annex B of this Manual. (Step 5, Figure A.1).

Eligibility to use Government-Furnished CCI equipment cannot be determined until each of these forms have been submitted to and evaluated by NSA. If the contractor already has a COMSEC account, he must complete these forms before CCI equipment may be transferred to his account. All forms and any questions shall be addressed to: NSA, Ft. George G. Meade, MD 20755-6000, ATTN: Y13.

2. Normally, NSA will act as the Central Office of Record (COR); Annex B to this manual describes the procedures for establishing a COMSEC account with the NSA COR. Some other departments and agencies of the Government operate COR's and their procedures for establishing a contractor account may vary somewhat from Annex B. Annex C describes the accounting procedures which must be followed for controlling CCI equipment which has been implemented at contractor facilities regardless of who operates the COR. When the GFP is returned to U.S. Government department or agency possession, it may then be placed into the CCI equipment accounting system approved for use by that department or agency.

3. The government purchaser must:

a. Ensure that CCI equipment is furnished only to those contractors with a current Government contract, who have a COMSEC account which can receive CCI and have executed a CCI Control Agreement with NSA.

b. Certify to the vendor that he is a U.S. Government department or agency and that the contractor(s) to whom he will furnish the CCI

equipment has a COMSEC account which can receive CCI and has executed a CCI Control Agreement with NSA.

c. Provide the vendor the address of the appropriate COR, and the COMSEC account number and shipping address of the location to which the CCI equipment is to be shipped.

4. Prior to shipment, the vendor shall verify the shipping address with the appropriate COR. If shipment is direct to a sub-account the above verification will be obtained from the primary COMSEC account.

#### **B. Contractor-Acquired Property**

When the CCI equipment is to be purchased by a U.S. Government contractor as Contractor-Acquired Property, as defined in FAR 45.101(a), under the method described in DoDI 5210.74, these requirements and procedures shall be followed:

1. Each existing contract(s) which requires the transmission of classified or sensitive Government information shall contain a specific statement of any requirements for securing or protecting telecommunications (FAR amendments pending).

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 protecting 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 III.C below).

3. The Contractor who will be purchasing CCI equipment as Contractor-Acquired Property must provide the following information to NSA:

a. Copy of the most recently completed Form DD 441s, Certificate Pertaining to Foreign Interests and any amendments thereto, if the contractor has a facility clearance (Step 3, Figure A.1.);

b. Completed Certificate Pertaining to Foreign Interests (form provided in Executive Summary to this Manual and in Appendix 2 to this Annex), if the contractor does not have a facility clearance (Step 3, Figure A.1.);

c. Executed CCI Control Agreement (Appendix 1 of this Annex) (Step 5, Figure A.1) and;

d. Request for the establishment of a COMSEC account in accordance with the requirements of Annex B of this Manual. (Step 5, Figure A.1).

e. Completed Contracting Officer's Authorization to Purchase COMSEC Equipment as Contractor Acquired Property signed by the Government Contracting Officer (Appendix 3 of this Annex; Step 5, Figure A.1).

Eligibility to purchase CCI equipment as Contractor-Acquired property cannot be determined until each of these forms have been submitted to and evaluated by NSA. If the contractor already has a COMSEC account, he must complete these forms before CCI equipment may be transferred to his account. All forms and any questions shall be addressed to: NSA, Ft. George G. Meade, MD 20755-6000, ATTN: Y13.

4. Normally, NSA will act as the COR; Annex B to this Manual describes the procedures for establishing a COMSEC account with the NSA COR. Some other departments and agencies of the Government operate CORs and their procedures for establishing a contractor account may vary somewhat from Annex B. Annex C describes the accounting procedures which must be followed for controlling CCI equipment which has been implemented at contractor facilities regardless of who operates the COR. When the Contractor-Acquired Property is returned to U.S. Government department or agency possession, it may then be placed into the CCI equipment accounting system approved for that department or agency.

5. The contractor must certify to the vendor that he has a COMSEC account, a current U.S. Government contract(s) and that he has executed a CCI Control Agreement with NSA. He must provide the vendor the address of the appropriate COR, and his COMSEC account number and shipping address.

6. Prior to shipment, the vendor shall confirm with the NSA COR the eligibility of the Contractor to receive the CCI equipment. (Step 8, Figure A.1). This step must be completed for each and every sale.

7. When the contract for which the CCI equipment was acquired is no longer executory, the contractor may, at the discretion of the Government, either purchase it at cost in accordance with FAR 45.605-1(a), (assuming all other ownership criteria of II.B. are met), or request retention/disposition instructions from the CO.

#### C. Contractor-Owned Property

In addition to the Contractor-Acquired Property acquisition described in Section B., CCI equipment may be purchased by contractors as plant equipment. When the CCI equipment is to be purchased and owned by a U.S. Government contractor the following requirements and procedures shall be followed:

1. The Contractor who will be purchasing CCI equipment as plant equipment must provide the following information to NSA:

a. Copy of the most completed Form DD 441s, Certificate Pertaining to Foreign Interests and any amendments thereto, if the contractor has a facility clearance (Step 3, Figure A.1.);

b. Completed Certificate Pertaining to Foreign Interests (form provided in Executive Summary to this Manual and in Appendix 2 to this Annex), if the contractor does not have a facility clearance (Step 3, Figure A.1.);

c. Executed CCI Control Agreement (Appendix 1 of this Annex) (Step 5, Figure A.1) and;

d. Request for the establishment of a COMSEC account in accordance with the requirements of Annex B of this Manual. (Step 5, Figure A.1).

Eligibility to purchase CCI equipment as Contractor-Owned property cannot be determined until each of these forms have been submitted to and evaluated by NSA. If the contractor already has a COMSEC account, he must complete these forms before CCI equipment may be transferred to his account. All forms and any questions shall be addressed to: NSA, Ft. George G. Meade, MD 20755-6000, ATTN: Y13.

2. Normally, NSA will act as the COR. Annex B to this Manual describes the procedures for establishing a COMSEC account with the NSA COR. Some other departments and agencies of the Government operate COR's and their procedures for establishing a contractor account may vary somewhat from Annex B. Annex C describes the accounting procedures which must be followed for controlling CCI equipment which has been implemented at contractor facilities regardless of who operates the COR.

3. The contractor must certify to the vendor that he has a Government contract(s), a COMSEC account, and that he has executed a CCI Control Agreement with NSA (Step 7, Figure A.1). He must provide the vendor the address of the appropriate COR, and his COMSEC account number and shipping address.

4. Prior to shipment, the vendor shall confirm with NSA the eligibility of the contractor to receive CCI equipment and verify the address with the appropriate COR (Step 8, Figure A.1.). If shipment is direct to a sub-account, the account number and shipping address must be verified with the primary COMSEC account. This step must be completed for each and every sale.

# APPENDIX 1 TO ANNEX A

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 Government Contractor CCI Manual (Manual), 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 Manual 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 Manual 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 Manual.

(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 Manual, 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 Manual, (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 Agency 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 Manual and the terms of this Agreement. Should the Agency 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 Manual 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 Agency 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. Users who do not have a facility clearance shall report to the Agency whenever there is a change in the corporate structure related to the FOCI factors specified in the Certificate Pertaining to Foreign Interests (Annex A, Appendix 2 of Manual). 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's 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 (see reverse) 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 an in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

\_\_\_\_\_  
(Signature)

## APPENDIX 2 TO ANNEX A

### CERTIFICATE PERTAINING TO FOREIGN INTERESTS

#### PENALTY NOTICE

**PENALTY** - Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of eligibility either to participate in the Commercial COMSEC Endorsement Program (CCEP) as a vendor or to acquire CCI equipment. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$10,000 fine, or both, knowingly to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.

---

#### PROVISIONS

1. This report is authorized by the Director, National Security Agency, pursuant to authority granted him by NSDD 145. While you are not required to respond, your eligibility to participate in the CCEP as a vendor or for acquisition of CCI equipment and associated materials cannot be determined if you do not complete this report. The retention of eligibility as described above is contingent upon your notifying NSA (Y13) immediately of any situation which would cause a change to the answer to any question in this report.
2. These reports are subject to the provisions of the Freedom of Information Act (FOIA), Section 552, Title 5, United States Code. Information considered proprietary information by company submitters should be so marked. Where information so marked is requested under the FOIA, the Agency will consult with the submitter company in the course of reaching its determination regarding the releasability of the information and to protect such information against disclosure as authorized by law.
3. Complete all questions on this report. Answer each question in either the "Yes" or "No" column. If your answer is "Yes" furnish in full the complete information under "Remarks".

## DIRECTIONS

**Question 1:** Identify the percentage of any class of shares or other securities issued, that is owned by foreign interests, broken down by country. If the answer is "Yes" and a copy of Schedule 13D and/or Schedule 13G filed by the investor with the Securities and Exchange Commission (SEC), has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 2:** Furnish the name, address by country, and the percentage owned. Include name and title of officials of the facility who occupy positions with the foreign entity, if any.

**Question 3:** Furnish full information concerning the identity of the foreign interest, and the position he or she holds in the organization.

**Question 4:** Identify the foreign interests(s) and furnish full details concerning the control or influence.

**Question 5:** Furnish name of foreign interest, country, and nature of agreement or involvement. Agreements include licensing, sales, patent exchange, trade secrets, agency, cartel, partnership, joint venture, and proxy. If the answer is "Yes" and copy of Schedule 13D and/or Schedule 13G filed by the investor with the SEC has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 6:** Furnish the amount of indebtedness and by whom furnished as related to the current assets of the organization. Include specifics as to the type of indebtedness and what, if any collateral, including voting stock, has been furnished or pledged. If any debentures are convertible, specifics are to be furnished.

**Question 7:** State full particulars with respect to any income from Communist countries, including percentage from each such country, as related to total income, and the type of services or products involved. If income is from non-Communist countries, give overall percentage as related to total income and type of services or products in general terms. If income is from a number of foreign countries, identify countries and include percentage of income by each country.

**Question 8:** Identify each foreign institutional investor holding 5 percent or more of the voting stock. Identification should include the name and address of the investor and percentage of stock held. State whether the investor has attempted to, or has in fact, exerted any management control or influence over the appointment of directors, officers, or other key management personnel, and whether such investors have attempted to

influence the policies of the corporation. If a copy of Schedule 13D and/or Schedule 13G filed by the investor with the SEC has been received, attach a copy of Schedule 13D and/or Schedule 13G.

**Question 9:** Include identifying data on all such directors. If they have a security clearance, state so. Also, the name and address of all other corporations with which they serve in any capacity.

**Question 10:** Provide complete information by identifying the individuals and the country of which they are a citizen.

**Question 11:** Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

---

## QUESTIONS

---

1. Do foreign interests own or have beneficial ownership in 5% of your organization's securities? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, to what extent? Please describe.
2. Does your organization own any foreign interest in whole or in part? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
3. Do any foreign interests have positions, such as directors, officers, or executive personnel in your organization? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
4. Does any foreign interest control or influence, or is any foreign interest in a position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel? Yes \_\_\_\_\_ No \_\_\_\_\_
5. Does your organization have any contracts, agreements, understandings, or arrangements with a foreign interest(s)? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
6. Is your organization indebted to foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
7. Does your organization derive any income from foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
8. Is 5% or more of any class of your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose the beneficial owner of equitable title? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.
9. Does your organization have interlocking directors with foreign interests? Yes \_\_\_\_\_ No \_\_\_\_\_ Please describe.
10. Are there any citizens of foreign countries employed by or who may visit your facility (or facilities) in a capacity which may permit them to have access to U.S. cryptographic information, or CCI equipment and related materials (exclude cleared immigrant aliens in answering this question)? Yes \_\_\_\_\_ No \_\_\_\_\_ If so, please describe.

11. Does your organization have any foreign involvement not otherwise stated in your answers to the above questions? Yes \_\_\_\_\_ No \_\_\_\_\_ .If so, please describe.

REMARKS (Attach additional sheets, if necessary)



---

## CERTIFICATION

I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge and are made in good faith.

WITNESS:

\_\_\_\_\_

\_\_\_\_\_ Date Certified

\_\_\_\_\_

BY \_\_\_\_\_

\_\_\_\_\_ Company

\_\_\_\_\_ Title

\_\_\_\_\_ Address

**NOTE:** For corporations, witnesses are not required, but the following certificate must be completed. The corporation, should execute the following certificate under its corporate seal, provided that the same officer shall not execute both the certification and the certificate. Type or print names under all signatures.

---

## CERTIFICATE

I, (name) \_\_\_\_\_ certify that I am the (title of certifier) \_\_\_\_\_ of the corporation named as Contractor herein; that (name of signatory) \_\_\_\_\_ who signed this certificate on behalf of the Contractor, was then (name of signatory) \_\_\_\_\_ of said corporation; that said certificate 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.

\_\_\_\_\_ Signature and Date

## APPENDIX 3 TO ANNEX A

### 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 identified 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

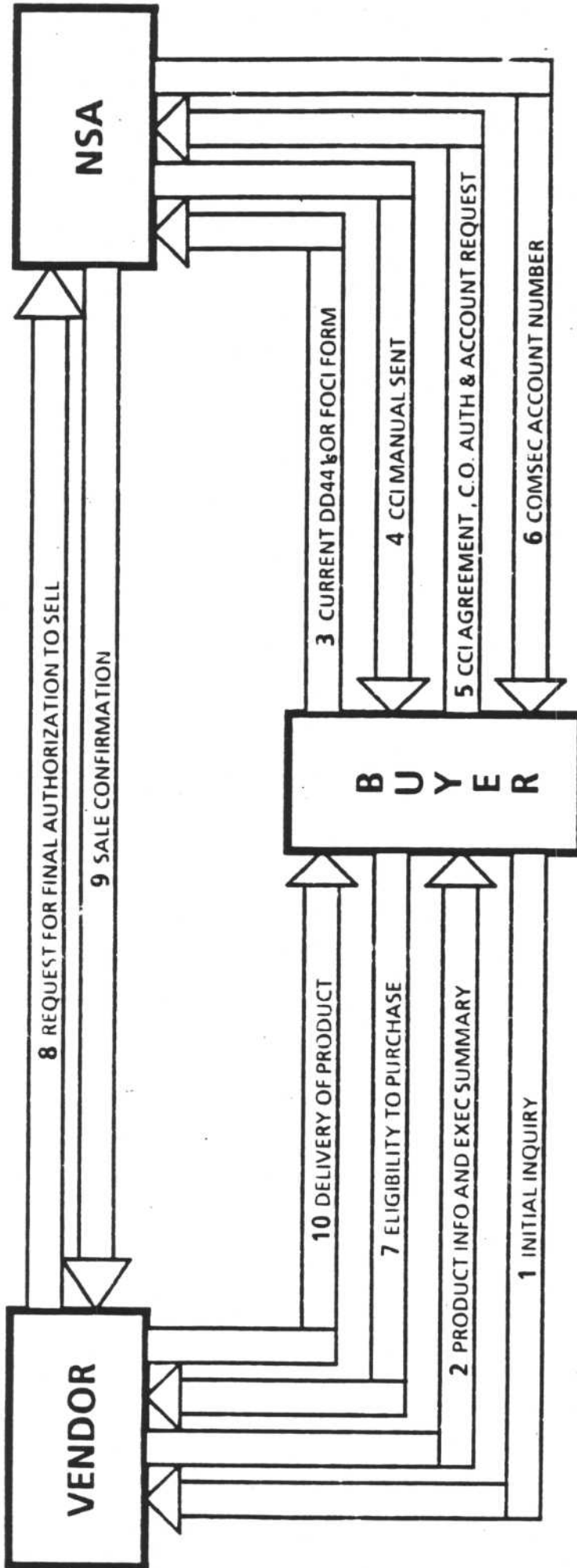
\_\_\_\_\_  
Position/Title

\_\_\_\_\_  
Date

A-3-1

**FOR OFFICIAL USE ONLY**

# CCI DIRECT SALES PROCESS



1. An interested buyer makes his initial inquiry to an authorized vendor for information regarding equipment purchase.
2. The vendor responds to the prospective buyer with price and availability of product and the CCI Manual Executive Summary, which includes a Foreign Ownership, Control or Influence (FOCI) questionnaire.
3. The buyer submits a current DD44 & or completes the FOCI questionnaire and returns it to NSA, ATTN: Y13.
4. NSA (Y13) evaluates the DD44 & or FOCI questionnaire and sends the CCI Manual to the buyer with a request for return of the manual should the sale not be consummated. Included in the manual is the CCI Control Agreement.
5. The buyer submits his request for a COMSEC account (if necessary), returns a completed CCI Control Agreement, and submits the Contracting Officer's authorization to purchase (required for Contractor-Acquired Property only) to NSA (Y13).
6. NSA (Y13) supplies a COMSEC account number and account information to the buyer.
7. The buyer certifies his eligibility to purchase to the vendor.
8. The vendor contacts NSA (Y13) for final authorization to sell.
9. NSA (Y13) grants authorization to sell.
10. Vendor delivers product to buyer.

Figure A.1

## **ANNEX B**

### **COMSEC ACCOUNTS**

#### **I. General**

##### **A. Introduction**

1. CCI equipment and classified or unclassified keying material and certain other associated documents will be controlled in a formal accounting system. This system will be based upon the establishment of COMSEC accounts at Government contractor facilities which will be reportable to a Central Office of Record (COR). The COR is responsible for establishing and monitoring the operation of the COMSEC accounts under its purview.

2. There can be two types of COMSEC accounts: primary accounts and sub-accounts. A primary account reports directly to the COR. Sub-accounts may be established to facilitate the operation of the COMSEC accounting system, for subsidiaries to a company or for divisions of a company which are geographically separated from the division at which the prime account is located. COMSEC sub-accounts should not be confused with sub-contractors of a prime contractor. Sub-accounts report to their prime account.

3. COMSEC accounts which will contain only unclassified equipment and materials can be established. The procedures for these accounts are different than for those accounts which may contain classified materials. Existing COMSEC accounts which were originally established to control classified equipment or keying material may be used to control CCI equipment and classified or unclassified keying materials.

##### **B. Central Office of Record**

1. A Central Office of Record (COR) will establish COMSEC accounts at user and vendor facilities in order to control COMSEC equipments produced under either formal U.S. Government contracts or the Authorized Vendor Program. The responsibilities of the COR are as follows:

- a. Establishing and closing primary COMSEC accounts.
- b. Maintaining a record of all primary COMSEC accounts, to include clearance verification of all Custodians, Alternate Custodians, Facility Security Supervisors (FSS) and verification of adequate storage capabilities.
- c. Maintaining a record of all primary COMSEC accounts' clearance levels and shipping addresses.

d. Formally appointing primary account COMSEC Custodians and Alternate Custodians, and maintaining a record of Facility Security Supervisors nominated by each contractor.

e. Maintaining a master record of all accountable material issued to a primary COMSEC account.

f. Providing guidance and COMSEC briefings, as required.

g. Annually verifying the primary COMSEC accounts' inventory.

h. Auditing primary COMSEC accounts.

i. Performing random, unannounced audits of COMSEC sub-accounts.

### C. COR Determination

1. NSA will be the responsible COR for COMSEC accounts at authorized vendor facilities and for all unclassified primary COMSEC accounts.

2. NSA currently performs the COR responsibilities at contractor facilities for the Department of the Army and Department of the Navy. The Department of the Air Force performs COR responsibilities for its contractor COMSEC accounts as do certain other civil agencies. NSA will determine the responsible COR for all new classified COMSEC accounts at Government contractors.

#### 3. COR Addresses:

a. NSA Accounting Headquarters

Director

National Security Agency

Operations Building Number 3

ATTN: Y131

Room C1B57

Fort George G. Meade, MD 20755-6000

b. Air Force Accounting Headquarters

Commander

U.S. Air Force Cryptologic Support Center

Electronic Security Command

ATTN: MMIC

San Antonio, TX 78243

## II. Procedures for Establishing a Primary COMSEC Account at a Contractor Facility When NSA is the COR

A. COMSEC accounts which will contain classified materials must be established in accordance with the following guidelines. The Contractor must nominate individuals to serve as COMSEC Custodian and Alternate Custodian, and identify the Facility Security Supervisor. Each shall be a U.S. citizen possessing the required security clearance based on a background investigation (BI) current within five years.<sup>1</sup> (If no classified material is involved, see paragraph C. below). The number of Alternate COMSEC Custodians should be kept to an absolute minimum. The nomination of more than two Alternates shall be justified to the NSA COR in the letter of request for appointment.

B. These nominations should then be furnished in writing to the DIS cognizant security office, with a copy to the NSA COR. The level of security clearance of the the selected individuals, the date on which their clearances were granted, their social security numbers (SSN) and their dates and places of birth shall also be provided. The letter should enclose a copy of the DD-254 and shall also contain the facility's Federal Supply Code (FSC), existing U.S. Government contract number, the address of the NSA COR, and a statement that access to operational keying material, installation, maintenance and operation of CCI equipment will be necessary. The person identified as the FSS shall arrange with the DIS cognizant security office or other responsible Government agency or department to provide a COMSEC Briefing (Appendix 1 of Annex D) to the Facility Security Supervisor, the COMSEC Custodian and Alternate COMSEC Custodian(s). In addition, DIS shall forward the names of the nominees and verification of their clearances to the NSA COR. The NSA COR will confirm in writing to the contractor, with a copy furnished to the DIS cognizant security office, that the account has been established, the assignment of an account number, the appointment of the COMSEC Custodian and Alternate COMSEC Custodian(s) and acknowledge for the record the name of the Facility Security Supervisor (FSS). The account number assigned will thereafter be referred to in all correspondence or transactions relating to the COMSEC account.

C. When the account will not handle classified material, an unclassified account may be established. NSA will be the COR for all unclassified primary accounts.

1. In order to establish an unclassified COMSEC account, the contractor shall provide the following information, in writing, to the NSA COR:

<sup>1</sup>While the required BIs are in process, a COMSEC account may be established and hold material (other than keying material) which is classified SECRET and below. However, no classified keying material marked CRYPTO shall be released to the account until favorable completion of all required BIs.

a. Title, complete address and Facility Supply Code (FSC) of the organization, if applicable, in which the account will be located.

b. CCI equipment and keying material to be included in the account.

c. A statement that minimum physical security standards prescribed by this document for safeguarding the unclassified keying material can be met.

d. Names and social security numbers of the individuals to be appointed as Custodian and Alternate(s). Persons selected to be Custodians and Alternate Custodians need not possess a clearance, but should be designated based on their trustworthiness (i.e., the Personnel Selection Criteria set forth in Section III, below, apply when establishing an unclassified account).

2. The NSA COR will make arrangements for the COMSEC Custodian and Alternate COMSEC Custodian(s) to receive a COMSEC Briefing.

3. The NSA COR will confirm in writing to the account applicant that the account has been established, the assignment of an account number, the appointment of the COMSEC Custodian and Alternate COMSEC Custodian(s).

D. When another Department or Agency is the responsible COR, the procedures for establishing a COMSEC account will be as that required by the appropriate COR directives. For record purposes, however, a copy of the letter establishing the COMSEC account must be provided to the NSA COR and must contain the COMSEC account number and the mailing and shipping addresses.

### **III. Personnel Selection Criteria (for Classified Accounts)**

A. Because of the sensitivity of COMSEC CCI equipment and keying material and the rigid controls required, the COMSEC Custodian and Alternate Custodian(s) must possess exemplary qualities of loyalty, reliability and honesty. Personnel must be carefully screened to ensure that the individuals selected:

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

2. Are in a position or level of authority which will permit them to exercise proper jurisdiction in fulfilling their responsibilities and be accountable to the FSS regarding their COMSEC duties.

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

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

5. Will not be assigned duties which will interfere with their duties as a COMSEC Custodian or Alternate Custodian.

6. Can perform the custodial functions on a day-to-day basis. These positions will not be assumed solely for the purpose of maintaining administrative or management control of the account functions.

B. The individual identified as a FSS shall be capable of supervising and directing security measures necessary for the proper application of U.S. Government furnished guidance or specifications for classification, downgrading, upgrading, and safeguarding of classified information.

#### **IV. Indoctrination and Guidance for COMSEC Custodians**

The National Security Agency Central Office of Record (NSA COR) has completed the development of the COMSEC Custodian Training Course (CS-140). The one week course, which is accredited by the National Cryptologic School (NCS), is taught in the Fort George G. Meade, Maryland area on a bimonthly basis. It is mandatory training for Contractor and Agency personnel who have been nominated to be COMSEC Custodians or Alternate Custodians of classified COMSEC accounts. Those current Custodians and Alternates who have held the position for many months are also invited to attend this training. CS-140 must be completed prior to appointment as Custodian or Alternate Custodian. Attendance may be scheduled by sending a written request to the NSA COR. Requests should include name, SSN, security clearance, and account number. Confirmation letters will be mailed to students within two weeks after receipt of request. Questions may be addressed to the NSA COR on (301) 688-8110. Special briefings will be provided for individuals who must be appointed on an emergency basis. Individuals who receive the special briefing will have to attend CS-140 at a later date.



**V. Duties of the Primary COMSEC Custodian, Alternate Custodian, and Facility Security Supervisor<sup>2</sup>**

A. The COMSEC Custodian - The COMSEC Custodian shall be responsible for the receipt, custody, issue, safeguarding, accounting, and disposition and/or 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. He shall be thoroughly familiar with the procedures for handling accountable material as outlined in this document. At an activity where the size of the COMSEC account is so large as to prevent the COMSEC Custodian from personally checking security packaging and markings, performing required page checks and posting amendments, such actions may be performed by other individuals who are appropriately cleared, when applicable, and authorized, so long as these individuals are properly instructed by the COMSEC Custodian. In fulfilling his responsibilities, the COMSEC Custodian will perform the following duties:

1. Protect accountable material and limit access to such materials to individuals who have a valid need to know. If the material is classified, ensure that the authorized individual is cleared to the classification level of the material involved.
2. As appropriate, 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 material.
3. Retain a copy of the Contracts Security Classification Specification (DD-254), if applicable, as part of the custodial records and ensure compliance with the specification.
4. Receive, receipt for, and ensure the safeguarding and accounting of all material issued to the COMSEC account.
5. Maintain COMSEC accounting and related records as outlined in Annex C of this document.

<sup>2</sup>Generally, there would be no FSS for unclassified accounts. Duties for other unclassified account personnel are the same, where applicable; that is, duties which are performed solely for the purpose of protecting classified material are not applicable to unclassified account personnel. Duties of the FSS which are not related to protecting classified material would generally be assigned to the COMSEC Custodian.

6. Conduct a semi-annual inventory, upon appointment of a new COMSEC Custodian, and when directed by the COR, U.S. Government Contracts Office, or FSS (if applicable). The inventory shall be accomplished by physically sighting all material held in his account and performing a records reconciliation with his sub-accounts, if any.

7. Perform routine destruction of accountable material when required, or effect other disposition of material as directed by the COR or U.S. Government Contracts Office.

8. Submit transfer, inventory, destruction, and possession reports when required.

9. Ensure that required page checks are accomplished on all keying material (except material in canisters) and on all accountable publications when they are received, returned, transferred, destroyed, when a change of custodian occurs, and when posting amendments which include replacement pages to ensure completeness of each publication.

10. Ensure the prompt and accurate entry of all amendments to accountable publications held by the account.

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

12. 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.

13. Ensure that appropriate accountable 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 hand receipts as provided for in Annex C, and advise recipients of their responsibility for safeguarding the material until it is returned to the Custodian.

14. Ensure that all accountable material shipped outside the contractor's facility is packaged and shipped in compliance with the requirements of Annexes C and D of this document.

15. Make the necessary shipping arrangements as outlined in Annex D.

16. Report immediately to the FSS any known or suspected incidents of COMSEC insecurities, as defined in Annex G.

17. Prepare for the safeguarding of accountable material during emergency situations in accordance with the guidance of this document and standard operating procedures.

18. Ensure that the COR and sub-account(s), as applicable, are provided up-to-date copies of all DD-254s on all contracts (if any) associated with the COMSEC account.

19. Verify the identification and need-to-know of any individual requesting access to the records and/or material associated with the COMSEC account. Further, if either the records and/or material are classified, verify the appropriate clearance of the requester.

20. Provide initial COMSEC briefings and annual rebriefings for all employees who have a need for access to classified COMSEC information, if so requested by FSS.

21. Train Sub-account Custodian, Alternate Custodian and FSS. For classified accounts training may be conducted by the FSS.

22. If applicable, provide to the Authorized Vendor upon request verification of its sub-account's shipping address and account number.

B. The Alternate Custodian - The purpose of an Alternate COMSEC Custodian(s) is to assist the COMSEC Custodian and provide continuity of operations in the absence of the COMSEC Custodian. The duties of the Alternate Custodian are as follow:

1. Keep aware of the day-to-day activity of the COMSEC account in order to assume the duties of the COMSEC Custodian, whenever necessary, without undue interruption of operations.

2. Perform the duties of the COMSEC Custodian during the temporary absence of the COMSEC Custodian. Ensure that only he or she signs semi-annual inventories in the absence of the COMSEC Custodian.

3. In the event of the permanent departure or unauthorized absence of the COMSEC Custodian, perform the duties of the COMSEC Custodian until the appointment of a new COMSEC Custodian.

4. Conduct initial COMSEC briefings and annual rebriefings for those individuals within the facility who require continued access to classified COMSEC information, if so designated by the FSS.

C. Facility Security Supervisor - The duties of the FSS are to:

1. Ensure implementation of procedures prescribed for safeguarding and control of accountable material and information as required by this document.

2. Ensure that the COMSEC Custodian is provided copies of all DD-254s related to any classified U.S. Government contracts supported by the COMSEC account.

3. Maintain a record of safe combinations, limit access to those individuals who have the need-to-know, and ensure that the combination changes are accomplished as required.

4. Establish procedures to limit access to classified operational key material to persons who have a need-to-know and possess the required security clearance.

5. Notify the DIS cognizant security office in writing, with a copy furnished to the COR, when a new COMSEC Custodian, Alternate COMSEC Custodian, or FSS is nominated or appointed.

6. Make the COR, the appropriate U.S. Government Contracting Office, DIS cognizant security office, and all known suppliers of accountable 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 accountable material.

7. Report immediately to the Controlling Authority and the COR any incident that may have subjected accountable COMSEC information or material to compromise. Where classified material is involved, a copy of the report should also be sent to the DIS cognizant security officer.

8. Ensure that the Alternate Custodian(s) assumes the responsibilities and duties of the COMSEC Custodian when the COMSEC Custodian is to be absent for a period not to exceed 60 days. (An absence in excess of 60 days should be treated as a permanent absence, and a new Custodian must be nominated).

9. Ensure that individuals requiring initial access to cryptographic information are provided a COMSEC Briefing.

10. Conduct initial COMSEC briefings and annual rebriefings for those individuals within the facility who require continued access to classified COMSEC information, or designate the COMSEC Custodian or Alternate Custodian to do so.

11. Act as the approving authority within the facility, as required, for the appointment of an appropriately cleared individual to act as a courier for cryptomaterial (See Annex D.) Such designation will be in writing and the original retained on file for a period of not less than three years.

12. Forward copies of the clearance certification received from the COR to all appropriate sub-account facility security officers.

13. Ensure training is provided to the COMSEC custodian and sub-custodian.

**VI. Sub-Accounts Where NSA is the Responsible COR** (Please refer to Paragraph IID for procedures where another department or agency is the responsible COR.)

A. Use of Hand Receipts - 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 should be employed. In general, corporate facility users located in buildings external to that of the COMSEC account may be supported by the 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 sub-account. Some factors to be considered when deciding on the best method of support is the geographical location of the user, the quantity of equipments and associated material required, and the number of such users within any one building.

B. When establishing a classified COMSEC sub-account, the following procedure shall be followed:

1. The contractor shall nominate individuals to fill the positions of COMSEC sub-account Custodian and Alternate Custodian, and identify the Facility Security Supervisor, each of whom shall be a U.S. citizen and possess the required security clearances. The number of sub-account alternate COMSEC custodians should be kept to an absolute minimum. The nomination of more than two sub-account alternate COMSEC custodians must be justified, and approval received from the primary COMSEC account.

2. The contractor shall furnish the name of the Facility Security Supervisor and the names of the individuals nominated as sub-account COMSEC Custodian and Alternate Custodian in writing to the primary COMSEC account. Individuals nominated for these positions shall have clearances based on background investigations. The level of security clearance of the selected individuals, the dates which their clearances were granted, their social security numbers and their dates and places of birth shall also be provided. The letter should also contain the facility's Federal Supply Code (FSC), the mailing and courier address of the facility, the address of the

DIS cognizant security office supporting that facility, and a statement that access to operational keying material, installation, maintenance and operations of CCI equipment shall be necessary. The primary COMSEC account will request that the DIS cognizant security office update the Background Investigations (BI) on the individuals selected, if not current within five years. A sub-account may not hold material to which the prime account custodian cannot have access.

3. The primary account shall make arrangements with other responsible Government agencies or departments to provide a COMSEC Briefing to the FSS, COMSEC Custodian(s) and Alternate COMSEC Custodian of the sub-account. The primary COMSEC account will confirm to the sub-account, with a copy furnished to the DIS cognizant security office, the establishment of the COMSEC sub-account, the assignment of an account number, and selection of the sub-COMSEC Custodian, sub-account Alternate(s), and sub-account FSS. The COMSEC sub-account number assigned will thereafter be referred to in all correspondence and transactions relating to the sub-account. Sub-account numbers will be derived from the primary COMSEC account number, followed by a dash and numerical designator (i.e., if the primary COMSEC account number is 870415, the first sub-account number will be 870415-1; the second 870415-2, etc.)

C. When establishing an unclassified COMSEC sub-account where NSA is the COR, the contractor shall provide the primary account with the same information as that described in Section II.C.I. The FSS of the primary account or his designated representative will arrange to provide the COMSEC Custodian and Alternate COMSEC Custodian of the sub-account with a COMSEC Briefing. The primary account will confirm in writing to the sub-account applicant the establishment of the account, the assignment of a sub-account number, and the selection of the sub-account COMSEC Custodian and Alternate(s). The COMSEC sub-account number assigned will thereafter be referred to in all correspondence and transactions relating to the sub-account. Sub-account numbers will be derived in the same manner as that specified in Paragraph VI.B.3., above.

D. Sub-account Personnel Selection Criteria - same as for Primary Account Personnel (see Section III of this Annex).

E. Duties of the Sub-account COMSEC Custodian, Alternate Custodian and Facility Security Supervisor - same as for Primary Account Personnel (See Section IV of this Annex).

F. Conversion from a COMSEC Sub-Account to a Primary COMSEC Account where NSA is the COR.

1. Conditions - The primary account may submit a request for the conversion of a sub-account to a primary account only when the primary COMSEC account can no longer provide the required support on a regular basis.

2. Procedures:

a. The primary account shall submit a letter of justification requesting the conversion of a sub-account to a primary account to the DIS cognizant security office, with a copy furnished to the NSA COR, and the COMSEC Sub-Account. The letter shall nominate the individuals presently performing the COMSEC sub-account custodial duties to fill the positions of the COMSEC Custodian, Alternate COMSEC Custodian(s), and identify the present COMSEC sub-account FSS. It shall provide the level of clearance (if applicable) of these individuals, the dates on which the clearance was granted, the BI completion or update dates, their social security numbers, and their dates and places of birth. The letter shall also include the Facility Supply Code (FSC), the existing U.S. Government contract number(s) and the date of the last COMSEC Briefing. DIS will verify the clearance information of the individuals to the NSA COR.

b. If the conversion is approved, the NSA COR shall acknowledge to the primary account and sub-account, in writing, with a copy furnished to the DIS cognizant security office, the establishment of the new primary account, assignment of the account number, appointment of the COMSEC Custodian and the Alternate COMSEC Custodian(s), and acknowledgment for the record of the name of the FSS. The account number will thereafter be referred to in all correspondence or transactions relating to the COMSEC account.

c. When the account will not hold any classified material, the letter requesting the conversion shall be submitted to the NSA COR, with a copy furnished to the COMSEC sub-account. The letter shall nominate the individuals presently performing COMSEC sub-account custodian duties to fill the positions of the COMSEC Custodian and Alternate Custodian. It shall provide their names, dates and places of birth and their social security number. It should also include the Facility Supply Code (FSC), if applicable, the date of the last COMSEC Briefing, and its present COMSEC sub-account number address.

d. If the conversion is approved, the NSA COR shall acknowledge in writing to the new primary account, with a copy furnished to its former primary account, the establishment of the new primary account, the assignment of the account number, and the appointment of the COMSEC Custodian and the Alternate Custodian(s). The account number will thereafter be referred to in all correspondence or transactions relating to the COMSEC account.

e. Transfer of COMSEC Material to New COMSEC Custodian -Upon approval of the conversion and establishment of a primary COMSEC account, the account's former primary Custodian will prepare a "paperwork" transfer of all the accountable COMSEC material charged to his account but actually held by his former sub-account. An original and one copy of the SF-153 will be provided to the new primary COMSEC account and an advance copy to the NSA 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 the NSA COR, retaining one for his files. All accounting files relating to the former sub-account will be retained by both custodians for a period of three years.

## VII. Closing COMSEC Accounts Where NSA is the COR

A. Requirements for Closing Primary Account - If a contractor determines there is no longer a requirement for a primary COMSEC Account and all COMSEC material has been properly disposed of and no discrepancies exist, he shall submit in writing a justification to close the account to the NSA COR with a copy furnished to DIS cognizant security officer (in those cases where the COMSEC account did not contain classified material, a copy to DIS is not required). If the NSA COR determines that there is no longer a requirement for the account, the contractor and DIS cognizant security officer will be notified in writing by the NSA COR of the account's closing and the termination of the appointment of the COMSEC Custodian and Alternate Custodian.

B. Requirements for Closing COMSEC Sub-Accounts - If a primary account determines there is no longer a requirement for a COMSEC sub-account and all COMSEC material has been properly disposed of and no discrepancies exist, the primary COMSEC account will notify the sub-account in writing that the COMSEC sub-account has been closed and that the sub-account COMSEC Custodian, Alternate(s), and FSS are relieved of their duties. The primary COMSEC account will provide the DIS cognizant office (if the account contained classified material) a copy of the letter closing the sub-account.

C. Disposition of Accounting Records and Files -Upon the termination of the COMSEC account or COMSEC sub-account, all pertinent files shall be retained for a period of no less than three years and then properly disposed of according to the level of the classification of the files.

D. When another Department or Agency is the responsible COR, the procedures for closing the COMSEC account will be as that required by the appropriate COR directives. The responsible COR will, however, provide notification to the NSA COR of the disestablishment of the account.



## ANNEX C

### ACCOUNTING PROCEDURES

#### I. GENERAL

A. Purpose and Scope - This annex describes the requirements and procedures for the accounting of:

1. Equipment and systems which are designated as "Controlled Cryptographic Items" (CCI).
2. Classified and unclassified keying material.
3. Other related COMSEC materials, such as operating instructions, manuals, etc., both classified and unclassified.

#### B. Accounting Legends Applicable in this Manual

1. An accounting legend code is a number assigned to COMSEC items which determines the minimum accounting controls required for the item. The number must be listed on the various accounting reports described in this annex.

2. The accounting legend codes applicable to this Manual and their definitions are:

a. AL-1: Continuous accountability by accounting number within the COMSEC accounting system described in this annex.

b. AL-2: Continuous accountability by quantity within the COMSEC accounting system described in this annex.

c. AL-4: Initial receipt required: accountability to a COR may be subsequently dropped (although accountability may be retained in accordance with local user procedures).

3. The accounting legends for individual CCI equipment and related ancillaries, key material, and documentation are contained in Annex I.

#### II. RECEIPT OF ACCOUNTABLE COMSEC MATERIAL

A. Sources - Accountable COMSEC material may be received from NSA, military departments, other governmental agencies, and contractors.

Accountable COMSEC material may arrive at a facility via one of the methods of shipment outlined in Annex D. The custodian should 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 which is addressed to the account may be forwarded, unopened, to the custodian.

B. Receipting for Packages and Examination of Container (see II D below for equipment) - Upon delivery of accountable COMSEC material to the COMSEC Custodian or other individuals authorized by the contractor to receipt for packages, the packages shall be carefully examined for tampering or exposure of their contents. If either is evident, a physical insecurity report shall be submitted as outlined in Annex G. The COMSEC Custodian shall carefully inventory and check contents against the enclosed transfer report. Any discrepancy in short titles, accounting numbers, or quantity shall be reported to the transferring account and the appropriate COR; and the transfer report shall be corrected to agree with the package contents. When the incoming check has been completed, the transfer reports shall be signed and distributed as follows:

1. One copy to the NSA COR.
2. One copy to the cognizant military department accounting headquarters, when appropriate (see Section III. D. for addresses).
3. One copy to the shipment originator.
4. One copy for file.

NOTE: It may be necessary to reproduce additional copies of the SF-153, COMSEC Material Report (see Appendix 1 to this Annex).

C. Page Checking - The COMSEC Custodian or an individual working under his direct supervision shall conduct checks of unsealed material to ensure the presence of all required pages. To conduct the page check, the presence of each page shall be verified against the "List of Effective Pages" or the "Handling Instructions", as appropriate. The "Record of Page Checks" page shall then be signed and dated; or, if the publication has no "Record of Page Checks" page, the notification shall be placed on the "Record of Amendments" page or the cover. If any pages are missing, the "Record of Page Checks" page shall be annotated accordingly. If the publication is classified, a report of physical insecurity shall be submitted as outlined in Annex G. Requests for disposition instructions and a replacement publication shall be submitted to the shipment originator. In case of duplicate pages, the duplicated pages shall be removed and destroyed. One copy of a destruction report shall be prepared citing the page number and the accounting number of the basic publication, e.g., "Duplicate page number 72 removed from

(publication short title), Number 183." The destruction report shall be signed by the COMSEC Custodian and witness, and shall be filed locally. (This locally retained destruction report will not be assigned a transaction number.) No notification to the COR is required. In addition, a notation of the duplicate page and the resultant destruction shall be entered on the "Record of Page Checks". Whenever the COMSEC Custodian is replaced the incoming COMSEC Custodian shall perform a page check of all unsealed material within 30 days after assuming custodial duties. If 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.

1. Keying material - Key tapes or key lists in protective canisters shall not have tape or lists removed for inventory or check purposes.

2. Other material - Upon receipt of a classified COMSEC document, the COMSEC Custodian or Alternate shall stamp or annotate the document "COMSEC MATERIAL--ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE." The publication shall 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 shall be accomplished within two work days after receipt of the material, immediately after entering an amendment, and two days prior to shipment or destruction.

D. Equipment Checking - Equipments received in sealed shipping cartons which have not been opened or do not show evidence of tampering may be receipted for without physically sighting the material inside so long as the label on the carton agrees with the transfer report; otherwise, the contents shall be physically inventoried. The COMSEC Custodian should bear in mind that, though the opening of certain types of material need not take place prior to actual usage, time should be allowed between opening and usage to obtain replacements for incomplete or defective items. Additionally, it is the custodian's responsibility to report all shipment discrepancies to the COR as soon as the discrepancy is discovered.

E. Hardware Keying Material and Associated Aids -Upon receipt of hardware keying material and associated aids, each item shall be inventoried by short title and accounting number.

### III. TRANSFER OF COMSEC MATERIAL

A. General - Accountable COMSEC material may be transferred from one primary COMSEC account to another or from prime account to sub-account only as prescribed by the procedures in this document. When the

validity of a shipping address or authority for the shipment is in question, it is the responsibility of the COMSEC Custodian to verify the address with the COR before making the shipment. COMSEC material, regardless of accounting legend code assigned, shall not be shipped unless a COMSEC account number is provided with the shipping address. Page checking and equipment checking provisions outlined in Section II, paragraphs C and D shall be accomplished prior to packaging COMSEC material for transfer. Such checks should normally be conducted no earlier than 48 hours prior to packaging.

## B. Procedures

1. Transfer of accountable COMSEC material to the U.S. Military Departments or civil agencies (For initial transfer of COMSEC material from COMSEC Vendors, see Annex C, VII.B.) - The shipping COMSEC Custodian shall prepare an original and four copies of form SF-153 and enclose the original and one copy with the shipment. He shall put the notation "ADVANCE COPY" on the second and third copies, staple a copy of the DD-250, if applicable, to both advance copies, and forward one advance copy to the NSA COR and one copy to the appropriate military (see Section D for addresses) or civil agency accounting headquarters. He shall retain the fourth copy for his records. In those instances where the addressee 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 shall prepare an additional advance copy of the transfer report and DD-250 and forward them to the COR 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 the Air Force purchased the equipment, an advance copy of the transfer report and DD-250 shall be forwarded to both the Navy and Air Force CORs. The following notation shall be put on all copies of the transfer reports going to the U.S. Military Departments:

"Custodian:

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

2. Transfer of COMSEC material to other COMSEC accounts or sub-accounts - The shipping COMSEC Custodian shall prepare an original and three copies of the SF-153 and enclose the original and one copy with the shipment. He shall mark "ADVANCE COPY" on the fourth copy, attach to it a copy of the DD-250, if applicable, and forward it to the NSA COR. He shall retain the third copy for file. The following notation shall be put on all copies on these transfer reports:

"Custodian:

Sign all copies;  
Return original copy to:

Director  
National Security Agency  
Operations Building Number 3  
ATTN: Y13  
Room C1B57  
Fort George G. Meade, MD 20755-6000"

NOTE: 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, when applicable, to the COR and the Service accounting headquarters, when appropriate, as soon as the material has been readied for shipment.

3. Transfer of COMSEC material from a Sub-account - Sub-accounts may not transfer material to other than the primary account.

4. Receipt Responsibility - Upon shipment of COMSEC material and receipt of an advance copy of an SF-153, the NSA COR or the Service accounting headquarters, as appropriate, shall assume responsibility for establishing a receipt suspense date and take subsequent tracer action if required. This does not relieve the shipper from ensuring that the material packaging, addressing, and shipping instructions are in compliance with approved procedures. This also in no way relieves the shipper of responsibility for errors which normally can only be detected upon the opening of the material by the recipient, (e.g., shipment of the wrong item, incorrect nameplate, etc.) In lieu of a signed copy of the transfer report, the shipper's recorded proof of shipment will be his file copy of the transfer report, combined with either a signed ARFCOS Form 1, Authorized Commercial Carrier Receipt, or other documentation of shipment.

C. Military Departments accounting headquarters

1. Army Accounting Headquarters

Commander  
U.S. Army Communications Security  
Logistics Activity  
ATTN: SELCL-NICP-OR  
Fort Huachuca, AZ 85613

2. Navy, Marine, and Coast Guard Accounting  
Headquarters

Director  
COMSEC Material System  
3801 Nebraska Avenue, N.W.  
Washington, DC 20390

3. Air Force Accounting Headquarters

Commander  
U.S. Air Force Cryptologic Support Center  
Electronic Security Command  
ATTN: MMIC  
San Antonio, TX 78243

D. Packaging Instructions -

1. General - Classified COMSEC material (Controlled Cryptographic Items (CCI)) and all key material marked CRYPTO shall be securely packaged for shipment in two opaque wrappers without any indication of the classification or CRYPTO markings on the outside wrapper. Each wrapper will be marked with the "TO" and "FROM" addresses including the account number without the word "COMSEC". The outer wrapper of packaged COMSEC material shall never bear identifying marks which reveal its COMSEC association. The inside wrapper of all accountable COMSEC material shall be marked with the notation "TO BE OPENED BY THE COMSEC CUSTODIAN ONLY." All transfer reports and other forms (e.g., DD FORM 250) pertaining to an individual shipment shall bear the individual shipment control number and shall be affixed to the inner wrapper of the package. NOTE: The transfer report and DD Form 250 shall not be placed inside the sealed inner container with the COMSEC equipment.

2. CCI - CCI material shall be securely wrapped and the equipment designator annotated on the package. No CCI markings, however, shall be placed on the package. The accompanying paperwork shall 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".

3. Cryptomaterial - The inside wrapper of cryptomaterial shall be marked CRYPTO together with the classification, if any. Additionally, "NOT RELEASABLE TO FOREIGN NATIONALS" shall be marked on the inside wrapper if the material has been designated as not releasable to foreign nationals.

4. Multiple-package shipments - The COMSEC material shall be marked beginning with package number 1, followed by a slant and the total number of packages comprising the shipment. Package numbers shall 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 (where applicable), etc.) shall be affixed to the inner wrapping of the first package of multiple-package shipments.

#### IV CCI AND COMSEC MATERIAL INVENTORY REPORTING

A. General - Preprinted inventories will be issued semi-annually by the COR and will reflect all accountable COMSEC material (Accounting Legends 1 and 2) charged to the account as of the date the preprinted inventory is issued. Physical (sight) inventories shall be conducted and inventory reports returned to the COR no later than ten days after receipt of the preprinted inventory, or as otherwise directed. (NOTE: Inventories which list classified operational keying material will be classified CONFIDENTIAL. These inventories may be returned via registered mail.)

B. Procedures - In order to complete the inventory report, the primary COMSEC custodian shall proceed in the following manner:

1. With a properly cleared witness, conduct a physical (sight) inventory of all accountable COMSEC material held by the account, to include that material which has been issued on hand receipt. 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 file. Normally, any accounting transactions occurring after the date of the preprinted inventory will not be added to or deleted from the inventory listing. However, if the inventory is being conducted due to replacement of the 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 Custodian replacement.

2. Particular attention should be given to additions or deletions to the account which were accomplished just prior to the date of the report. In some instances, accounting reports may not have reached the COR in time for processing against the account. In that case, the custodian shall update the preprinted inventory by deleting an item or by supplementing it, with an SF-153. Each item to be deleted will be lined out in ink by the Custodian (erasures are not authorized). Complete details to support the deletion shall be given in the "remarks" column opposite the item. In the case of a transfer, remarks shall include the addressee's name and account number, the outgoing transfer number, and the transfer report date (e.g., transferred to Army Account 5AP111, Accounting Report Control Number 311003, dated 830310).

If the deletion is based on a destruction report, the date and transaction number shall 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 shall indicate the name, account number, transaction number, date of incoming transfer, and/or details, as appropriate, to support the supplement. Supplements to a preprinted inventory will be assigned the same transaction number as that given to the inventory.

3. During each inventory, the COMSEC custodian shall determine whether or not any material which is either Contractor-Acquired or Government-Furnished Property is still required. If any such 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 U.S. Government Contracting Officer.

4. When the preprinted inventory has been reconciled and agrees with the account's actual holdings, both the Custodian and witness will sign and date the certifications on the preprinted inventory and any supplemental SF-153. The number of supplemental forms accompanying the report shall be indicated in the space provided in the Custodian's certification block. If no supplemental forms were required, mark "NONE" in the Custodian's certification block. The 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 shall be retained by the Custodian for his files and the original forwarded to the COR.

5. Upon receipt of the certified inventory report, the COR will reconcile with its own records. The Custodian will be advised only if discrepancies are noted. If the account is cited with any discrepancy, the Custodian shall 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.

C. Special Inventories - The COMSEC Custodian shall conduct a special inventory when directed by the COR, U.S. Government Contracting Officer (if applicable), or Facility Security Supervisor (FSS), for reasons of suspected loss of COMSEC material or frequent deviation from accounting procedures. Special inventories shall be recorded on an SF-153. They shall not be forwarded to the COR unless the COR so requests or unless the authority directing the special inventory desires that the COR verify its accuracy.

D. Negative Inventories - Even though an active COMSEC account may not hold accountable COMSEC material (Accounting Legends 1 and 2), annual



preprinted inventories will be forwarded to the COMSEC account from the COR. Both the COMSEC Custodian and a properly cleared witness (usually the Alternate COMSEC Custodian) shall sign the negative inventory, thereby certifying that the account does not hold accountable COMSEC material. COMSEC accounts will continue to receive annual preprinted inventories until the COMSEC account is formally closed. If the COMSEC account has received or still holds accountable COMSEC material when a negative preprinted inventory is received, the inventory should be supplemented (see paragraph B. 2., above) to reflect the accountable COMSEC material held by the COMSEC account.

E. Sub-Accounts Inventories - When the primary COMSEC account receives its annual preprinted inventory from the COR, the primary account shall cause its sub-accounts to conduct a physical (sight) inventory of its holdings in the same manner as described in Paragraph B, above. Upon completion of the physical (sight) inventory, the sub-account COMSEC custodian shall provide the primary COMSEC account with the listing of all its accountable COMSEC holdings. The primary account COMSEC custodian shall then reconcile the sub-account's listing with both his master records and the preprinted inventory. When a total reconciliation has been effected, the primary account COMSEC custodian shall complete the required certification as prescribed in paragraph B. 4 above.

## V. DESTRUCTION REPORTS

### A. Keying Material

1. In no case will used or superseded keying material be held longer than 72 hours. Only when all key segments contained in a particular edition of key are used or superseded, will a destruction report be prepared and submitted to the NSA COR.

2. The 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 Custodian who is provided operational keying material for use must ensure that this monthly destruction report is submitted to the NSA COR no later than the 16th day of each month following supersession.

3. The completed disposition record card for key tape segments will be used by the Custodian to prepare the destruction report.

4. 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 will be retained by the COMSEC Custodian for a period of three years and protected in the same manner as other classified COMSEC material. Additionally, the

following remark will be reflected below the "NOTHING FOLLOWS" line on the SF-153: "The official records in my possession indicate that the above listed items have been properly destroyed by duly authorized individuals."

B. Other COMSEC material - The prompt physical destruction of accountable COMSEC material is mandatory. The Custodian may elect to submit a destruction report as soon as destruction is accomplished or consolidate the destruction information and submit it to the NSA COR on a monthly basis.

C. Verification of material to be destroyed -Because the destruction of the wrong item can result in a possible compromise, the COMSEC Custodian and witness should take extreme care to assure they are destroying the correct COMSEC material and that the destruction report is completely accurate.

D. Submission of Destruction Report - A destruction report will be prepared for all accountable COMSEC material. To submit a destruction report, the COMSEC Custodian will prepare an SF-153 and will enter the authority for destruction below the "NOTHING FOLLOWS" line, e.g., "Superseded by KAM-220B;" "residue of Amend 2 of KAM-212;" "letter from Contracting Officer, dated 1 January 1982." The signed and properly witnessed original copy of the destruction report will be forwarded to the NSA COR and the signed duplicate copy will be retained for file.

## VI. AUDIT OF COMSEC ACCOUNTS

### A. Auditing Primary COMSEC Accounts

1. Basis - Primary COMSEC accounts will be audited by the appropriate COR at least annually, and as deemed necessary, based on the following considerations:

- a. Size of the COMSEC account and volume of transactions.
- b. Frequency of COMSEC custodian changes.
- c. Classification and sensitivity of COMSEC material held.
- d. Frequency of deviation from COMSEC accounting procedures.

2. Notification - Prior notice may or may not be provided to the COMSEC account when that account has been selected for audit.

3. Auditor Access - The Auditor shall present proper identification prior to gaining access to the COMSEC account and, prior to auditing a classified COMSEC account, shall provide verification of the appropriate clearances.

4. Scope of the Audit - The audit of a COMSEC account shall include:

a. Verification of the completeness and accuracy of COMSEC accounting reports and files.

b. Assessment of COMSEC Custodian's and Alternate's knowledge of and adherence to provisions of COR directives.

c. Normally physical sighting of all accountable COMSEC material.

d. Assessment of compliance with packaging and marking instructions.

e. Solicitation of COMSEC Custodian's problems in maintaining the account.

f. Recommendations for the improvement of local COMSEC accounting and control procedures.

5. Report of Audit - Immediately upon completion of the audit, the Auditor shall notify the COMSEC custodian of any situation requiring immediate action and shall conduct an exit interview with the FSS (if applicable) and management, if deemed necessary. A formal report of audit outlining any discrepancies noted during the audit, condition of the COMSEC account, and recommendations shall be forwarded to the contractor. When the Audit Report outlines actions required of the COMSEC Custodian, FSS (if applicable) or others, a Certificate of Action Statement shall accompany the report. The letter forwarding the Audit Report will normally specify that all required action shall be completed within ten days after receipt of the report or, if circumstances warrant within a more extended period of time. Upon completion of the action, the COMSEC Custodian shall complete the Certificate of Action Statement and return it to the COR.

#### B. Auditing COMSEC Sub-Accounts

1. By the Primary COMSEC Custodian - Sub-accounts shall be audited at least annually by the COMSEC Custodian of the primary COMSEC account, based on the same considerations and in the same manner as outlined in paragraph V. A. above. The report of the auditing COMSEC custodian's findings shall be submitted to the sub-account's Custodian and a copy retained by the primary account to be made available to the COR at the time of the primary account's annual audit or upon request. When the Audit Report outlines actions required of the COMSEC sub-custodian, a Certificate of Action Statement shall accompany the report. The required actions shall be

completed by the sub-custodian within ten days after the receipt of the report. Upon completion of the actions, the COMSEC sub-custodian shall complete the Certificate of Action Statement and return it to the primary COMSEC account for retention.

2. By the COR auditor - COR audits of sub-accounts will be conducted on a random, unannounced basis and in the same manner as that for primary accounts. Prior to the audit, the NSA COR will request the primary COMSEC account to provide a preprinted inventory of the sub-account's holdings. The formal report of the audit shall be forwarded to the COMSEC Custodian of the primary account, with a copy furnished to the sub-account 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 is the responsibility of the primary COMSEC Custodian to ensure that required corrective actions are accomplished by the sub-COMSEC Custodian within the specified period of time. Once the required actions have been completed, the sub-account Custodian shall return a signed copy of the Certificate of Action Statement to the primary COMSEC Custodian who will then countersign it and return it to the COR, retaining a copy for his files.

## VII. CHANGE OF COMSEC CUSTODIAN

A. Submission of New COMSEC Custodian to NSA COR -When it becomes necessary to terminate the COMSEC Custodian's appointment, the contractor will select, nominate, and forward for confirmation to the Cognizant Security Office (with a copy furnished to the NSA COR) the newly appointed COMSEC Custodian.

B. Transfer of Inventoried Material. Upon receipt of the confirmation letter from the NSA COR, the newly appointed COMSEC Custodian and his 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 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 listed on the transfer, the SF-153 will be stamped "CONFIDENTIAL." Identifying the report in block 1 as a "change of Custodian" and check both "received" and "inventoried" in block 14. The report will be addressed from the contractor (block 2) to the NSA COR (block 3). The new Custodian will sign in block 15 and the departing Custodian will sign as the witness in block 17. The signed original copy will be forwarded to the NSA 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 Custodian may request a preprinted inventory/transfer from the NSA COR. The request for a preprinted inventory/transfer should accompany the letter of nomination.

#### C. Transfer of Responsibility

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

2. After receipting for COMSEC material charged to the COMSEC account, the new Custodian will assume full responsibility for its operation.

3. The former COMSEC Custodian will be relieved of responsibility for only that COMSEC material included on the transfer/inventory report. He 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 NSA COR.

#### D. Resolution of Discrepancies

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 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.

#### E. Change of Alternate Custodian

When a change in Alternate Custodian is necessary, the contractor will select, nominate, and forward the name of the new Alternate. A change of Alternate Custodian should be made prior to the departure of the present Alternate Custodian if possible.

#### F. Change of Facility Security Supervisor

When it is necessary to make a change in the Facility Security Supervisor, notification must be sent to the cognizant security office, with a copy provided to the NSA COR.

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

1. 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 Custodian) in compliance with the provisions of Annex B, Para VI. B. 1 and VI.B.2. 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 NSA COR and the cognizant security office.

2. Upon 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 NSA COR and a signed duplicate copy will be retained in the COMSEC account's file.

3. The NSA COR should be notified as soon as possible in the event that an Alternate COMSEC Custodian or Facility Security Supervisor must be replaced due to a sudden, indefinite, or permanent departure. The unauthorized absence must be immediately reported to the NSA COR and the cognizant security office.

**VIII. CCI EQUIPMENT DISTRIBUTION**

A. Requirement - Contractors who purchase CCI equipment shall arrange for equipment distribution with the vendor, and in coordination with the U.S. Government Contracting Officer (if applicable), as follows:

1. In compliance with the procedures outlined in Annex A enter into a contract with the vendor for the quantity of COMSEC equipment required.

2. Provide the vendor with the COMSEC account number and shipping address of the facility to which the equipment will be sent.

3. Provide, as appropriate, the COMSEC sub-account number and their shipping addresses, if direct shipment to the sub-accounts is warranted.

B. Procedures - All COMSEC equipment purchased will be charged to the primary COMSEC account by the appropriate COR.

1. Direct shipment to primary COMSEC Accounts -The required equipment for both the primary COMSEC account and its sub-accounts will normally be shipped directly to the primary COMSEC account. The SF-153 will be addressed to the primary and will be included with the shipment. An advance copy shall 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 shall verify the contents of the shipment against the accompanying paperwork. If no discrepancies exist, the COMSEC Custodian shall 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 files. If a discrepancy is noted, follow the procedures specified in paragraph II.B in Annex C of this Manual.

a. Redistribution to COMSEC sub-accounts - Upon receipt of the shipment at the primary COMSEC account, the COMSEC custodian will prepare the appropriate equipment for shipment to its sub-accounts, following the packaging procedures specified in Section III, paragraph E, above. He shall include in each separate sub-account shipment an SF-153 identifying the contents therein. The SF-153 shall be assigned a transaction number as prescribed in Section VIII, B.2.i., below.

b. Receipt by sub-accounts - Upon receipt of the equipment by the COMSEC sub-account, the sub-account COMSEC Custodian shall verify the contents of the package against the accompanying SF-153. If no discrepancies exist, he shall sign the SF-153, assign to it an incoming transfer number, return a copy to the primary COMSEC account and retain the original for his files.

2. Direct shipment to COMSEC sub-accounts -When a direct shipment of COMSEC equipment is made to the COMSEC sub-account, the vendor shall provide a copy of the SF-153 along with the shipment, but advance copies shall also be provided to the primary account, the NSA COR and the appropriate Department or Agency COR, if applicable. The advance copy will serve as notice to the primary account of the issuance of the equipment directly to one of its sub-accounts.

3. Upon receipt of the signed SF-153 from its COMSEC sub-account, the primary COMSEC custodian 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 advance copy of the SF-153 to the vendor, he will duplicate a sufficient number of copies and will forward one to the NSA COR, the Department or Agency COR if applicable, and will retain one for his files along with the SF-153 received from the sub-account. It will be the primary COMSEC

custodian's responsibility to ensure that his sub-account custodians execute their SF-153s within 48 hours from receipt of the equipment, thereby alleviating the need for tracer action. Tracer action for equipment shipped directly to COMSEC sub-accounts rests with the primary COMSEC account custodian.

#### IX. FORMS, REPORTS, AND FILES

A. Forms - The standard forms used for reporting and filing information in the COMSEC Material Control System are listed below (see Appendix 1 to this Annex for examples).

1. The Armed Forces Courier Service (ARFCOS) regulations require personnel who may be required to accept ARFCOS material to complete an Armed Forces Courier Authorization Record (ARFCOS Form 10) prior to receipting for material. ARFCOS Form 10 may be obtained from the servicing ARFCOS station (see Appendix 1 to this Annex for a list of ARFCOS addresses).

2. ARFCOS Form 1 - The receipt for material shipped via ARFCOS.

3. SF 153, COMSEC Material Report - A Multipurpose report to record transfer, possession, inventory, residually and supplemental inventory, and destruction of accountable COMSEC Material.

4. DD250, Material Inspection and Receiving Report - proof of sale for government-funded (GFPOCAP) sale by vendor to contractor.

5. Form L6061, COMSEC Material Record - per item record of COMSEC Material

6. Form A1721, COMSEC Material Hand Receipt -for local transfer.

#### B. Accounting Reports

1. Types - Accounting reports which indicate the transfer, possession, inventory, residual and supplemental inventories, and the destruction of COMSEC material are recorded on the SF-153. The various reports and a brief description of their use are as follows:

a. Transfer Report - To record COMSEC material transferred from one COMSEC account to another or from the primary account to its sub-accounts.

b. Destruction Report - To report the physical destruction or other authorized expenditure of COMSEC material.



c. Inventory Report - To report the physical (sight) inventory of COMSEC material.

d. Possession Report - To report the possession of COMSEC material when such material is received without an accompanying SF-153.

e. Residual Inventory Report - To report to the Government Contracting Officer, upon the completion of a contract, all accountable CCI or COMSEC material (including spares) which is Contractor-Acquired Property or Government Furnished Equipment which resides in the account.

1) The report should indicate which of those residual items will be required for the performance of current and future contracts.

2) Upon receipt of the residual inventory report, the Government Contracting Officer shall review the report and provide the Contractor with disposition instruction.

2. Preparation - Proper preparation, accuracy, and timely submission of COMSEC accounting reports are essential for effective control of COMSEC material. SF-153 shall be completed for each type of report in the following manner:

a. Reports shall include the official titles and addresses of the activities involved; account numbers, transaction and contract numbers, and DD-250 partial shipment numbers, when appropriate; date of report (entered: year, month, date: e.g., 821031 indicating 31 October 1982); typed or stamped names of individuals signing reports, and signatures in ink.

b. All short titles shall be listed in alphanumeric order.

c. All line item entries on a report shall be single spaced. The last line item shall be followed by "NOTHING FOLLOWS," entered in capital letters on the next line.

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

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

f. Ensure that series of accounting numbers agree with the entries made in the "quantity" column.

g. Include any clarifying remarks deemed appropriate for the receiving COMSEC Custodian or the COR in Block 13 below the "NOTHING FOLLOWS" line.

h. Initial all deletions or corrections in ink.

i. 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 for COMSEC Account 870342 would be 342001). These transaction numbers will be used exclusively for primary COMSEC account's accounting reports. A separate sequential system will be used for those transactions between the primary accounts and its sub-accounts, as follows: The first yearly transaction from the primary account 870342 to sub-account 870342-1 would read 342-1-001; likewise, if it were the sixth transaction of the calendar year from primary account 870342 to sub-account 870342-3, it would read 342-3-006. NOTE: Transaction numbers are not assigned to hand receipts or reconciliation statements.

j. Review all reports for completeness and accuracy.

k. Ensure the legibility of each copy of each report.

l. All unclassified SF-153s must be stamped FOR OFFICIAL USE ONLY at the bottom of the form.

3. All accounting reports should be submitted within 48 hours after receipt or preparation. Preprinted inventories should be returned within ten working days after receipt, or as otherwise directed.

C. Hand Receipts - When COMSEC material is to be issued by the COMSEC Custodian to User personnel, it will be issued on a hand receipt. A hand receipt may be executed on a Form SF-153, the reverse side of Form L6061, or Form A1721.

1. Prior to issue of material on a hand receipt, the COMSEC Custodian shall ensure that the proposed recipient:

a. Has a need to know and the required clearance, if the material is classified.

b. Will be the person who has direct control of equipment and associated keying materials.

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

2. 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 office of the recipient, it must be returned to the COMSEC custodian for reissue.

3. Users who need to transport COMSEC material held 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 Annex D, C. 7. d.

4. Hand receipts for COMSEC material should be reviewed periodically to ensure their accuracy and to verify the continued need of the material by the recipient.

5. 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 initialing and dating the reverse side of Form L6061 or Form A1721, as appropriate.

D. Files - Each COMSEC custodian will establish and maintain COMSEC accounting and related files as indicated 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).

f. Master Disposition Record of Accountable COMSEC Material (when applicable)

2. Related Files:

a. Courier, mail, and package receipts.

b. Correspondence to include such records as COMSEC custodian and alternate custodian appointment confirmation letters, messages, and other documentation related to COMSEC accounting.

E. Classification of COMSEC Accounting Reports and Files. A minimum classification of CONFIDENTIAL will be assigned to a list of complete holdings which includes classified operational keying material or reports which supply classified keying material effective dates. Files which contain only lists of unclassified key and CCI equipment are unclassified. Additionally, the following guidance is provided:

1. 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 File, the container will also be classified CONFIDENTIAL if it contains inactive L6061s for classified operational keying material.

2. Accounting Files - Although individual destruction reports/transfer reports for classified operational keying material are unclassified, 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 accordingly.

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

4. Classification is the responsibility of the COMSEC Custodian or FSS, and will be determined by evaluating the contents of each COMSEC accounting report, COMSEC accounting file, or DD-254.

5. Each report or file which contains classified COMSEC information will also bear in addition to the classification the following statement: "Classified by NSA/CSS 123-2, Declassify on: Originating Agency's Determination Required."

6. All COMSEC accounting files will be retained for a minimum of three years at which time they may be retired or destroyed.

#### **X. VENDOR ACCOUNTING RESPONSIBILITIES**

A. All vendors of CCI equipment shall establish a primary COMSEC account, (or use one already in existence) for the purpose of complying with COMSEC accounting requirements. (See Annex B, Section II, Procedures for Establishing a Primary COMSEC Account at a Contractor Facility).

B. The custodian of the vendor's COMSEC account is responsible for the following:

1. Ensuring that the purchaser has established a COMSEC account or sub-account prior to shipment of the equipment.

2. Verifying, through the NSA COR, the shipping address of material to be sent to a primary account. For material to be shipped to sub-accounts, verification will be obtained from the primary account.

3. Ensuring that the purchaser has obtained and completed ARFCOS Form 10, if shipment is to be via ARFCOS.

4. Recording and retaining the user's account number, mailing address, and courier address.

5. Maintaining a Master Disposition Record for all COMSEC equipment produced under the Authorized Vendor Program which shall include:

a. The serial number of the item.

b. The number of the COMSEC account to which the equipment was shipped.

c. The date of shipment.

d. The vendor's transaction number.

e. The intermediate shipment control number (ARFCOS, authorized commercial carrier, etc.).

f. The DD-250 partial shipment order.

6. Ensuring the availability of its records to the NSA COR upon request and during audit.

7. Submitting to the NSA COR a copy of the Master Disposition Record upon termination of the MOU/MOA.

<b>MATERIAL INSPECTION AND RECEIVING REPORT</b>	1 PROC INSTRUMENT IDEN (CONTRACT) APPENDIX 1 TO ANNEX C MOUS 1001-24-85-99	(ORDER) NO	6 INVOICE	7 PAGE 1 OF 1
				8 ACCEPTANCE POINT S

2 SHIPMENT NO VEF 4091	3 DATE SHIPPED 85JUNE13E	4 B/L TON	5 DISCOUNT TERMS
---------------------------	-----------------------------	--------------	------------------

9 PRIME CONTRACTOR VENDOR, INC. 166 WESTWOOD DRIVE COLUMBIA, MD 21045	CODE 45678	10 ADMINISTERED BY VENDOR, INC. 166 WESTWOOD DRIVE COLUMBIA, MD 21045	CODE
--	---------------	--	------

11 SHIPPED FROM (if other than 9) CODE	FOB	12 PAYMENT WILL BE MADE BY U. S. NAVAL SECURITY COMMAND NORFOLK, VA 66743	CODE
---	-----	---	------

13 SHIPPED TO 870999 XYZ CORPORATION 5296 RESEARCH PARK ROAD SAN DIEGO, CA 92121	CODE	14 MARKED FOR CM/F: Mr. James Williams ACCT: 870999 REF: XYZ CORP. P/O T-F1372	CODE
--	------	---	------

15. ITEM NO	16. STOCK/PART NO <small>(Indicate number of shipping containers - type of container - container number.)</small>	DESCRIPTION	17. QUANTITY * SHP/REC'D	18. UNIT	19. UNIT PRICE	20. AMOUNT
1	STU-II KY-71A ON359620-2: Consisting of: See Page 2		1	EA		
2 Cartons: Gross Shipping Wt. 115						

21. PROCUREMENT QUALITY ASSURANCE		22. RECEIVER'S USE	
<input checked="" type="checkbox"/> POA <input checked="" type="checkbox"/> ACCEPTANCE of listed items has been made by me or under my supervision and they conform to contract except as noted herein or on supporting documents.		<input type="checkbox"/> POA <input type="checkbox"/> ACCEPTANCE of listed items has been made by me or under my supervision and they conform to contract, except as noted herein or on supporting documents.	
DATE	SIGNATURE OF AUTH GOVT REP G. Jones	DATE	SIGNATURE OF AUTH GOVT REP
TYPED NAME AND OFFICE S0000A		TYPED NAME AND TITLE	
23. CONTRACTOR USE ONLY		Quantities shown in column 17 were received in apparent good condition except as noted. DATE RECEIVED _____ SIGNATURE OF AUTH GOVT REP _____ TYPED NAME AND OFFICE _____ * If quantity received by the Government is the same as quantity shipped, indicate by ( ✓ ), mark, if different, enter actual quantity received below quantity shipped and encircle.	

ACTIVITY (Address, Location, Room/Building No., Account No., etc.)

DUTY HOURS

NON-DUTY HOURS

TELEPHONE NUMBERS / AUTOVON and COML

The authorizing official acknowledges that the individuals identified below by name, social security number, and signature, are assigned to his/her activity, are authorized to enter and receive Armed Forces Courier Service (ARFCOS) qualified material; and possess an appropriate personal security clearance for the qualified material they will be entering or receiving through ARFCOS. A new ARFCOS Form 10 will be submitted to your servicing ARFCOSTA one year from the date of this form or if there are any additions and/or deletions concerning the authorizing official or the individuals named below.

NAME	GRADE	SSN	PHONE NO	SIGNATURE

DATE	AUTHORIZING OFFICIAL (Name, grade, title)	SIGNATURE
------	---	-----------

**ARMED FORCES COURIER SERVICE**

**RECEIPT TO SENDER**

**FROM:** (Originator's complete geographic address APO/FPO not acceptable)

ARTICLES LISTED HEREON (CONTAIN MATERIAL QUALIFIED FOR TRANSPORTATION VIA THE ARMED FORCES COURIER SERVICE IN ACCORDANCE WITH PARAGRAPH A464/OPNAVINST 5100.7/AFM 102.14, WHEN APPLICABLE, INDICATE SPECIAL HANDLING INSTRUCTIONS FOR EACH ARTICLE IN COLUMN 4. ENTRY OF UNQUALIFIED MATERIAL MAY RESULT IN APPROPRIATE DISCIPLINARY ACTION.

ENTRY CERTIFICATION SIGNATURE(S) AND GRADE OF ORIGINATOR'S AUTHORIZED REPRESENTATIVE(S)

DATE

ARFCOSTA ARTICLE NUMBER	WEIGHT OF ARTICLE		ORIGINATOR'S CONTROL NO	ORIGINATOR'S SPECIAL HANDLING INSTRUCTIONS (If appropriate)	ADDRESSEE (Complete geographic address)	DISPOSITION (ARFCOSTA USE ONLY)		
	LB	OZ				ARFCOS FORM 3	ARFCOS FORM 4	ARFCOS FORM 5
NUMBER OF ARTICLES							TIME/DATE	ARFCOSTA SYMBOL
TOTAL WEIGHT							TIME/DATE	

RECEIPT ACKNOWLEDGED (Signature(s) and Grade of Courier(s))

RECEIPT ACKNOWLEDGED (Signature(s) and Grade of Duty Courier(s) or authorized representative(s))



COMSEC  
MATERIAL REPORT

OMB  
Approval No. 23-40164

<input checked="" type="checkbox"/> TRANSFER <input type="checkbox"/> INVENTORY <input type="checkbox"/> DESTRUCTION <input type="checkbox"/> HAND RECEIPT <input type="checkbox"/> OTHER (Specify)			
2 EAST COAST ELECTRONICS 830 WASHINGTON AVENUE BALTIMORE, MARYLAND ROBERT L. SHEA	ACCT NO. 870399	4 DATE OF REPORT (Yr., Mo., Da.) 841031	5 OUTGOING NUMBER 399001
	DATE REPORT IS PREPARED	6 DATE OF TRANSAC-TION (Yr., Mo., Da.) LEAVE BLANK	7 INCOMING NUMBER LEAVE BLANK
3 COMMANDER 505106 10TH SIGNAL GROUP FORT HOOD, TEXAS ATTN: COMSEC CUSTODIAN	ACCT NO. 505106	*ACCOUNTING LEGEND CODES 1 ACCOUNTABLE BY SERIAL NO. IN CMCS 2 ACCOUNTABLE BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4 INITIAL RECEIPT CONTROL LAW SERVICE/AGENCY DIRECTIVES	

SHORT TITLE	QUANTITY	ACCOUNTING NUMBERS		ALC	REMARKS
		BEGINNING	ENDING		
KG-84 CONSISTING OF					
KGB-11	3	642	644	4	New Material
KGB-11	1	-	650	4	" "
KGG-7	4	1809	1812	1	" "
KGG-7	1	-	1823	1	" "
KGG-7	1	-	1827	1	" "
KGG-7	1	-	1831	1	" "
KGG-7	4	1840	1843	1	" "
KGS-5	4	612	615	4	" "
KGS-6	6	614	617	4	" "
KGD-9	3	651	653	1	" "
KGD-9	1	-	683	1	" "
KGD-10	4	707	710	1	" "
KGP-3	3	667	669	4	" "
KGP-3	4	800	803	4	" "
E-ABE	2	N/N	N/N	2	CONTAINED IN
E-ABH	2	N/N	N/N	2	KG-94/ERP/KIT
E-ABL	2	N/N	N/N	2	KG-94/ERP/KIT
E-ABX	2	N/N	N/N	2	KG-94/ERP/KIT

//////////NOTHING FOLLOWS//////////  
 CUSTODIAN: SIGN ALL COPIES AND DISTRIBUTE IN ACCORDANCE WITH INSTRUCTIONS OF YOUR SERVICE.

THIS SHIPMENT CONSISTS OF 7 CONTAINERS. ← REQUIRED NOTATIONS

EXAMPLE OF A TRANSFER REPORT OF COM-SEC MATERIAL TO A MILITARY SERVICE

ARFCOS CONTROL NO., REGISTERED MAIL NO., GBL NO., OR OTHER CONTROL NO., AS APPROPRIATE

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 ARFCOS NO. 15002	CONTRACT NO. DA18-119-AMC-52(X) DD-250 PARTIAL NO. 118

FORM 7540-00-408-6859

FOR OFFICIAL USE ONLY

PAGE 1 of 1 PAGES  
 STANDARD FORM 163 (Rev. 8-79)  
 PRESCRIBED BY GPO  
 OGD KAG-1 163-118

Transfer Report of COMSEC Material to a Military Service (SF-153)

COMSEC  
MATERIAL REPORT

OMB  
Approval No 22-R0184

<input checked="" type="checkbox"/> TRANSFER <input type="checkbox"/> INVENTORY <input type="checkbox"/> DESTRUCTION <input type="checkbox"/> HAND RECEIPT <input type="checkbox"/> OTHER (Specify)									
FROM	EAST COAST ELECTRONICS 830 WASHINGTON AVENUE BALTIMORE, MARYLAND ROBERT L. SHEA			ACCT NO. 870399	4. DATE OF REPORT (Y., Mo., Da.) 841031	5. OUTGOING NUMBER 399008			
	DATE REPORT IS PREPARED				6. DATE OF TRANSACTION (Y., Mo., Da.) LEAVE BLANK	7. INCOMING NUMBER LEAVE BLANK			
TO	BOSTON COMPUTER CORP. 8366 ATLANTIC AVENUE CAMBRIDGE, MASSACHUSETTS ATTN: COMSEC CUSTODIAN			ACCT NO. 870344	*ACCOUNTING LEGEND CODES 1. ACCOUNTABLE BY SERIAL NO. IN CMCS 2. ACCOUNTABLE BY QUANTITY IN CMCS 3. ACCOUNTABLE BY SERIAL NUMBER 4. INITIAL RECEIPT CONTROL (AW SERVICE/ AGENCY DIRECTIVES)				
	8. SHORT TITLE			9. QUANTITY	11. ACCOUNTING NUMBERS		12. ALC	13. REMARKS	
KW-62			1	-	4		1	New Material	
KWX-40			1	-	11		4	" "	
KWX-40			2	21	22		4	" "	
E-ABC			5	N/N	-		2	" "	
////////// /NOTHING FOLLOWS/									
CUSTODIAN SIGN ALL COPIES. RETURN ORIGINAL COPY TO: DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MARYLAND 20755-6000								REQUIRED NOTATIONS	
DISPOSE OF REMAINING COPIES IN ACCORDANCE WITH INSTRUCTIONS OF YOUR ORGANIZATION.									
THIS SHIPMENT CONSISTS OF 4 CONTAINERS									
EXAMPLE OF A TRANSFER REPORT OF COMSEC MATERIAL TO AN ACCOUNT OTHER THAN A MILITARY SERVICE.									
ARFCOS CONTROL NO., REGISTERED MAIL NO., GBL NO., OR OTHER CONTROL NO. AS APPROPRIATE.									
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: ARFCOS NO.                                  CONTRACT NO.                                  DD-250 PARTIAL NO.									
15091                                  DA19-119-AMC-1777(x)                                  4                                  20                                  PAGE 1 of 1 PAGES									

FOR OFFICIAL USE ONLY

Transfer Report of COMSEC Material to an Account Other Than a Military Service (SF-153)

COMSEC  
MATERIAL REPORT

OMB  
Approved No. 22-R0164

<input type="checkbox"/> TRANSFER <input type="checkbox"/> INVENTORY <input type="checkbox"/> DESTRUCTION <input type="checkbox"/> HAND RECEIPT <input checked="" type="checkbox"/> OTHER (Specify)		<b>POSSESSION</b>																																																						
2 EAST COAST ELECTRONICS 830 WASHINGTON AVENUE BALTIMORE, MARYLAND ROBERT L. SHEA	ACCT NO. 870399	4 DATE OF REPORT (Y., Mo., Da.) 841031	5 OUTGOING NUMBER 399009																																																					
	DATE REPORT IS PREPARED		6 DATE OF TRANSACTION (Y., Mo., Da.) LEAVE BLANK	7 INCOMING NUMBER LEAVE BLANK																																																				
3 DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MARYLAND 20755-6000	ACCT NO.	*ACCOUNTING LEGEND CODES 1 ACCOUNTABLE BY SERIAL NO. IN CMCS 2 ACCOUNTABLE BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4 INITIAL RECEIPT CONTROL LAW SERVICE/ AGENCY DIRECTIVES																																																						
	<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th rowspan="2">8 SHORT TITLE</th> <th rowspan="2">10 QUANTITY</th> <th colspan="2">11 ACCOUNTING NUMBERS</th> <th rowspan="2">12 ALC</th> <th rowspan="2">13 REMARKS</th> </tr> <tr> <th>BEGINNING</th> <th>ENDING</th> </tr> </thead> <tbody> <tr> <td>KW-76</td> <td style="text-align: center;">1</td> <td style="text-align: center;">-</td> <td style="text-align: center;">78</td> <td style="text-align: center;">1</td> <td rowspan="4" style="text-align: center; vertical-align: middle;">           ACCOUNTING LEGEND         </td> </tr> <tr> <td>KW-76</td> <td style="text-align: center;">1</td> <td style="text-align: center;">-</td> <td style="text-align: center;">83</td> <td style="text-align: center;">1</td> </tr> <tr> <td>KWK-43</td> <td style="text-align: center;">1</td> <td style="text-align: center;">-</td> <td style="text-align: center;">45</td> <td style="text-align: center;">4</td> </tr> <tr> <td>KWX-65</td> <td style="text-align: center;">1</td> <td style="text-align: center;">-</td> <td style="text-align: center;">98</td> <td style="text-align: center;">4</td> </tr> <tr> <td colspan="6" style="text-align: center;">           // // // // // // // // NOTHING FOLLOWS // // // // // // // //         </td> </tr> <tr> <td colspan="6">           THE ABOVE LISTED ITEMS WERE RECEIVED ON 12 OCTOBER 1984 FROM ELECTRONIC INTERNATIONAL CORP., BOSTON, MASS., ARFCDS NO. 15806. NO PAPERWORK OR TRANSFER REPORTS WERE INCLUDED IN THE SHIPMENT.         </td> </tr> <tr> <td colspan="6" style="text-align: center;">           APPROPRIATE REASON FOR PREPARING POSSESSION REPORT AND ADDITIONAL INFORMATION AS AVAILABLE.         </td> </tr> <tr> <td colspan="6" style="text-align: center;">           EXAMPLE OF A POSSESSION REPORT PREPARED WHEN COMSEC MATERIAL IS RECEIVED LESS TRANSFER REPORT.         </td> </tr> </tbody> </table>				8 SHORT TITLE	10 QUANTITY	11 ACCOUNTING NUMBERS		12 ALC	13 REMARKS	BEGINNING	ENDING	KW-76	1	-	78	1	ACCOUNTING LEGEND	KW-76	1	-	83	1	KWK-43	1	-	45	4	KWX-65	1	-	98	4	// // // // // // // // NOTHING FOLLOWS // // // // // // // //						THE ABOVE LISTED ITEMS WERE RECEIVED ON 12 OCTOBER 1984 FROM ELECTRONIC INTERNATIONAL CORP., BOSTON, MASS., ARFCDS NO. 15806. NO PAPERWORK OR TRANSFER REPORTS WERE INCLUDED IN THE SHIPMENT.						APPROPRIATE REASON FOR PREPARING POSSESSION REPORT AND ADDITIONAL INFORMATION AS AVAILABLE.						EXAMPLE OF A POSSESSION REPORT PREPARED WHEN COMSEC MATERIAL IS RECEIVED LESS TRANSFER REPORT.				
8 SHORT TITLE	10 QUANTITY	11 ACCOUNTING NUMBERS		12 ALC			13 REMARKS																																																	
		BEGINNING	ENDING																																																					
KW-76	1	-	78	1	ACCOUNTING LEGEND																																																			
KW-76	1	-	83	1																																																				
KWK-43	1	-	45	4																																																				
KWX-65	1	-	98	4																																																				
// // // // // // // // NOTHING FOLLOWS // // // // // // // //																																																								
THE ABOVE LISTED ITEMS WERE RECEIVED ON 12 OCTOBER 1984 FROM ELECTRONIC INTERNATIONAL CORP., BOSTON, MASS., ARFCDS NO. 15806. NO PAPERWORK OR TRANSFER REPORTS WERE INCLUDED IN THE SHIPMENT.																																																								
APPROPRIATE REASON FOR PREPARING POSSESSION REPORT AND ADDITIONAL INFORMATION AS AVAILABLE.																																																								
EXAMPLE OF A POSSESSION REPORT PREPARED WHEN COMSEC MATERIAL IS RECEIVED LESS TRANSFER REPORT.																																																								
14 THE MATERIAL HEREON HAS BEEN		<input checked="" type="checkbox"/> RECEIVED <input type="checkbox"/> INVENTORED <input type="checkbox"/> DESTROYED																																																						
15 SIGNATURE OF COMSEC CUSTODIAN <i>Robert L. Shea</i>		17 SIGNATURE OF <input type="checkbox"/> WITNESS <input type="checkbox"/> OTHER LEGION																																																						
16 TYPED OR STAMPED NAME, GRADE, SERVICE ROBERT L. SHEA		18 TYPED OR STAMPED NAME, GRADE, SERVICE																																																						
19 FOR DEPARTMENT OR AGENCY USE		20 PAGE 1 of 1 PAGES																																																						

FORM 7602-02-455-8880

FOR OFFICIAL USE ONLY

STANDARD FORM 163 (Rev. 8-75)  
 PRESCRIBED BY GPO  
 DOD KAG-1 163-118

Possession Report Prepared When COMSEC Material is Received Less Transfer Report (SF-153)

CLASSIFICATION

DATE 06 AUG 84

EXAMPLE OF COMSEC MATERIAL INVENTORY

OUTGOING TN 395008

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 82	880092	1		TRANSFERRED
KAM-143	A	A	1	540	540	1	106001	12 DEC 82	880099	1		TO NSA ACCT
KG-10	-	-	-	1070	1070	1	166809	16 DEC 82	880099	1		880641 TN
KG-10(V-1)	-	-	-	34	34	1	111105	20 DEC 82	880091	1		NO. 395074
ST-26	-	-	-	20	30	1	100000	31 DEC 82	880099	1		DATED 4AUG84

Preprinted Inventory

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)

DATE OF INVENTORY

*Jack A. Jones*

16 Aug 1984

SIGNATURE (WITNESS)

DATE OF INVENTORY

*Robert Elliott*

16 Aug 1984

CLASSIFICATION

CLASSIFICATION

DATE 25 JAN 84

EXAMPLE OF CONSE  
MATERIAL INVENTORY  
WITH SUPPLEMENT

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 82	880092	1	TRANSFERRED	TO NSA ACCT 880641 TN NO. 395074 DATED 4JAN84
KAM-143	A	A	1	540	540	106001	12 DEC 82	880099	1			
KG-10	-	-	-	1070	1070	166809	16 DEC 82	880099	1			
KG-10(V-1)	-	-	-	34	34	111105	20 DEC 82	880091	1			
ST-26	-	-	-	30	30	100000	31 DEC 82	990099	1			
/	/	/	/	/	/	/	/	/	/	/	/	/

NOTHING FOLLOWS / / / / /

I CERTIFY THAT I HAVE PHYSICALLY INVENTORIED  
THE MATERIAL LISTED HEREON. I FURTHER CERTI-  
FY 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 1 PAGE(S)  
OF SUPPLEMENTAL SF-153, CONSTITUTES A COM-  
PLETE INVENTORY OF ACCOUNTABLE CONSEC 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.

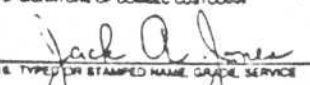
SIGNATURE (CUSTODIAN) DATE OF INVENTORY  
*Jack A. Givner* 2 Feb 1984

SIGNATURE (WITNESS) DATE OF INVENTORY  
*Robert Elliott* 2 Feb 1984

CLASSIFICATION

COMSEC  
MATERIAL REPORT

OMB  
Approval No. 27-R0164

<input type="checkbox"/> TRANSFER		<input type="checkbox"/> INVENTORY		<input type="checkbox"/> DESTRUCTION		<input type="checkbox"/> HAND RECEIPT		Supplement to Inventory <input checked="" type="checkbox"/> OTHER (Specify)				
F R O M  JONES ASSOCIATES 5959 COMSEC WAY NOWHERE, MT 12345				ACCT NO. 870395		DATE OF REPORT (Y., Mo., Da.) 840202		OUTGOING NUMBER 395008				
T O  DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MARYLAND 20755-6000				ACCT NO.		ACCOUNTING LEGEND CODES 1 ACCOUNTABLE BY SERIAL NO. IN CMCS 2 ACCOUNTABLE BY QUANTITY IN CMCS 3 ACCOUNTABLE BY SERIAL NUMBER 4 INITIAL RECEIPT CONTROL (AW SERVICE/ AGENCY DIRECTIVES)						
SHORT TITLE						QUANTITY		ACCOUNTING NUMBERS		ALC	REMARKS	
KAG-48						1		445 445		1	NOTE: ABOVE RECEIVED FROM 880099 ON TN395004 ON 13 JANUARY 1984.	
////////////////////////////////////NOTHING FOLLOWS////////////////////////////////////												
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:						
						<input checked="" type="checkbox"/> WITNESS <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						

NSM 7540-00-005-4000

FOR OFFICIAL USE ONLY

STANDARD FORM 163 (Rev. 6-78)  
PRESCRIBED BY GPO  
DOD KAG-1 163-118

Supplement to Preprinted Inventory (Continued)



COMSEC  
MATERIAL REPORT

OMB  
Approval No. 22-R0164

<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., Day) 3/4/03	5. OUTGOING NUMBER 399004		
	<div style="border: 1px solid black; border-radius: 50%; padding: 5px; display: inline-block;">             DATE REPORT IS PREPARED           </div>	6. DATE OF TRANSACTION (Yr., Mo., Day) LEAVE BLANK	7. INCOMING NUMBER LEAVE BLANK			
3 T O	DIRECTOR NATIONAL SECURITY AGENCY OPERATIONS BUILDING NO. 3 (Y13) ROOM C1B51 FORT GEORGE G. MEADE, MARYLAND 20755-6000	ACCT. NO.	8. ACCOUNTING LEGEND CODES 1. ACCOUNTABLE BY SERIAL NO. IN CMCS 2. ACCOUNTABLE BY QUANTITY IN CMCS 3. ACCOUNTABLE BY SERIAL NUMBER LAW SERVICE/AGENCY DIRECTIVES 4. INITIAL RECEIPT CONTROL LAW SERVICE/ AGENCY DIRECTIVES			
9	SHORT TITLE	10 QUANTITY	11 ACCOUNTING NUMBERS		12 ALC	13 REMARKS
			BEGINNING	ENDING		
1	KAM-109 A	2	1125	1126	1	
2	KAM-114 C	1	-	965	1	
3	AMEND 1 TO KAM-140 A	1	-	169	4	RESIDUE
4	AMEND 2 to KAM-140 A	1	-	185	4	RESIDUE
5	// // // // // // // // // // NOTHING FOLLOWS // // // // //					
6						<div style="border: 1px solid black; border-radius: 50%; padding: 5px; display: inline-block;">             ACCOUNTING LEGEND           </div>
7						
8						
9						
10						
11	AUTHORITY FOR DESTRUCTION: HANDLING INSTRUCTIONS OF SUPERSEDING					
12	EDITIONS.					
13						
14						
15	<div style="border: 1px solid black; padding: 5px; display: inline-block;">             EXAMPLE OF A DESTRUCTION REPORT OF COMSEC MATERIAL.           </div>					
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 type="checkbox"/> INVENTORIED <input checked="" type="checkbox"/> DESTROYED						
15. SIGNATURE OF COMSEC CUSTODIAN <i>Robert L. Shea</i>			17. SIGNATURE OF <input checked="" type="checkbox"/> WITNESS <i>Walter J. Hoffman</i> <input type="checkbox"/> OTHER (Specify)			
16. TYPED OR STAMPED NAME, GRADE, SERVICE ROBERT L. SHEA			18. TYPED OR STAMPED NAME, GRADE, SERVICE WALTER J. HOFFMAN, ALTERNATE CUSTODIAN			
19. FOR DEPARTMENT OR AGENCY USE:						
					20. PAGE   of   PAGES	

NSM 7540-00-405-8880

STANDARD FORM, 153 (Rev. 9-79)  
 PRESCRIBED BY GPO  
 OGD KAO-1 153-118

FOR OFFICIAL USE ONLY

Destruction Report (SF-153)



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 84		
	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 Jul 84	BS	1 Jul 84

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 reissue. Signature signifies understanding.

RECIPIENT	PRINTED NAME	ORGANIZATION	RECEIVED
	SIGNATURE	PHONE	DATE
REMOVAL AUTHORIZED BY	RETURNED TO		DATE

Jack E. Jones  
 Eng Lab  
 Jack Jones  
 Bill Smith, Comsec Custodian  
 Bill Smith  
 1 Jul 69  
 3 Jul 69  
 11 Jul 69

FORM A1721 REV MAR 82 (Supersedes A1721 REV MAR 71 which is obsolete)

COMSEC Material Hand Receipt Utilizing an A-1721



[CLASSIFICATION]

MASTER DISPOSITION RECORD OF ACCOUNTABLE COMSEC MATERIAL  
BY SERIAL NUMBER

SHORT TITLE KGP-94	CONTRACTOR OK, INC.	CONTRACT NO. DAAB03-67-C-9999
-----------------------	------------------------	----------------------------------

ACCOUNTING (SERIAL) NUMBERS	RECEIVING ACCOUNT	DATE SHIPPED	TRANSACTION NUMBER	ARFCOS REG. MAIL, GBL NUMBER OR OTHER APPROPRIATE CONTROL NUMBER	DD 250 PARTIAL NUMBER
1	880686	5 MAY 69	396010	500309	13
2	880604	7 MAY 69	396012	500310	14
3	880645	27 APR 69	396001	500215	6
4	┆	┆	┆	┆	┆
5	┆	┆	┆	┆	┆
6	780030	1 JUN 69	396021	500325	18
7	┆	┆	┆	┆	┆

[CLASSIFICATION ]

MASTER DISPOSITION RECORD OF ACCOUNTABLE COMSEC MATERIAL  
CONTRACT SUMMARY

SHORT TITLE <u>KGP-94</u>	CONTRACTOR <u>OK, INC.</u>	CONTRACT NO. <u>DAAB03-69-C-9199</u>
------------------------------	-------------------------------	---

SERIAL NUMBERS ASSIGNED BY NSA COR: 1-1459

CONSUMERS:

QUANTITIES:

<u>ARMY</u>	<u>211</u>
<u>NAVY</u>	<u>900</u>
<u>AIR FORCE</u>	<u>300</u>
<u>FBI</u>	<u>48</u>

TOTAL 1,459

PAGE 1 OF XX

[CLASSIFICATION]

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.

Sample COMSEC Material Identification Markings

APPENDIX 2 TO ANNEX C



The encircled numbers represent the address listed.

ARFCOS STATIONS

- |  |   |   |
|--|---|---|
| <p>1. ANCHORAGE<br/>Building 31-200<br/>Elmendorf AFB, Alaska<br/>Commercial: (907)552-3612/5534</p>                                       | <p>7. JACKSONVILLE<br/>Building 934<br/>Naval Air Station<br/>Jacksonville, FL<br/>Commercial: (904)772-2784</p>                    | <p>Norfolk, VA<br/>Commercial: (804)444-3471/3472/<br/>3473</p>   |
| <p>2. BOSTON<br/>Building 225<br/>Naval Air Station<br/>South Weymouth, MA<br/>Commercial: (617)786-2780/2781/<br/>2957/2958<br/>/2558</p> | <p>8. KELLY<br/>Building 1470<br/>Kelly AFB, TX<br/>Commercial: (512)925-3704</p>   | <p>13. OFFUTT<br/>MOD "B"<br/>Offutt AFB, NE<br/>Commercial: (402)294-5354/5355/<br/>5356</p>   |
| <p>3. CHARLESTON<br/>Air Freight Building (S-178)<br/>Charleston AFB, SC<br/>Commercial: (803)554-2191/3603/<br/>2401</p>                  | <p>9. LOS ANGELES<br/>Building 205<br/>Los Angeles Air Force Station<br/>El Segundo, CA<br/>Commercial: (213)643-1878/1879</p>      | <p>14. SAN DIEGO<br/>Building 1<br/>937 North Harbor Drive<br/>San Diego, CA<br/>Commercial: (714)235-3381/3382</p>                         |
| <p>4. DENVER<br/>Building 612<br/>Rocky Mountain Arsenal<br/>Commerce City, CO<br/>Commercial: (303)289-0287/0293/<br/>0294</p>            | <p>10. MCCHORD<br/>Building 1410<br/>McChord AFB<br/>Tacoma, WA<br/>Commercial: (206)984-5903/2426</p>                              | <p>15. TRAVIS<br/>Building 934<br/>Travis AFB<br/>Fairfield, CA<br/>Commercial: (707)438-2641/2642</p>                                      |
| <p>5. DOVER<br/>Building 505<br/>Dover AFB, DE<br/>Commercial: (302)678-6063/6064</p>  | <p>11. MCGUIRE<br/>Building 17-02<br/>Air Freight Warehouse<br/>McGuire AFB, NJ<br/>FTS: 484-4534<br/>Commercial: (609)723-7937</p> | <p>16. WASHINGTON<br/>Special Activities Building 3, NSA<br/>Fort George G. Meade, MD<br/>Commercial: (301)688-7454/7455/<br/>7456/7457</p> |
| <p>6. HONOLULU<br/>Building 4069<br/>Air Freight Building<br/>Hickam AFB, HI</p>   | <p>12. NORFOLK<br/>Building LP-82<br/>Naval Air Station</p>   | <p>17. WRIGHT-PATTERSON<br/>Building 829, Area "A"<br/>Wright-Patterson AFB, OH<br/>Commercial: (513)257-3121/3517/<br/>6130</p>            |

ARFCOS Stations Addresses

**APPENDIX 3 TO ANNEX C**

**Certificate of Action Statement**

I certify that the actions requiring my attention have been accomplished as required by the COMSEC audit of COMSEC Account 870435 on 27 September 1984.

Signature \_\_\_\_\_

COMSEC Custodian, Account 870435

Date \_\_\_\_\_

C-3-1

**FOR OFFICIAL USE ONLY**



## ANNEX D

### PHYSICAL SECURITY

#### I. GENERAL

A. This Annex describes the minimum requirements for the physical security of, and access to:

1. Equipments and components which are designated as "Controlled Cryptographic Items" or "CCI." This Annex only applies to CCI equipment which are finished products (the physical security of CCI equipment during their development and production is addressed elsewhere).

2. Classified and unclassified keying materials.

3. Other related materials, such as operating instructions, maintenance manuals, etc., both classified and unclassified.

B. CCI equipments are by definition unclassified, but controlled. Because the unclassified CCI equipment can be used to protect classified information, (in which case they are keyed with classified key), they require different levels of physical protection at different times, depending upon the sensitivity of the keying material which is being used. This Annex, therefore, prescribes minimum controls for CCI equipment under two different conditions: keyed and unkeyed.

C. The requirements dealing with physical security and access in this chapter pertain to all CCI equipment, keying material, and related materials owned, acquired, or used by U.S. Government contractors. In the case of particular equipment or materials there may be special requirements unique to that item. These unique requirements are listed in Annex I, where there is an Appendix for each equipment or other item which has additional or different control requirements.

#### D. References

1. The following reference documents may be useful to certain Government contractors in addressing questions on physical security and access to classified information, keying material, and related materials.

a. DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information", dated December 1985 (UNCLASSIFIED).

b. DoD 5220.22-S-1, "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information", dated 12 August 1983 (UNCLASSIFIED).

## II. CCI Equipment

### A. Access

1. Equipments designated by the National Security Agency (NSA) as CCI equipment will be identified by a "Controlled Cryptographic Item" or "CCI" label permanently affixed in a clearly visible location on the equipment. Cryptographic components (e.g., printed circuit boards, modules, LSI chips, etc.) designated as Controlled Cryptographic Items will be clearly marked as "CCI" on the component. For the purposes of this Annex, the term "CCI equipment" encompasses all designated CCI components. The primary difference in controls between CCI equipment and components is that CCI equipment are continuously tracked by serial number, whereas CCI components, spare parts, etc., are accounted for by quantity. Accounting procedures for both CCI equipment and components are contained in Annex C.

2. Certain requirements must be met in order to access CCI equipment. "Access" to CCI equipment is defined as installing, troubleshooting, maintaining, and keying the CCI equipment. "Keying" includes all keying-related changes to the equipment, such as inserting Crypto Ignition Keys (CIKs), loading electronic key, and updating or zeroizing existing keys.

3. Contractor personnel who need access (as defined in the previous paragraph) to CCI equipment must meet the following requirements:

a. Be a U.S. citizen whose duties specifically require access.

b. Be thoroughly indoctrinated and aware of the importance of safeguarding CCI equipment and keying materials prior to being given access.

(1) The contractor is responsible for ensuring that all personnel having access to CCI equipment have been given, and understand, the COMSEC briefing contained in Appendix 1 to this Annex.

(2) The contractor will maintain records of each briefing for at least five years from its date, identifying the person briefed, the person who administered the briefing, and the date and place of the briefing.

(3) Note: Annual rebriefings are required for all personnel who have continuing access to classified information or equipment.

c. Be completely familiar with the contents of the contractor's Standard Practice Procedures (SPP) for CCI Equipment.

(1) The Industrial Security Manual for Safeguarding Classified Information requires contractors with classified contracts to publish an SPP

which explains the Government's security requirements in terms of the particular contractor's procedures and facilities.

(2) The COMSEC Supplement to the Industrial Security Manual additionally requires that COMSEC security procedures be included in the SPP, or attached as a supplement to the SPP.

(3) If an SPP is or has been established as part of a classified contract and facility clearance, then specific security procedures pertaining to the handling of CCI equipment will be included in the SPP. If access to CCI equipment is required in connection with an unclassified contract, in which case an SPP may not already exist, then an SPP will be prepared which covers the security requirements of CCI equipment. In either situation, the SPP will address the points contained in the "SPP Checklist" contained in Appendix 5 to this Annex.

d. Possess a security clearance at least equal to the classification level of any keying material associated with or being used by the CCI equipment during the period of access.

4. Access to CCI equipment by a foreign national or resident alien is prohibited. Requests for access by non-U.S. citizens must be submitted to NSA for approval on a case-by-case basis.

5. Unescorted users of keyed CCI equipment or its connected telecommunications systems, who do not require access as defined above, must:

a. Be familiar with the contractor's Standard Practice Procedures for CCI equipment.

b. Possess a security clearance at least equal to:

(1) The classification level of the keying material being used; or

(2) The classification level which is self-authenticated when the system is used (i.e., a given system may have TOP SECRET keying material installed, but a self-authenticating level of SECRET, because all users of the system require at least a SECRET clearance).

#### B. Physical Security

1. Installed and unkeyed (e.g., with key zeroized) 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. Where it is practical, rooms containing unkeyed CCI equipment should be locked at the end of the work day.

2. Installed equipment which is keyed must be protected as follows:

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. If the keying material is unclassified, 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: CCI equipment must be in an area that is constructed and controlled to protect the highest level of classified keying material in use. If any of the keying material is classified, the construction and controls on the area housing the CCI equipment must meet the requirements of section IV. B. of this Annex. If the keying material is unclassified, the contractor is responsible for preventing access by unauthorized personnel through the use of adequate physical controls (e.g., locked room, alarms, random checks, etc.).

3. Storage (uninstalled)

a. With the exception of permanently keyed devices noted below, CCI equipment must never be stored in a keyed condition. Prior to placing a CCI equipment in storage all keying material must be removed, and internal key storage registers must be zeroized. Permanently keyed devices (e.g., equipment with the key hard-wired into the circuitry) will be provided physical security commensurate with the installed key.

b. 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).

4. As a general rule, CCI equipment should be protected as high value property, with access (as defined above) limited to U.S. citizens who require access as part of their normal duties. When a CCI equipment is keyed with classified keying materials, however, the equipment must be protected in accordance with the classification level of the key.

C. Transportation

1. The accounting procedures in Annex C will be followed during the transportation of CCI equipment. The basic requirement is that proper receipting be employed to maintain accountability. "Transportation" here refers only to physical transfers between COMSEC accounts; local movements of unkeyed CCI equipment (i.e., within a building) may be performed by any contractor personnel who are U.S. citizens, have been given the COMSEC

briefing in Appendix 1 of this Annex, and who are completely familiar with the contents of the contractor's Standard Practice Procedures (SPP) for CCI equipment.

2. CCI equipment will be transported only in the following ways (see section VI of this Annex):

- a. By NSA-approved commercial carrier.
- b. By the Government contractor's authorized company courier.
- c. By U.S. registered mail (the package will not have any exterior markings, however, which indicate that it contains a cryptographic or CCI device).

d. By authorized U.S. Government courier service, including the Armed Forces Courier Service (ARFCOS) and the U.S. Diplomatic Courier Service.

e. CCI equipment will normally be shipped to contractor COMSEC accounts via authorized commercial carrier, authorized company courier, or U.S. registered mail. Certain CCI equipment which may have permanently installed "hard-wired" keying materials may be required to be transported by a Government courier service, cleared commercial carrier, or appropriately cleared and authorized company courier. Unkeyed CCI equipment will not normally be transported via a Government courier service without the approval of the appropriate COR.

3. CCI equipment will not be transported outside the United States without the prior approval of the NSA or its designated representative. Requests for such approval will be submitted to NSA (Y1) via the contractor's COMSEC account Central Office of Record (COR).

4. CCI equipment will not be transported while they are in a keyed condition, unless the CCI equipment is designed to operate with a permanently installed hard-wired key. In this case the equipment will be transported in a way which meets all the security requirements for transporting the installed key.

#### D. Maintenance

1. Initial installation and all subsequent maintenance of CCI equipment will be performed only by U.S. citizens who are authorized for access to CCI equipment, and who are qualified to perform such installation and maintenance.

2. Personnel performing maintenance on CCI equipment must possess a security clearance at least equal to the classification level of the NSA-approved maintenance manual (if it is classified).

3. Maintenance of CCI equipment by foreign nationals or resident aliens is prohibited. Proposals for CCI equipment maintenance by foreign nationals or resident aliens must be submitted to the NSA for approval on a case-by-case basis.

4. Qualified maintenance personnel are those individuals who have satisfactorily completed an NSA-approved maintenance training course.

5. Re-installation of CCI equipment in an otherwise previously certified (see Annex H) installation can be performed by knowledgeable personnel who do not meet the criteria of "qualified maintenance personnel" above. Personnel performing re-installation must, however, meet the CCI equipment access requirements, and be careful not to disturb the security integrity of the installation.

6. Personnel who are qualified to perform limited or full maintenance may install CCI equipment and perform board replacements. Personnel performing piece-part replacement of components, previously identified as defective by either automated test equipment or qualified maintenance personnel, do not require NSA-approved training on the equipment. However, supervision by a qualified full maintenance technician is required. Qualified maintenance personnel must verify the proper operation of the repaired equipment prior to operation use.

7. When maintenance is performed on elements of the telecommunications system other than the CCI equipment or component, care must be exercised so that the total system security integrity is not reduced.

8. When maintenance involves the replacement of piece-parts for any CCI equipment or component, the qualified maintenance technician performing or supervising the parts replacement will ensure that only standard/specified parts are used. Modifications or the use of non-standard parts must be proposed and approved by NSA in advance of the modification or replacement.

#### E. Protected distribution systems

1. Distribution systems (e.g., cables) carrying unencrypted classified (RED) information must be protected to prevent unauthorized access or the compromise of the classified information.

2. Where the distribution system remains entirely within the confines of a controlled space, that space is considered to provide the

necessary protection. A controlled space is the three dimensional space surrounding the CCI equipment and the distribution system, within which access to and use of CCI equipment is controlled.

3. When the distribution system is installed within the United States, and runs outside the controlled space, installation of distribution cables will be made visually inspectable (i.e., either hidden or visible, but easily capable of being periodically inspected). Except as specified in Annex I, conduit is not required for distribution lines installed within the United States.

4. Additional protection may be required for particular equipment (see Annex I), for operation in high risk areas, or in cases which involve extremely sensitive information.

5. Inspections shall be made by the Facility Security Supervisor or by a person designated by the FSS with authorized access to the information protected by the distribution system. Inspections should be performed on an irregular/random basis (at least four times a year), to ensure the continued integrity of the distribution system.

#### F. Disposition

1. Under the CCI Control Agreement, all contractors holding CCI equipment as contractor acquired property (Government ownership) or as contractor owned property have a formal agreement with the Government, and legal responsibility, to dispose of the equipment only in a prescribed fashion. The primary interest of the Government is that CCI equipment must:

a. Be sold or re-sold only to recipients authorized to use or possess them.

b. Be destroyed only with NSA approval and in accordance with NSA-prescribed procedures.

2. Contractors will not destroy any CCI equipment without specific written approval from NSA.

3. CCI equipment may only be sold to:

a. U.S. Government departments and agencies (civilian and military) which have COMSEC Accounts. Information on the current status of Government COMSEC Accounts may be obtained from the appropriate Central Office of Record (COR) from the list in Annex B, or from the NSA.

b. Government contractors having a current contract with the Government and an established COMSEC Account (classified or unclassified).

4. When a contractor re-sells CCI equipment to another authorized Government contractor, the seller is required to verify with the NSA that:

a. The receiving contractor has a current COMSEC Account.

b. The receiving contractor has a current memorandum of agreement with NSA on the terms and conditions for receiving CCI equipment, called the "CCI Control Agreement." A copy of the standard CCI Control Agreement is contained in Annex A.

5. When a contractor re-sells CCI equipment to any U.S. Government department or agency, the seller is required to verify with the NSA that the Government department or agency has a current COMSEC Account.

### **III. Fill Devices for Loading Key**

A. Fill devices are ancillary devices used for loading electronic key, reading keying tapes, etc., in order to key CCI equipment. Although they do not contain circuitry embodying sensitive cryptographic algorithms, they are critical pieces of the cryptographic system which require protection.

B. The access, physical security, transportation, storage, maintenance and disposition requirements for fill devices used to key CCI equipment are identical to those of the CCI devices themselves (fill devices will normally be designated "CCI").

C. Due to the nature of fill devices, special care should be taken to ensure that they are neither stored nor shipped while in a keyed condition. When keyed with classified key, fill devices will be handled in the same manner required for the keying material they contain.

### **IV. Keying Material**

#### **A. General**

1. Only NSA-produced or NSA-authorized keying material will be used with CCI equipment.

2. Keying material used in CCI equipment will be marked "CRYPTO," with the exception of maintenance or test key. Non-"CRYPTO" test keys may be used to test or for on-the-air demonstrations, provided that all traffic encrypted and transmitted is limited to unclassified, non-operational information (e.g., "Testing, one, two, three..." etc.).



3. Additional control requirements for certain types of keying material may appear in the handling or operating instructions of particular systems.

4. Access to keying material must be kept to a minimum, based upon a strict need-to-know. All individuals granted access to keying material must be thoroughly indoctrinated and aware of the special sensitivity of keying material marked "CRYPTO", must have received the cryptographic briefing contained in Appendix 1 to this Annex.

5. Access to keying material is defined as the handling of hard copy keying material (e.g., paper tapes, code books, key lists, tape canisters, etc.) loaded electronic transfer and key fill devices, and loaded crypto ignition keys.

6. Access to keying material in any form, classified or unclassified, by foreign nationals or resident aliens is prohibited.

7. Users of CCI equipment should be given access only to the current edition of keying material for that equipment. Superseded keying material will be destroyed (and accounted for) as soon as possible after supersession.

8. Keying material in segmented key tape form must remain in its protective canister until actually used.

9. Future editions of keying material should be stored where access is limited to the COMSEC account custodian and alternate custodian.

10. Currently effective keying material should be retained by the COMSEC account custodian/alternate and only be issued as needed to authorized users. If an entire edition or canister of keying material is issued to users, they are required to provide adequate safeguards for the material as specified in the following sections.

#### B. Classified Keying Material

##### 1. Access

a. Access to classified keying material may be granted to personnel who:

(1) Are U.S. citizens.

(2) Have been granted a final Government security clearance equal to or higher than the classification of the keying material.

(3) Have duties which require access.

(4) Have received the COMSEC briefing contained in Appendix 1 to this Annex within the past year.

(5) Are completely familiar with the contents of the contractor's Standard Practice Procedures for classified keying materials.

b. Contractor granted CONFIDENTIAL clearances are not valid for access to classified keying material.

c. Personnel performing the keying material loading function (via hard copy or electronic fill device) must meet the requirements for access to the keying material. They must also be knowledgeable of the key loading procedures for the particular CCI equipment which they are keying.

## 2. Transportation

a. Individual keying materials must be moved in the custody of authorized, cleared Government couriers, NSA-approved cleared commercial carriers, or authorized company couriers with the appropriate security clearance (see section VI. of this Annex).

a. Individual editions of CONFIDENTIAL keying material may be transported via U.S. registered mail, provided that 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.

b. Bulk shipment (i.e., more than one edition) of CONFIDENTIAL keying material must be sent in the same manner as SECRET and higher keying materials.

## 3. Storage

Unless appropriately cleared personnel are using or otherwise safeguarding keying material, it will be stored in accordance with the following minimum requirements:

a. TOP SECRET keying material shall be stored in:

(1) A GSA approved Class 5 or 6 steel security file cabinet procured from the GSA Federal Supply Schedule; or

(2) A Class "A" vault

(a) Floors and walls should be of poured, reinforced concrete which has a minimum thickness of eight inches. The walls shall solidly connect with the vault roof and floor. The floors and walls shall be reinforced with reinforcing rods, at least 3/8 inch in diameter, mounted vertically and horizontally on centers not less than two inches and not greater than ten inches.

(b) The roof should be a monolithic reinforced concrete slab with a minimum thickness of eight inches.

(c) The vault door and frame shall afford protection not less than that provided by a Class 5 vault door.

(d) The combination lock shall conform to the Underwriters' Laboratories, Inc., Standard 768, for Group 1.

(3) An alarmed or guarded area, provided the area is substantially constructed and has adequate physical barriers to prevent surreptitious entry. The physical barriers must be such that forcible entry will give evidence of such entry into the room and register an alarm or alert a guard. The alarm system must as a minimum provide notice to a security force which must be able to respond in 15 minutes.

b. SECRET keying material shall be stored in:

(1) Any manner approved for TOP SECRET; or

(2) A GSA approved steel security file cabinet procured from the GSA Federal Supply Schedule. Previously authorized containers may remain in use. New procurements must be GSA approved Class 5 or 6 steel security file cabinets; or

(3) A Class "B" vault:

(a) Floor must be monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than six inches thick.

(b) Walls must be of not less than eight inch thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least six inches thick may also be used, and shall be used in seismic areas.

(c) The roof must be a monolithic reinforced concrete slab of not less than six inches in thickness.

(d) The vault door and frame unit and the combination lock must meet the same requirements as for a Class "A" vault (see paragraphs b. (2) (c) and (d) above).

c. CONFIDENTIAL keying material shall be stored in:

(1) The same manner as SECRET or TOP SECRET keying material;  
or

(2) A steel file cabinet having a built-in, changeable Group 1R three-position combination lock which conforms to the Underwriters' Laboratories, Inc., Standard 768, for Group 1R locks.

#### 4. Destruction

a. Routine destruction of classified keying material - Keying material which is superseded or has otherwise served its intended purpose is normally destroyed by the COMSEC Custodian or by the Alternate COMSEC Custodian and witnessed by an appropriately cleared person. The short title, edition number and accounting number of each item shall be verified immediately prior to destruction.

(1) However, the COMSEC Custodian may delegate the destruction authority to others within the facility in those instances where adherence to this restriction would delay destruction even for a short time. The following subparagraphs outline various types of procedures which might be followed in representative situations.

(2) In a large facility, operators may be granted authority to destroy keying material they use, as soon as the material is replaced or superseded. Operators may accomplish destruction by placing the material in an approved destruction device, if one is available in the immediate vicinity. The individual performing keying material destruction and an appropriately cleared witness shall initial an appropriate record, e.g., the segment information card enclosed with the canister or other appropriate local form, showing the material which is being destroyed. This record shall be provided to the COMSEC Custodian, who shall review and consolidate similar information and use it to prepare formal destruction reports.

(3) In a small communications facility with only a few COMSEC equipments, the COMSEC Custodian may personally collect used or superseded keying material, replace it with new material, and effect timely destruction of the old material, in the presence of an appropriately cleared witness.

(4) In mobile situations, routine destruction may be accomplished at the using facility by a responsible individual and an appropriately cleared witness. The issuing COMSEC Custodian must be advised by the user in writing that he has destroyed the material. 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 the superseded material, and for prompt reporting of loss of control of material before destruction could be accomplished.

b. Routine destruction scheduling.

(1) Keying material designated CRYPTO which has been issued for use should be destroyed as soon as possible after supersession, and may not be held for longer than 72 hours following supersession. In the case of an extended holiday period (over 72 hours), the material shall be destroyed the first normal work day following the holiday period.

(2) Used maintenance keying materials not designated CRYPTO are not regularly superseded and need only be destroyed when physically unserviceable.

(3) DO NOT DESTROY defective or faulty COMSEC material. Such material should be reported to NSA, ATTN: S2, and held for disposition instructions.

(4) COMSEC Custodians are authorized to destroy future keying material when it is reasonably certain that actual use will not be needed. This would occur, for example, during scheduled holiday periods, temporary facility closings, etc. If there is any question concerning the possible use for routine destruction, the keying will not be destroyed until it is superseded.

c. 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.

(1) A variety of destruction methods are approved for destroying keying materials. These are listed in Appendix 2, Annex D ("NSA-Approved Paper Destruction Devices"). The general rules are:

(a) When destroying keying 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.

(b) When pulping, pulverizing, or chopping devices are used to destroy keying materials, they must reduce the materials to bits no larger than five millimeters in any dimension.

(c) Crosscut (double cut) shredders may be used which reduce residue to shreds not more than 3/64-inch (1.2 mm) in width and not more

than 1/35-inch (13.0 mm) in length, or not more than 1/35-inch (0.73 mm) in width and not more than 7/8 (22.2 mm) in length.

(2) Obtaining approval from DIS for any devices used to accomplish destruction, as discussed above, is the responsibility of the contractor. Such approval will be withheld until it has been demonstrated that the device meets the above stated criteria and that periodic checking will be instituted to ensure that the above stated criteria will continue to be met. An additional significant consideration in selecting and approving devices for routine destruction is their usefulness should emergency destruction ever become necessary. In this regard, devices requiring long or complicated setup or make-ready procedures should be avoided as should devices which are not capable of extended full-capacity operation.

(3) Destruction procedures for key tape canisters - When an entire canister has been used and all the segments destroyed, the segment information card will be returned to the COMSEC Custodian. The Custodian will review the card to ensure that all tape segments were used and properly recorded on the card. The Custodian will then prepare a destruction report and return one copy to the NSA COR. COMSEC Custodians are to dispose of empty tape canisters: two methods are recommended below. The destruction objective is to disfigure the two large flat surfaces (sides) of the canister.

(a) Puncture: To protect personnel from possible injury from flying fragments while puncturing the empty canister, first place the canister inside the ziplock plastic bag provided. Then with a widebladed screwdriver and hammer, puncture one flat side of the canister approximately 3/4" from the rounded edge, avoiding the exact center. Turn the canister over and repeat. Dispose of the broken canister as unclassified trash. This method is recommended for single canister destruction.

(b) Smash: To protect personnel from possible injury from flying fragments while smashing empty canisters, first place each canister inside the ziplock bag provided. Then place the bagged canisters inside a canvas bag or wrap loosely in a protective cloth before smashing. After checking to assure the flat sides are destroyed, dispose of the residue as unclassified trash.

d. Reporting Destruction - The prompt physical destruction of keying material is mandatory. Procedures to be used in reporting destruction are described in Annex C, Section VI. Because the destruction of the wrong item can result in a possible compromise, the COMSEC Custodian and witness should take extreme care to assure that they are destroying the correct COMSEC Material and that the destruction report is completely accurate.

e. Emergency destruction of classified keying material - Should it become necessary to destroy classified keying material under emergency conditions (e.g., terrorist attack), emergency destruction will be performed

without undue risk to human life. In this case the priority for destruction is as follows:

- (1) Superseded keying materials still on hand.
- (2) Currently effective keying materials (including the zeroization of keyed equipment).
- (3) Future effective keying materials (if time and circumstance permit).

C. Unclassified Keying Material

1. Access:

a. Access to unclassified keying material marked "CRYPTO" will be limited to personnel who:

- (1) Are U.S. citizens.
- (2) Require access as part of their duties.
- (3) Have received the COMSEC briefing contained in Appendix 1 to this Annex.

4) Are completely familiar with the contents of the contractor's Standard Practice Procedures for unclassified keying materials.

b. Personnel performing the keying material loading function (via hard copy key or electronic fill device) must meet the requirements for access to the keying material. They must also be knowledgeable of the key loading procedures for the particular CCI equipment which they are keying.

2. Transportation

a. Unclassified keying material may be transported via any means suitable for classified keying material.

b. Individual editions or canisters of unclassified keying material may be sent via U.S. registered mail.

c. Multiple editions or canisters of unclassified keying material must be sent via U.S. Government courier services, a contractor's authorized company courier, or via NSA-approved commercial carriers.

3. Storage

a. Unclassified keying material may be stored in any means suitable for classified material.

b. Unclassified keying material will be stored in the most secure manner available (e.g., a locked desk or cabinet).

#### 4. Destruction

a. Routine destruction of unclassified keying material -Unclassified keying material which is superseded or has otherwise served its intended purpose is normally destroyed by authorized personnel in the presence of a witness.

(1) However, the COMSEC Custodian may delegate the destruction authority to others within the facility in those instances where adherence to this restriction would delay destruction even for a short time. The following subparagraphs outline various types of procedures which might be followed in representative situations.

(2) In a large facility, operators may be granted authority to destroy keying material they use, as soon as the material is replaced or superseded. Operators may accomplish destruction by placing the material in an approved destruction device, if one is available in the immediate vicinity. The individual performing keying material destruction and a witness shall initial an appropriate record, e.g., segment information card enclosed with the canister or other appropriate local form, showing the material which is being destroyed. This record shall be provided to the COMSEC Custodian, who shall review and consolidate similar information and use it to prepare formal destruction reports.

(3) In a small secure communications facility with only a few COMSEC equipments, the COMSEC Custodian may personally collect used or superseded keying material, replace it with new material, and effect timely destruction of the old material, in the presence of a witness.

(4) In mobile situations, routine destruction may be accomplished at the using facility by a responsible individual and a witness. The issuing COMSEC Custodian must be advised by the user in writing that he has destroyed the material. 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 the superseded material, and for prompt reporting of loss of control of material before destruction could be accomplished.

b. Routine destruction scheduling.



(1) Keying material designated CRYPTO which has been issued for use should be destroyed as soon as possible after supersession, and may not be held for longer than 72 hours following supersession. In the case of an extended holiday period (over 72 hours), the material shall be destroyed the first normal work day following the holiday period.

(2) Used maintenance keying materials not designated CRYPTO are not regularly superseded and need only be destroyed when physically unserviceable.

(3) DO NOT DESTROY defective or faulty COMSEC material. Such material should be reported to NSA, ATTN: S2, and held for disposition instructions.

(4) COMSEC Custodians are authorized to destroy future keying material when it is reasonably certain that actual use will not be needed. This would occur, for example, during scheduled holiday periods, temporary facility closings, etc. If there is any question concerning the possible use for routine destruction, it will not be destroyed until it is superseded.

c. 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.

(1) A variety of destruction methods are approved for destroying keying materials. These are listed in Appendix 2, Annex D ("Cryptographic Material Destruction Guidelines") and Appendix 3, Annex D ("NSA-Approved Paper Destruction Devices"). The general rules are described in IV.B.4.c. above.

d. Reporting Destruction - The prompt physical destruction of keying material is mandatory. Procedures to be used in reporting destruction are described in Annex C, Section VI. Because the destruction of the wrong item can result in a possible compromise, the COMSEC Custodian and witness should take extreme care to assure that they are destroying the correct COMSEC Material and that the destruction report is completely accurate.

e. Emergency destruction of unclassified keying material - Should an emergency situation (e.g., terrorist attack) occur, unclassified keying material will be destroyed only if time permits and there is no risk involved to personnel.

## V. Other Related Materials

### A. Classified Materials

#### 1. General

a. General COMSEC instructional documents, TEMPEST information, equipment operating and limited maintenance manuals, keying material not marked "CRYPTO," and other types of COMSEC information which are not covered elsewhere in this Annex will be safeguarded (during access, transportation, use, storage, and disposition) in a manner comparable to other national security information of equal classification, in accordance with the DoD 5220.22-M, the Industrial Security Manual for Safeguarding Classified Information.

#### 2. Other Cryptographic Materials

##### a. Access

(1) Other cryptographic materials may also be both classified and accountable (see Annex C). These will normally be media which embody, describe, or implement a classified cryptographic logic, such as full/depot maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications which describe a cryptographic logic, or cryptographic software. Access to these materials will be limited to:

(a) U.S. citizens.

(b) Personnel granted a final Government security clearance equal to or higher than the classification of the material involved.

(c) Personnel who have received the COMSEC briefing contained in Appendix 1 to this Annex.

(d) Personnel who require access as part of their duties.

(e) Personnel who are completely familiar with the contents of the contractor's Standard Practice Procedures as they pertain to handling these classified cryptographic materials.

##### b. Transportation

Other cryptographic materials shall be transported only by the following means:

(1) Authorized and cleared Government courier service (e.g., ARFCOS, Diplomatic Courier Service).

- (2) Authorized company couriers.
- (3) NSA-approved cleared commercial carriers.

c. Storage

Other cryptographic materials will be stored in the same manner as equally classified keying material. These requirements are contained in section IV.B.3 of this Annex.

d. Disposition

(1) Other cryptographic materials which are no longer required may be destroyed by the COMSEC account custodian/alternate, or returned to the account's Central Office of Record (COR) for disposition. The COMSEC account custodian/alternate should check with his COR for the correct disposition.

(2) If the custodian is to destroy the material, the procedures in section IV.B.4.g (for destroying classified keying material) apply.

B. Unclassified Materials

1. The distribution, use and possession of non-accountable, unclassified materials which are not marked "CRYPTO" but are related to the installation, operation and maintenance of CCI equipment will be restricted to those individuals who require such materials in the course of their duties.

**VI. Transportation**

A. The following paragraphs provide some additional information on the various means available for transporting classified and unclassified keying materials, other cryptographic materials, and CCI equipment.

B. The basic methods of transporting materials mentioned in this Annex have included the following:

1. Authorized/cleared Government courier services.
2. NSA-approved commercial carriers.
3. Authorized company couriers.
4. U.S. registered mail.

C. Authorized/cleared Government Courier Services

1. These are the established Government organizations dedicated to couriating materials of all types and classifications from unclassified through top secret.

2. The two primary Government courier services are the Armed Forces Courier Service (ARFCOS), and the U.S. Diplomatic Courier Service.

3. If there is any doubt about the exact status of a Government courier service, contractors should contact their COMSEC account's Central Office of Record for information.

#### D. NSA-Approved Commercial Carriers

1. Selected commercial transportation companies may be authorized by the NSA to transport specific levels of cryptographic materials, including keying material classified SECRET and below, CCI equipment, as well as unclassified keying material.

2. NSA approval of a commercial carrier to transport a particular level of classified or unclassified cryptographic material (including CCI equipment) depends on an evaluation of numerous factors, including:

- a. U.S. ownership and operation
- b. The proposed carrier's reputation and trustworthiness.
- c. The carrier's capability to impose access controls and physical security.
- d. Capability to maintain a continuous signature accountability system.
- e. Establishment of full-time carrier company contact points for couriers who may have questions or experience difficulties while transporting material.
- f. Appropriate Government security clearances and storage facilities (if classified material is involved).

#### E. Authorized Company Couriers

1. Authorization to act as a courier or escort for CCI equipment and components may be granted by the company Facility Security Supervisor to company employees who meet the access requirements for those materials (see section II.A of this Annex). These persons must be designated in writing by the Company Facility Security Supervisor and may act as a courier provided the following conditions are met:

- a. The materials are not transported outside of the United States.
- b. Time or other constraints do not permit the use of other approved means of transportation.
- c. An appropriate courier identification pass is issued to the employees. The issuing contractor must retain a record of issued courier passes and the information they contain for at least three years. Courier passes will contain the following:
  - (1) Employee's full name, social security number, and security clearance (if applicable).
  - (2) Issue date.
  - (3) Employee's signature.
  - (4) Pass expiration date (no longer than one year from the date of issue).
  - (5) Identification of contractor, with name and signature of issuing official.
- d. Transportation is begun and completed during normal daytime duty hours of the same day. If commercial air is used by the courier, the following will apply:
  - (1) The Facility Security Supervisor will ensure that the courier is briefed on proper security procedures.
  - (2) The FSS will 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 the destination.
- e. All requirements for access and the physical security of the equipment or materials can be complied with.

2. The company Facility Security Supervisor may also appoint company employees to courier SECRET or CONFIDENTIAL keying material or other cryptographic material, provided such employees meet the access requirements for these materials (see sections IV.B and V.A of this Annex), and the conditions stated in a. through e., above. Such couriers must be designated in writing by the company Facility Security Supervisor. For TOP SECRET materials, courier authorization must be obtained on a case-by-case

basis from the contracting officer or his/her representative. When transporting classified material, such couriers shall not utilize commercial passenger aircraft without the specific approval of the contracting officer or his/her representative.

## VII. Displays, Demonstrations, and Marketing

A. 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 CCI or COMSEC information.

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

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

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

a. Access to the demonstration of CCI equipment shall 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 shall also contain a Privacy Act Statement to be read and signed by the individual.\* A sample form is attached as Appendix 6 to this Annex. In addition, the individual must present identification which verifies his name and signature. Subsequent to the demonstration, but within 30 days, the vendor shall verify the information provided on citizenship, etc., with the company. Any discrepancies which are detected will be reported immediately to NSA.

b. Visual access and demonstrations of the equipment will be conducted in a room separated 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 shall be conducted at the unclassified level.

c. Vendors shall not disclose any classified characteristics of the CCI equipment, nor provide photographs, diagrams, or schematics of the inside of the equipment.

\* Appropriate Privacy Act Statement will be provided as soon as it is available.

C. Recognizing that certain information needs to be available to potential purchasers of CCI devices 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 as indicated below:

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 device (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 certified 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 by using the procedures identified in section VII.B. 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 certified/endorsed.
- j. All unclassified physical and personnel security control requirements contained in this document, its annexes and appendices.

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 Project Manager, or other specific NSA points-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.



## **APPENDIX 1 TO ANNEX D**

### **COMSEC BRIEFING**

1. This appendix contains a three-page briefing which will be read and understood by all contractor personnel before they may have access to CCI or classified cryptographic equipments, classified or unclassified keying materials, or other cryptographic materials.
2. The contractor is responsible for retaining records of the COMSEC Briefing given to each employee for at least five years from its date.
3. The briefing should be administered in connection with a review of the pertinent parts of the contractor's Standard Practice Procedures, covering local procedures for implementing the control requirements of this document.
4. Personnel who have a continuing need for access to classified cryptographic information or equipment shall also be given periodic rebriefings, at least annually. In addition to reminding personnel of their continuing responsibility for safeguarding classified cryptographic information, the rebriefing should emphasize any specific security deficiencies noted in the interval since the last briefing.
5. Personnel whose access is strictly limited to unclassified equipment, materials, and keying material only require an initial briefing.
6. Should the contractor require disposition of the briefing records prior to the expiration of the five year period (e.g., the company goes out of business), contractor security officials must contact the NSA for instructions.

#### **COMSEC Briefing**

A. You have been selected to perform duties which will require access to sensitive cryptographic equipment or materials. 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 cryptographic 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. Cryptographic materials and equipments are especially sensitive because they are used to protect other information against unauthorized access during the process of communicating information from one point to another. Any particular piece of cryptographic 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 cryptographic 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 cryptographic 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 parts: 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 part 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 cryptographic 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 cryptographic materials and equipments: "COMSEC channels" and "administrative channels." The COMSEC channel, called the COMSEC Material Control System, is used to distribute accountable cryptographic items such as keying material, maintenance manuals, and cryptographic equipments. This 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 other than that which is accountable in the COMSEC Material Control System.

1. Access to cryptographic equipment and materials is granted only to those persons who:

- a. Are U.S. citizens.
- b. Have a specific need-to-know associated with their work assignments.
- c. Have read and understand this briefing.
- d. Are familiar with local security procedures as specified in the company's Standard Practice Procedures.

2. Additionally, if the access is to be granted to classified equipment, keying material, or other cryptographic material, the person having access must possess a final Government security clearance at least equal to the classification of the material or equipment involved.

E. Particularly important to the protection of cryptographic 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 variables, 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 cryptographic equipment and materials to which you will have access.

F. Public disclosure of any COMSEC information, other than those specific cases discussed in the Government Contractor's Controlled Cryptographic Item (CCI) Manual 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 cryptographic information, and means that you may not prepare newspaper articles, speeches, technical papers, or make any other "release" of cryptographic information without specific Government approval. The best personal policy is to avoid any discussions which reveal your knowledge of or access to cryptographic 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 cryptographic equipment, keying material, or other cryptographic materials 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, section 641, 793, 794, 798, and 952.

H. If your personal exposure includes access to classified information, material or equipment, 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 should be notified sufficiently in advance so that you may receive a defensive security briefing. Any attempt to elicit the cryptographic information you have, either through friendship, favors, or coercion must be reported immediately to security.

D-1-4

**FOR OFFICIAL USE ONLY**

APPENDIX 2 TO ANNEX D

MATERIAL DESTRUCTION GUIDELINES

MATERIAL	DESTRUCTION METHOD	PARTICLE SIZE
Printed COMSEC material (Keying material, and media which embody, describe, or implement a classified cryptologic) <sup>1</sup>	Burn  Pulp <sup>2</sup> , Pulverize, Disintegrate, Chop  Crosscut Shred	White ash  5mm  3/64 x 1/2 inches (1.2mm x 13mm); OR 1/35 x 7/8 inches (0.73mm x 22.2mm)
Paper-Mylar-Paper Tape	Burn  Pulverize, Disintegrate, Chop  Crosscut Shred	White ash  5mm  1/35 x 7/8 inches <sup>3</sup> (0.73mm x 22.2mm)

<sup>1</sup> Includes all paper keying material and paper documents such as full maintenance manuals, cryptologic descriptions, drawings of cryptologic logic, specifications describing a cryptologic logic, and cryptologic software.

<sup>2</sup> High wet-strength paper (map stock) and durable-medium paper substitute (e.g., TYVEK Olefin, Polyethylene Fiber) to be destroyed by dry disintegration, shredding, or burning. DO NOT PULP.

<sup>3</sup> Intershred Model 33, Intimus 8007, Akten Model II, and Cummins Model 48 Only.

MATERIAL	DESTRUCT METHOD	PARTICLE SIZE
Secondary Variables (CRIBs, Rotors)	Peel CRIB from metal backing plate and cut CRIB. Remove rotor wiring and notch rings and cut. Durn rotors <sup>1</sup>	15mm  Crush ashes
Floppy Disks	Durn Molt (SEM MICRO-MELT desk-top unit -- 2 disks at a time) Pulverize, Disintegrate, Chop Crosscut Shred	Crush ashes -- 5mm 1/35 x 7/8 inches <sup>2</sup> (0.73mm x 22.2mm)

<sup>1</sup> Includes all paper keying material and paper documents such as full maintenance manuals, cryptologic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic software.

<sup>2</sup> High wet-strength paper (map stock) and durable-medium paper substitute (e.g., TYVEK Olefin, Polyethylene Fiber) to be destroyed by dry disintegration, shredding, or burning. DO NOT PULP.

<sup>3</sup> Intershred Model 33, Intimus 8007, Akten Model II, and Cummins Model 48 Only.

<sup>4</sup> May produce toxic gases; could be hazardous.

MATERIAL	DESTRUCT. METHOD	PARTICLE SIZE
Typewriter Ribbons	Burn, Disintegrate	5mm
Microfiche, Microfilm, Photo Negatives, and Photomasks	Chemical <sup>1</sup> (bleach for film asters; acetone or meth- elyno chloride for diazo reproductions)	Complete immersion removes information from base materiapl
	Burn	Crush ashes
	Melt (for microfiche - SEM MICRO-MELT desk-top unit -- up to 6 microfiche at a time)	--
MOS Wafers, Integrated Circuits, and Hybrid Circuits	Burn (temperature above 2800 degrees Fahrenheit required)	Crush ashes
	Pulverize	75 microns
	Chemical <sup>1,2</sup>	Complete dissolution

<sup>1</sup> Guidance available from DIRNSA, ATTN: 5232.

<sup>2</sup> Heated caustic solution or acid bath could be hazardous.

MATERIAL	RECOVERY METHOD	PARTICLE SIZE
Magnetic Tape (Digital and Analog)	Disintegrate	9mm
PROMs (Programmable Read-Only Memories): -Older grid-type PROMs -Integrated circuit PROMs	Burn (do not burn magnetic tape on aluminum reels) Chemical <sup>1</sup> (remove tape from reel) Degauss (Non-CRYPTO)	Crush ashes  --  Erasure level -90 dB <sup>2</sup> (Non-CRYPTO)
	Pulverize	125 microns
	Pulverize	75 microns

<sup>1</sup> Includes all paper keying material and paper documents such as full maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic software.

<sup>2</sup> HACSI No. 4005 (Reference DoD Manual 5200.28 or USSID 701).



MATERIAL	DESTRUCT METHOD	PARTICLE SIZE
Printed-Circuit Boards (PCBs)	Burn	Crush ashes
P-Plugs	Pulverize or chop	(Case-by-Case) <sup>1</sup>
Magnetic Cores	Disintegrator, Smelt	5mm (circuit board)
Magnetic Discs	Burn, Smelt	Crush ashes
	Grind or sand recording surface with emery wheel or sander	--
	Smelt (temperature of 1362 degrees Fahrenheit required)	--
	Degauss (Non-CRYPTO)	Erasure level -90 dB (Non-CRYPTO)

<sup>1</sup> Depends on state-of-the-art of PCBs to be destroyed. Guidance available from DIRNSA, ATTN: 5232.

<sup>2</sup> NACSI No. 4005 (Reference DoD Manual 5200.28 or USSID 701).

## **APPENDIX 3 TO ANNEX D**

### **NSA-APPROVED PAPER DESTRUCTION DEVICES**

1. This Appendix contains a list of equipments which have been tested and approved by the National Security Agency (NSA) and which when equipped as specified, meet the routine destruction standards for paper COMSEC materials.

2. Approval of a specific equipment has been based only on examination of residue and a physical security evaluation of the equipment. Such factors as reliability, rate of wear, and frequency of parts replacement have not been evaluated, and NSA does not endorse manufacturers' claims concerning these aspects. Hourly volume rates stated are estimates based on average rates for destruction of paper materials and may vary depending on variety, volume, and loading.

3. Other equipments will be added to this Annex as they are evaluated and approved. Queries or information concerning equipments not shown on the list may be addressed to the Director, NSA (DIRNSA), ATTN: S04, Fort George G. Meade, MD 20755-6000.

4. Many, though not all, of the devices listed in this Annex are available from the GSA Federal Supply Schedule.

5. Inclusion of an equipment in this Appendix does not constitute NSA or U.S. Government endorsement, or lack thereof, of commercially available products.

NSA-APPROVED PAPER DESTRUCTION DEVICES

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS./HOUR	UNIT COST <sup>1</sup>	REMARKS
<p><u>Mel Pulpers</u></p> <p>Waring 7-Speed Blender</p>	<p>Waring Products Div. Dynamics Corporation of America New Hartford, CN 06057</p>		14.95	<p>Not approved for paper-mylar-paper key tape or high wet-strength paper.</p>
<p>SOMAT Model 30 15 Pulper</p>	<p>SOMAT Corporation Box 831 Coatesville, PA 19320</p>	200		<p>Discontinued. Not approved for paper-mylar-paper key tape or high wet-strength paper. 5/16" ring hole strainer required.</p>
<p><u>Shredders</u></p> <p>Destroyit Cross Cut Shredder (Model CC AM)</p>	<p>The Michael Lith Sales Corporation 145 West 45th Street New York, NY 10036</p>	25	902.50	<p>Not approved for paper-mylar-paper key tape.</p>
<p>Shredmaster Cross Cut 200 Shredder</p>	<p>Shredmaster Corp. 1101 Skokie Boulevard Northbrook, IL 60062</p>	25	1,116.00	<p>Not approved for paper-mylar-paper key tape.</p>

<sup>1</sup> Approximate cost ns of 1981.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS/HOUR	UNIT COST	REMARKS
<u>Shredders Cont.</u>				
Intershred Model 33 Desk Top Cross Cut Shredder	Whitaker Brothers Business Machines, Inc. 5913 Georgia Ave., NW Washington, DC 20011	50	1,599.20	
Akten Model 11 Cross Cut High Security Shredder	Benchmark Security Systems, Inc. 2000 N. 16th Street Arlington, VA 22201	75	3,241.00	Identical to Intimus 8007.
Intimus 8007 Shredder (Cross Cut)	Whitaker Brothers Business Machines, Inc. 5913 Georgia Ave., NW Washington, DC 20011	75	5,439.20	
Cummins Model 48 Shredder	Cummins - Allison Co. 7900 Westpark Drive McLean, Va 22101	75	5,439.20	Identical to Intimus 8007.
Disintegrators (Knifemills)				
Security Engineered Disintegrator Model 700	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	50	2,635.00	Office model. Low noise level.

\* Approximate cost as of 1981.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS/HOUR	UNIT COST <sup>1</sup>	REMARKS
Disintegrators (Kraftmills, Cont.) Security Engineered Disintegrator Model 1	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	50		Discontinued. 3/32" filter screen required. Sound enclosure available (1,195.00).
Security Engineered Disintegrator Model 2	Security Engineered Machinery Co. 5 Walkup Street Westboro, MA 01581	100	4,135.00	3/32" filter screen required. Sound enclosure available (1,345.00).
Security Engineered Disintegrator Model 3	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	200		Discontinued. 3/32" filter screen required. High noise level.
Security Engineered Disintegrator Model 1012	Security Engineered Machinery Company 5 Walkup Drive Westboro, MA 01581	300	6,295.00	3/32" filter screen required. Sound enclosure available. (1,597.00).

<sup>1</sup> Approximate cost as of 1981.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LPS/HOUR	UNIT COST <sup>1</sup>	REMARKS
Disintegrators (Knifecrills, Cont.)	Security Engineering Machinery Co. 5 Walkup Drive Westboro, MA 01581	600	12,150.00	3/32" filter screen required. Sound enclosure available (1,777.00). Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
Security Engineering Disintegrator Model 1424	Security Engineering Machinery Co. 5 Walkup Drive Westboro, MA 01581	1000	26,865.00	3/32" filter screen required. Sound enclosure available (3,415.00). Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
Disintegrators (Hannemills)	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	50-75	3,195.00	3/16" filter screen required. Moderate noise level.

<sup>1</sup> Approximate cost as of 1981.

<sup>2</sup> Filter screen size depends on "state-of-the-art" of PCDs to be destroyed.  
Guidance available from DIRNSA, ATTN: 5232.

EQUIPMENT DESIGNATION	MANUFACTURER OR RESALEMUR	CAPACITY LBS/HOUR	UNIT COST	REMARKS
Disintegrators (Harrisville, Cont.)				
Jay-Bee Model 30H Office Disintegrator	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	75-100	3,510.00	3/16" filter screen required. Moderate noise level.
Jay-Bee Model AB Disintegrator	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	75-150		Discontinued. 3/16" filter screen Required. High noise level and some dust.
Jay-Bee Model 3CB Disintegrator	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	200	3,400.00	3/16" Filter screen required. High noise level.
Jay-Bee Model 2 15W Disintegrator	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	300	24,021.00	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>1</sup>

<sup>1</sup> Approximate cost as of 1981.

<sup>2</sup> Filter screen size depends on "state-of-the-art" of PCBs to be destroyed.  
Guidance available from DIRNSA, ATTH: 5232.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS/HOUR	UNIT COST <sup>1</sup>	REMARKS
DD5 Hammermill Model 12	Document Disintegration Systems 2075 Dolgrave Avenue Huntington Park, CA 90255	600		Discontinued. 3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
Jay-Bee Model 3 ISM Disintegrator	Jay-Bee Manufacturing Company, Inc. P.O. Box 986 Tyler, TX 75701	750	25,911.00	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
DD5 Hammermill Model DDS-18	Document Disintegration Systems 2075 Belgrave Avenue Huntington Park, CA 90225	1000	36,716.00 (Less power plant)	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>

<sup>1</sup> Approximate cost as of 1981.

<sup>2</sup> Filter screen size depends on "state-of-the-art" of PCBs to be destroyed. Guidance available from DIRNSA, ATTN: S232.



EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY RDS/HOURS	UNIT COST <sup>1</sup>	REMARKS
Disintegrators Hammermills, Cont.)  Joy-Bee Model 4 ISW Disintegrator	Joy-Bee Manufacturing Company, Inc. P.O. Box 906 Tyler, TX 75701	1500	28,836.00	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
DDS Hammermill Model DDS-24	Document Disintegration Systems 2075 Delgrave Avenue Huntington Park, CA 90255	2300	51,966.00 (Less power plant)	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>
DDS Hammermill Model DDS-36	Document Disintegration Systems 2075 Delgrave Avenue Huntington Park, CA 90255	3000	64,249.00 (Less power plant)	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen. <sup>2</sup>

<sup>1</sup> Approximate cost as of 1981.

<sup>2</sup> Filter screen size depends on "state-of-the-art" of PCBs to be destroyed.  
Guidance available from DIRISA, ATRN: 5232.

## **APPENDIX 4 TO ANNEX D**

### **REFERENCE MATERIALS**

This appendix contains copies of the pertinent portions of the following U.S. laws and Executive Orders, all of which are referred to in the Cryptographic Access Briefing:

United States Code, Title 18, Sections:

- 641
- 793
- 794
- 798
- 952

## § 641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of \$100, he shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

June 25, 1948, c. 645, 62 Stat. 725.

### Historical and Revision Notes

*Reviser's Note.* Based on Title 18, U. S.C., 1940 ed., §§ 82, 87, 100, 101 (Mar. 4, 1909, c. 321, §§ 32, 33, 47, 48, 35 Stat. 1093, 1096-1098; Oct. 23, 1918, c. 194, 40 Stat. 1015; June 18, 1934, c. 587, 48 Stat. 906; Apr. 4, 1938, c. 60, 52 Stat. 197; Nov. 22, 1943, c. 302, 57 Stat. 591).

Section consolidates sections 82, 87, 100, and 101 of Title 18, U.S.C., 1940 ed. Changes necessary to effect the consolidation were made. Words "or shall willfully injure or commit any depredation against" were taken from said section 82 so as to confine it to embezzlement or theft.

The quoted language, rephrased in the present tense, appears in section 1351 of this title.

Words "in a jail" which followed "[imprisonment]" and preceded "for not more than one year" in said section 82, were omitted. (See reviser's note under section 1 of this title.)

Language relating to receiving stolen property is from said section 101.

Words "or aid in concealing" were omitted as unnecessary in view of definitive section 2 of this title. Procedural language at end of said section 101 "and such person may be tried either before or after the conviction of the principal offender" was transferred to and rephrased in section 3433 of this title.

Words "or any corporation in which the United States of America is a stockholder" in said section 82 were omitted as unnecessary in view of definition of "agency" in section 6 of this title.

The provisions for fine of not more than \$1,000 or imprisonment of not more than 1 year for an offense involving \$100 or less and for fine of not more than \$10,000 or imprisonment of not more than 10 years, or both, for an offense involving a greater amount were written into this section as more in conformity with the later congressional policy, expressed in sections 82 and 87 of Title 18, U.S.C., 1940 ed., than the nongraduated penalties of sections 100 and 101 of said Title 18.

Since the purchasing power of the dollar is less than it was when \$50 was the figure which determined whether larceny was petit larceny or grand larceny, the sum \$100 was substituted as more consistent with modern values.

The meaning of "value" in the last paragraph of the revised section is written to conform with that provided in section 2311 of this title by inserting the words "face, par, or".

This section incorporates the recommendation of Paul W. Hyatt, president, board of commissioners of the Idaho State Bar Association, that sections 82 and 100 of Title 18, U.S.C., 1940 ed., be combined and simplified.

Also, with respect to section 101 of Title 18, U.S.C. 1940 ed., this section meets the suggestion of P. F. Herrick, United States attorney for Puerto Rico, that the punishment provision of said section be amended to make the offense a misdemeanor where the amount involved is \$50 or less.

Changes were made in phraseology.

**§ 793. Gathering, transmitting, or losing defense information**

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in process of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative,

blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. 645, 62 Stat. 736; Sept. 23, 1950, c. 1024, Title I, § 18, 64 Stat. 1003.

#### Historical and Revision Notes

**Reviser's Note.** Based on sections 31 and 38 of Title 50, U.S.C., 1940 ed., War and National Defense (June 13, 1917, c. 30, Title I, § 1, 6, 40 Stat. 217, 219; Mar. 29, 1940, c. 72, § 1, 54 Stat. 79).

Section consolidated sections 31 and 38 of Title 50, U.S.C., 1940 ed., War and National Defense.

Words "departments or agencies" were inserted twice in conformity with definitive section 6 of this title to eliminate any possible ambiguity as to scope of section.

The words "or induces or aids another" were omitted wherever occurring as unnecessary in view of definition of "principal" in section 2 of this title.

Mandatory punishment provision was rephrased in the alternative.

Minor changes were made in phraseology.

**1950 Amendment.** Act Sept. 23, 1950 divided section into subdivisions, added laboratories and stations and places where material or instruments for use in

time of war are the subject of research or development to the list of facilities and places to which subsec. (a) applies, made subsec. (d) applicable only in cases in which possession, access, or control is lawful, added subsec. (e) to take care of cases in which possession, access, or control is unlawful, made subsec. (f) applicable to instruments and appliances, as well as to documents, records, etc., and provided by subsec. (g) a separate penalty for conspiracy to violate any provisions of this section.

**Indictment for Violating This Section: Limitation Period.** Limitation period in connection with indictments for violating this section, see note under section 702 of this title.

**Canal Zone.** Applicability of section to Canal Zone, see section 14 of this title.

**Legislative History.** For legislative history and purpose of Act Sept. 23, 1950, see 1950 U.S. Code Cong. Service, p. 3880.

**§ 794. Gathering or delivering defense information to aid foreign government**

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. 645, 62 Stat. 737; Sept. 3, 1954, c. 1261, Title II, § 201, 68 Stat. 1219.

**Historical and Revision Notes**

**Reviser's Note.** Based on sections 32 and 34 of Title 50, U.S.C., 1940 ed., War and National Defense (June 15, 1917, c. 30, Title I, §§ 2, 4, 40 Stat. 214, 219).

Section consolidates sections 32 and 34 of Title 50, U.S.C., 1940 ed., War and National Defense.

The words "or induces or aids another" were omitted as unnecessary in view of definition of "principal" in section 2 of this title.

The conspiracy provision of said section 34 was also incorporated in section 2383 of this title.

Minor changes were made in phraseology.

**1954 Amendment.** Act Sept. 3, 1954 increased the penalty for peacetime espionage and corrected a deficiency in the sentencing authority by increasing penalty to death or imprisonment for any term of years.

**Temporary Extension of Section.** Temporary extension of section, see section 784 of this title.

Section 7 of Act June 30, 1953, c. 175, 67 Stat. 173, repealed Joint Res. July 3, 1952, c. 370, § 1(a)(29), 66 Stat. 333, Joint Res.

Mar. 31, 1953, c. 13, § 1, 67 Stat. 18, which had provided that this section should continue in force until six months after the termination of the national emergency proclaimed by 1950 Proc. No. 2914, which is set out as a note preceding section 1 of Appendix to Title 50, War and National Defense.

Section 6 of Joint Res. July 3, 1952, repealed Joint Res. Apr. 14, 1952, c. 204, 66 Stat. 54, as amended by Joint Res. May 28, 1952, c. 329, 66 Stat. 96. Intermediate extensions by Joint Res. June 14, 1952, c. 457, 66 Stat. 137, and Joint Res. June 30, 1952, c. 526, 66 Stat. 296, which continued provisions until July 3, 1952, expired by their own terms.

**Indictment for Violating This Section; Limitation Period.** Limitation period in connection with indictments for violating this section, see note under section 792 of this title.

**Canal Zone.** Applicability of section to Canal Zone, see section 14 of this title.

**Legislative History.** For legislative history and purpose of Act Sept. 3, 1954, see 1954 U.S. Code Cong. and Adm. News, p. 7133.

**§ 798. Disclosure of Classified Information**

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Added Oct. 31, 1951, c. 655, § 24(a), 65 Stat. 719.

<sup>1</sup>As enacted. See second section 796 enacted on June 30, 1952 set out below.

#### Historical Note

Canal Zone. Applicability of section to Legislative History. For legislative history and purpose of Act Oct. 31, 1951, see 1951 U.S. Code Cong. and Adm. News, p. 2578.



## § 952. Diplomatic codes and correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both. June 25, 1948, c. 645, 62 Stat. 743.

### Historical and Revision Notes

**Reviser's Note.** Based on section 135 of Title 22, U.S.C., 1940 ed., Foreign Relations and Intercourse (June 10, 1933, c. 57, 48 Stat. 122). Minor changes of phraseology were made.

### Cross References

Classified information, disclosure by government official, penalty for, see section 783 of Title 50, War and National Defense.  
Classified information, disclosure of, see section 798 of this title.

### Library References

United States ~~62~~

C.J.S. United States §§ 60, 61.

## APPENDIX 5 TO ANNEX D

### FACILITY STANDARD PRACTICE PROCEDURE

1. The purpose of this Appendix is to provide guidance on the security items related to COMSEC which should be considered in implementing a facility Standard Practice Procedure (SPP).

a. For those facilities holding classified information or equipment, the Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M) requires contractors to implement a written SPP in sufficient detail to place into effect all required Government security controls. The COMSEC Supplement to the Industrial Security Manual further requires that contractors include procedures in or prepare a supplement to the SPP which adequately addresses all COMSEC requirements.

b. For those facilities holding only unclassified information and equipment (e.g., CCI equipment), there is no requirement for establishing an SPP external to this Manual.

c. In either case, however, an SPP will be implemented which adequately covers COMSEC requirements for that particular facility. The purpose of the COMSEC portions or supplements to the SPP is to translate the requirements of this Manual into language directly applicable to a contractor's facility, clearly understandable to its employees.

2. Although not every item applies in every case, the following points should be considered for inclusion into the COMSEC portions of a contractor's SPP. Each item is followed (where appropriate) by a reference, in parenthesis, to its location in the CCI Manual.

a. Identification and location of the contractor's office responsible for implementation of the SPP.

b. Identification and location of whom to contact for any questions concerning COMSEC requirements.

c. Requirements for access to spaces containing cryptographic materials or equipment (Annex D). Address access by employees, escorted and unescorted visitors, and emergency personnel.

d. Identity of the COMSEC Account and Custodian serving the facility.

- e. Responsibilities of the COMSEC Custodian, Alternate Custodian, and Facility Security Supervisor (Annex B).
- f. Accounting requirements and procedures for CCI equipment. (Annex C)
- g. Local procedures covering the removal, transfer, maintenance and repair of CCI equipment (Annexes C and D).
- h. Identification of the person authorized to key and rekey cryptographic devices. (Annex D)
- i. Identification of the person responsible for inspections of Protected Distribution Systems. (Annex D)
- j. Local procedures for the disposition (destruction, sale, return to Government, etc.) of CCI equipment. (Annex D)
- k. Use and storage of key fill devices. (Annex D)
- l. Procedures for keying and re-keying cryptographic equipments. (Annex D and I)
- m. Procedures for the storage and disposition of keying materials. (Annex D)
- n. Procedures for the use, storage, and disposition of other cryptographic documents and materials. (Annex D)
- o. Procedures for determining if someone has been granted access to keying materials, equipment, and other materials. (Annex D)
- p. List of reportable COMSEC insecurities. (Annex B)
- q. Local procedures for reporting actual or potential COMSEC insecurities (to whom to report, location or office receiving reports, etc.). (Annex G)
- r. Local procedures and restrictions on equipment modifications and changes to certified system configurations. (Annex H)
- s. Procedures and requirements unique to specific cryptographic equipments. (Annex I).

**APPENDIX 6 TO ANNEX D**  
**COMPANY INFORMATION FORM**

Please provide the following information and present identification that verifies your name, company affiliation, and signature.

**NAME** \_\_\_\_\_  
(Please Print)

**SIGNATURE** \_\_\_\_\_

**CITIZENSHIP** \_\_\_\_\_

**SOCIAL SECURITY NUMBER** \_\_\_\_\_

**COMPANY AFFILIATION** \_\_\_\_\_

**POSITION** \_\_\_\_\_

**BUSINESS TELEPHONE** \_\_\_\_\_

## ANNEX F

### KEYING MATERIAL MANAGEMENT

#### I. INTRODUCTION

##### A. Purpose:

1. The purpose of this Annex is to address the subject of keying material management in general terms which are applicable to all cryptographic networks.

2. Specific topics covered in this Annex include the following:

a. The responsibilities of a "controlling authority" for keying material.

b. Guidance and procedures in the selection and designation of a controlling authority.

c. The basic steps and concepts involved in the establishment of a cryptographic network, or cryptonet.

d. The procedures for acquiring keying materials.

e. The Keying Material Support Plan (KMSP), which is prepared by the controlling authority.

f. Procedures for the periodic review of keying materials by the controlling authority (for adequacy and quantitative requirements forecasting).

##### B. General:

1. This Annex only addresses what is termed "hard-copy" key, i.e., physical keying material such as printed key lists, punched key tape, punched key cards, etc. "Soft" key in electronic form is often employed in newer cryptographic equipments for key updating and similar functions, but is addressed in the operating instructions for the particular equipments which use it, or is covered under Annex I for a particular cryptographic system (e.g., Appendix 1 to Annex I on the KY-71A Secure Telephone Unit).

2. Some basic concepts:

a. A "cryptonet" is a telecommunications network in which information is protected by the use of cryptographic equipments which are keyed with a common key. Although there are many possible types of cryptonets, the important point is that for multiple parties to communicate securely with each other, each member of the net must be using the same key, and the same (or cryptographically compatible) cryptographic equipments. This rule applies whether the "net" consists of two parties in a point-to-point arrangement, or numerous parties in a common net.

b. The hardcopy keying materials come in many forms, but each is designated by a long title (e.g., KG-13 operation key card), and a short title (e.g., USKAY-216). Normally, only the short title is printed on the keying material. Each short title is further identified by "edition," usually designated by letters, which indicates a particular set of cryptovariabes. For cryptographic equipments to operate successfully with each other, therefore, they must be keyed with keying material bearing the same short title and edition. For the purposes of accounting, each piece of keying material is further identified by a unique copy number or similarly unique identification.

c. Each edition has a cryptoperiod, which is scheduled replacement of one edition by another. Supersession rates vary from system to system, e.g., weekly, monthly, quarterly, and yearly. Each edition contains a set of keys (e.g., tape segments) which are assigned a cryptoperiod. Cryptoperiods may cover virtually any period of time, from minutes to months, but usually are daily, weekly or monthly.

d. To establish and maintain order, to supervise cryptographic logistics, and to evaluate and respond to security issues affecting a cryptonet, an organization is designated as the "controlling authority" for each cryptonet. Because a cryptonet is defined by the cryptographic materials it uses, controlling authorities are in practice designated for each short title of cryptographic keying material. The controlling authority's responsibilities are detailed below.

C. Designation of the controlling authority:

1. Controlling authorities should be designated primarily on the basis of their ability to perform their responsibilities. The controlling authority, therefore:

- a. Is a member of the cryptonet.
- b. Has some seniority or authority over the other members of the cryptonet.

c. Has 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).

d. Is in a position to monitor the status of the cryptonet, i.e., to identify problems, or receive adequate information about net problems.

2. Controlling authorities may be Government or contractor organizations, regardless of the make-up of the net membership. The most important point in the selection of a controlling authority is that it is fully able to carry out its many responsibilities.

3. When a new cryptonet is established, the authorized COMSEC vendor who provides the cryptographic equipment is required to offer assistance in the preparation of the Keying Material Support Plan (KMSP), which necessarily involves designation of the controlling authority. (NOTE: The level of assistance offered is at the discretion of the vendor - the basic requirement is for the vendor to inform the purchaser of the essentials of key management, that a Keying Material Support Plan will be required, and what it must contain). The contractor who purchases the cryptographic equipment may work with the vendor, with his Government contracting officer(s), or with the National Security Agency (Y1) in proposing a controlling authority for the new cryptonet. If multiple Government contracting officers are involved with a particular cryptonet, the contractor should coordinate with each of them in the designation of the controlling authority.

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 DIRNSA (Y1).

c. It is the purchasing contractor's responsibility to ensure that a controlling authority designation proposal is made to DIRNSA 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 DIRNSA (Y1).

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

4. For existing cryptonets which are significantly modified or expanded by the addition of new members, the current controlling authority must re-validate his role. This should be accomplished through existing Department and Agency regulations and procedures, if applicable, or directly to DIRNSA (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.

5. 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 DIRNSA (Y1).

## II. RESPONSIBILITIES OF A CONTROLLING AUTHORITY

A. The controlling authority for a cryptonet has responsibilities which fall into three broad categories: cryptonet management, logistics, and security. Additional guidance concerning the security responsibilities of the controlling authority are found in Annex G and Appendix in 1 to Annex G.

B. The responsibilities of the controlling authority include:

1. Cryptonet management:

a. Establishing a cryptonet by designating cryptonet members.

b. 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.

c. Specifying the key change time for the cryptonet.

d. 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.

e. Reporting to DIRNSA (Y1 and S042) incidents of faulty keying material or the unauthorized transmission of keying information.



f. 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).

g. Ensuring that prescribed allowances of on-hand keying materials at cryptonet member locations are adequate for potential emergency supersessions.

h. Initiating the conducting of an annual review 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 (KMSP) described in section IV of this Annex.

2. Logistics:

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

b. Notifying DIRNSA (Y1) of any changes in the effective dates of times of cryptonet keying material.

3. Security (see also Annex G: Insecurity Reporting):

a. 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.

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

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

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

e. 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 DIRNSA (S21) of this action.

### III. CONSIDERATIONS IN ESTABLISHING A CRYPTONET

A. 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.

B. Some of the specific items to consider in establishing a cryptonet include the following:

1. The effective dates and 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 several time zones, is helpful in picking an optimum key change date and time.

2. Cryptonets, for security reasons, should be kept as small as possible. A goal should be to limit the number of people who have access to any given edition of keying material at any one time.

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

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

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

6. Operational interoperability requirements may dictate cryptographic netting and sub-netting schemes.

7. 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.

8. The Keying Material Support Plan should be filed with DIRNSA (Y1) to allow adequate lead time for the production and distribution of the right amounts of keying material. For planning purposes, a minimum of 90 to 120 days is required from the time DIRNSA receives an order for keying material until it is produced and shipped from NSA headquarters.

9. Cryptoperiods should be determined after considering the type of keying material, cryptonet size, established doctrinal limits on cryptoperiod, sensitivity and classification of information being communicated, and any cryptonet operational constraints. In nearly every case, however, a given type of keying material will have a standard cryptoperiod associated with it.

#### **IV. KEYING MATERIAL SUPPORT PLAN (KMSP)**

A. The cryptonet controlling authority is responsible for preparing a comprehensive Keying Material Support Plan (KMSP) which will be submitted to DIRNSA (Y1) for review and approval. Authorized COMSEC Vendors are required under their Memorandum of Agreement with NSA to offer assistance in the preparation of the KMSP, although as controlling authority for a cryptonet, he may prepare the KMSP himself, use the COMSEC vendor's services, or seek assistance from the Government through his lead contracting officer. If a Government entity is the controlling authority, it will prepare the KMSP in accordance with its department or agency procedures.

B. The Keying Material Support Plan will be submitted to DIRNSA (Y1) for review and approval as follows:

1. 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 office. The contracting office will forward the KMSP via department or agency channels, or, if appropriate, directly to DIRNSA (Y1).

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

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

#### **C. Contents of the Keying Material Support Plan**

1. The KMSP must contain adequately detailed information about the cryptonet so that DIRNSA 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 the DIRNSA 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.

2. The following are the specific topics which must be addressed in a Keying Material Support Plan:

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 sub-netting.

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) Keying material format (e.g., standard hole tape, key list, punched key card, etc.) where there is an option.

3) Use of keying material: operational; maintenance; training.

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

5) Date required initial operational capability.

6) Classification (or specify UNCLASSIFIED).

f. **The Distribution Plan:** Description of which keying materials are 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 keying materials in bulk shipments from DIRNSA, and identify any sub-accounts which are not going to be serviced by their primary accounts (and which will therefore require direct service from DIRNSA). The distribution plan must also address how the keying materials will be distributed from the COMSEC accounts to the actual users.

g. Proposed Carriers: Identity of which material will be shipped by which carrier (e.g, ARFCOS, particular authorized commercial carriers, etc.)

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

D. Annual Reviews of Keying Material:

1. The controlling authority is required to review the adequacy and currency of the Keying Material Support Plan (KMSP) annually, and provide any changes in writing to DIRNSA (Attention 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.

2. 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, book-keeping, etc.)

1) User level inventories should generally not exceed four months' total supply, including effective material.

2) A minimum of one back-up edition of keying material must be held at the user level COMSEC account regardless of the normal cryptoperiod length.

e. Any planned changes or cancellations of requirements.

## **ANNEX G**

### **INSECURITY REPORTING**

#### **I. GENERAL**

A. Insecurities which involve cryptographic equipments, keying material, and related materials, may have severely adverse effects on the security of the information which is being protected by the cryptographic system. In particular, if an insecurity exists which remains undetected or unreported, its damage may be multiplied by users of the cryptographic system who believe that their communications are still secure. It is of paramount importance, therefore, that all insecurities to COMSEC equipment and materials be promptly reported so that any information losses can be minimized.

B. Because electronic information processing systems are capable of handling large amounts of sensitive information in short periods, it is essential that insecurities be reported as promptly as possible. The immediate reporting of any incident which may have subjected cryptographic equipment or materials to compromise is critical to the continued integrity of the information. In almost all cases, timely reporting of insecurities will minimize the impact of the loss of sensitive information. The longer the delay in reporting incidents of security interest, the more difficult it becomes to determine and minimize the impacts on national security.

C. Because one item of keying material or one element of a cryptographic system, may be the critical element protecting very sensitive information, or large amounts of sensitive information, it is imperative that all insecurities be reported. When in doubt, report it.

D. All personnel with access to cryptographic equipment and materials are personally responsible for ensuring that insecurities involving these things are reported. Reports will normally be made first to the local person in charge of security for the equipment or material in question. At cleared facilities handling classified information, this will usually be the Facility Security Supervisor. At contractor facilities not processing classified information, this would be the person designated in the Standard Practice Procedure (SPP) document as responsible for security. Should there be any confusion, insecurities involving cryptographic equipment or materials may always be first reported to the local COMSEC Account Custodian or his

Alternate. Every contractor holding CCI equipment, or classified or unclassified cryptographic materials must have a clearly identified office or person designated as responsible for locally processing insecurity reports, and for reporting insecurities to Government authorities in accordance with this Annex.

E. It is important that all personnel understand that the purpose of reporting insecurities involving cryptographic equipment and materials is NOT to discipline, punish, or prosecute those who may be responsible for the insecurity. On the contrary, it is the Government's policy that Government and contractor personnel will NOT be disciplined, punished, or prosecuted for honest security mistakes, oversights, etc. The requirement for insecurity reporting exists so that appropriate measures can be taken in a timely manner to reduce or eliminate the compromise of sensitive national security information. It is the Government's policy that disciplinary actions be taken against individuals only in cases of gross negligence or willful and deliberate violations of security requirements which jeopardize the security of cryptographic equipment or materials.

F. Contractors holding classified keying materials, classified cryptographic equipment or other cryptographic materials, CCI equipment, or unclassified keying materials must have a local security education program which includes information on local responsibilities for reporting insecurities in accordance with this Annex.

## II. REPORTABLE COMSEC INSECURITIES

There are three broad categories of reportable COMSEC insecurities: cryptographic, personnel, and physical. Representative examples of each are described in the following paragraphs. It is important to note that particular cryptographic equipments or keying materials may have unique requirements for insecurity reporting. Where such system-unique requirements exist, they are listed in Annex I, or in the system or keying material handling instructions supplied with the item.

### A. Cryptographic Insecurities:

1. The use of keying material which is compromised, superseded, defective, previously used and not authorized for reuse, or in any way incorrect for the cryptoperiod or application for which it is used, is prohibited. For example:

- a. Unauthorized use of any key for other than its intended purpose.
- b. Use of keying material which was locally produced without the authorization of Director, National Security Agency (DIRNSA).

2. Use of cryptosystem operating or maintenance practices which are not approved by DIRNSA, e.g.:

a. Operational use of cryptographic equipment without completion of required alarm-check tests, or after the failure of an alarm-check test.

b. Maintenance of a cryptographic equipment by unqualified personnel.

3. Operational use of cryptographic equipment having defective cryptographic logic circuitry.

4. Discussion via non-secure communications of the details of any cryptographic equipment failures or malfunctions.

5. Any tampering or unauthorized modification of a cryptographic equipment, key, or other materials.

6. Compromising emanations from a cryptographic equipment or system.

7. Any other occurrence which may have resulted in a cryptographic insecurity.

B. Personnel Insecurities:

Actions and circumstances involving persons with access to cryptographic equipment and materials which have jeopardized, or could jeopardize, the security of cryptographic equipment and materials. Examples of such action and circumstances include the following:

1. Known or suspected defection, espionage, treason, sabotage, or capture by hostile parties.

2. Any attempts at subverting personnel to commit espionage, sabotage, treason or to violate security procedures.

3. Theft or loss of cryptographic equipment, key, or related materials.

4. Deliberate falsification of COMSEC records.

5. Unauthorized disclosure of cryptographic information, or the transfer of cryptographic equipment or materials to unauthorized persons.



6. Any other personnel matter which may adversely affect the security of cryptographic equipment and materials.

### C. Physical Insecurities

Occurrences which adversely affect the physical security and access protection which is provided to cryptographic equipment and materials. Examples of reportable physical insecurities include the following:

1. The physical loss of cryptographic equipment or materials, including portions or parts thereof (e.g., a CCI equipment component, or a page from an accountable cryptographic maintenance manual).
2. The discovery of cryptographic equipment or materials outside their required accountability and physical controls, e.g.:
  - a. Cryptographic material or equipment listed on a destruction report, but not actually destroyed.
  - b. Cryptographic equipment or material left unsecured or unattended where unauthorized persons could have access.
3. The discovery of cryptographic equipment or materials which are improperly packaged, shipped, or destroyed, e.g.:
  - a. Cryptographic equipment or materials which are received in a package which has been damaged or which shows evidence of tampering.
  - b. Destruction of cryptographic materials by other than the authorized means by authorized personnel.
  - c. Cryptographic materials which have not been completely destroyed, but were left unattended.
4. Unauthorized access to cryptographic equipment, keying material, or other cryptographic materials.
5. Unauthorized copying, reproducing, or photographing of cryptographic equipment or materials.
6. Discovery of a clandestine intercept or recording device in or near an area which contains cryptographic equipment or information.
7. Any other incident which jeopardized or may jeopardize the security of cryptographic equipment or materials.

### III. BASIC REQUIREMENTS FOR REPORTING INSECURITIES

#### A. To whom to report

##### 1. Classified Keying Materials

a. All cryptographic, personnel and physical insecurity reports involving classified keying materials will be reported:

(1) For action to the Controlling Authority designated for the keying material (see Annex F for description of Controlling Authorities).

(2) For information to:

(a) The Government contracting officer.

(b) The Defense Industrial Security Program's cognizant security office.

(c) DIRNSA (Attention: S21)

(d) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency (if such an entity exists).

-- Some civil departments and agencies have COMSEC insecurity monitoring activities. When they do exist, their identities and addresses may be obtained from the contracting officer.

-- The military service insecurity monitoring activities are as follows:

U.S. Army: DCDRINSCOM FT MEADE MD//IAOPS-OP-OS//

U.S. Air Force: AFCSC KELLY AFB TX//EPX//

U.S. Navy, Marine Corps, and Coast Guard:

For cryptographic insecurities:

COMNAVSECGRU WASHINGTON DC

For personnel and physical insecurities:

DCMS WASHINGTON DC

(e) If the keying material is accountable under the COMSEC Material Control System (CMCS), then the material's Central Office of Record (COR) must also be included as an information addressee (see Annex C).

(3) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency (see paragraph III.A.1.a.(2).(d) above).

b. If an insecurity incident occurs at a controlling authority, and/or involved multiple controlling authorities, DIRNSA will perform the evaluation of the incident. In this case, insecurity reports will be addressed to DIRNSA (Attention: S21) for action, with information copies sent to:

- (1) Each controlling authority for the keying material involved.
- (2) The Government's contracting officer(s).
- (3) The Defense Industrial Security Program's cognizant security office.
- (4) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency.

c. If an insecurity incident involves keying material which is related to the information of multiple Government contracting offices, each Government contracting office will be included as an information addressee on the insecurity reports for that incident.

d. Controlling authorities will normally evaluate insecurities involving keying material. This means that the controlling authority has the primary responsibility for determining if a compromise has occurred, for taking corrective action (e.g., emergency supersession of a particular keying material edition), and for ensuring that all parties who need to be aware of the insecurity are properly informed.

(1) When evaluating insecurities, controlling authorities will follow the guidance contained in Appendix 1 to this Annex.

(2) Controlling authorities will submit reports on their evaluations of insecurity incidents involving classified keying materials in accordance with section IV below, addressed to DIRNSA (Attention S21) for action, with information copies to all parties addressed by the initial insecurity report, and (if not already covered), to:

(a) The Defense Industrial Security Program's cognizant security office.

(b) The Government contraction officer(s).

(c) The COMSEC insecurity monitoring activity for the contractor-user's sponsoring Government department or agency.

2. Classified cryptographic equipment or other COMSEC materials:

a. All cryptographic, personnel, and physical insecurity reports involving classified cryptographic equipment or other COMSEC materials will be reported:

1) For action to DIRNSA (Attention: S21).

2) For information to:

a) The Government contracting officer(s).

b) The Defense Industrial Security Program's cognizant security office.

c) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency (where such an entity exists).

d) If the equipment or materials are accountable under the COMSEC Material Control System (CMCS), then the item's Central Office of Record (COR) must also be included as an information addressee.

b. If the security of any particular cryptonet is involved, the appropriate controlling authority(ies) will be added to the information addressees above.

c. If an insecurity incident involves classified equipment or other COMSEC materials which relate to the sensitive information of multiple Government contracting offices, each Government contracting office will be included as an information addressee on the insecurity reports for that incident.

d. DIRNSA will evaluate all insecurity incidents involving classified cryptographic equipment or other classified materials.

3. Controlled Cryptographic Items (CCI) Equipment:

a. All cryptographic, personnel, and physical insecurity reports involving Controlled Cryptographic Item (CCI) equipment will be reported:

(1) For action to DIRNSA (Attention S21)

(2) For information to:

(a) The Government contracting officer(s).

(b) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency (where such an entity exists).

(c) The COMSEC Material Control System (CMCS) Central Office of Record (COR) for the CCI equipment involved.

b. If the security of any particular cryptonet is involved, the appropriate controlling authority(ies) will be added to the information addressees above.

c. If the insecurity incident involves CCI equipment relating to the sensitive information of multiple Government contracting offices, each Government contracting office will be included as an information addressee on the insecurity reports for that incident.

d. DIRNSA will evaluate all insecurity incidents involving CCI equipments.

e. If the insecurity incident involves a fill device loaded with classified key, or a CCI equipment which contains a classified key, the insecurity report will be addressed as follows:

(1) For action to DIRNSA (Attention: S21)

(b) The appropriate controlling authority or authorities.

(2) For information to:

(a) The appropriate Government contracting officer(s).

(b) The Defense Industrial Security Program's cognizant security office.

(c) The COMSEC insecurity monitoring activity for the contractor's sponsoring Government department or agency (where such an entity exists).

(d) The COMSEC Material Control System (CMCS) Central Office of Record (COR) for both the CCI equipment(s) and the keying material(s) involved.

#### 4. Unclassified Keying Materials for CCI Equipments

a. All cryptographic, personnel, and physical insecurity reports involving unclassified keying materials for CCI equipment will be reported to the local COMSEC official identified as responsible for COMSEC insecurity reporting in the Standard Practice Procedure document. This will normally be the Facility Security Supervisor for contractors with classified contracts, or the local COMSEC custodian.

b. The person locally responsible for COMSEC security will evaluate the actual or potential impact of the insecurity, evaluate what actually happened, and take appropriate corrective actions.

c. If it is locally determined that a compromise of the keying material is possible or probable, a report of the insecurity will be made to the appropriate controlling authority(ies).

d. If there is any evidence or suspicion of sabotage, tampering, or espionage involving unclassified keying materials, insecurity reports will be made as follows:

(1) For action to DIRNSA (Attention S21).

(2) For information to the appropriate controlling authority(ies).

e. DIRNSA will evaluate all insecurity incidents involving suspected or actual sabotage, tampering, or espionage related to unclassified keying materials.

#### 5. Unclassified Related Cryptographic Materials:

a. Insecurities involving unclassified related cryptographic materials such as operating instructions, troubleshooting manuals, etc., will be handled locally in the same way that unclassified keying materials are handled, i.e., they will be locally reported, evaluated, and corrected.

b. If there is any evidence or suspicion of sabotage, tampering, or espionage involving unclassified related cryptographic materials, however, insecurity reports will be addressed to DIRNSA (Attention S21).

B. Classification and Security for Insecurity Reports:

1. Insecurity reports will be handled and, if appropriate, classified according to their content.

a. Classified insecurity reports will be sent via secure electrical means.

b. Contractors not holding any classified materials will limit distribution to those with a clear need-to-know.

c. It has not proven effective to establish detailed "rules" concerning the classification and protection of insecurity reports, as common sense must prevail. Some insecurity reports are obviously more sensitive than others. For example, insecurity reports involving the following should be provided adequate protection and limited distribution:

(1) Tampering, sabotage, defection or espionage.

(2) Sensitive information concerning personnel.

(3) Insecurities (e.g., cryptographic insecurities) which, if known to a hostile party, would be more likely to be exploited.

(4) Attempts at subversion

(5) Theft of CCI equipment or keying material

(6) Compromising emanations from a cryptographic equipment or system.

(7) Deliberate falsification of COMSEC records.

C. Timeliness of Reports

1. Insecurity reports should be made as soon as possible after the insecurity is detected and the necessary information gathered for an initial report.

2. As with classification and protection of insecurity reports, common sense and good judgment provide the best guides. Particular points to consider include:

a. The potential impact of the insecurity on currently effective and future keying material, i.e., the timeliness requirements for corrective actions such as superseding or bypassing selected editions.

b. The need for quick action in response to cases of sabotage, subversion, espionage, tampering, etc.

#### IV. TYPES OF INSECURITY REPORTS

A. From the point of view of the total insecurity reporting system, there are two basic types of reports:

1. Insecurity Reports: Those that initially report an insecurity, or follow up on an initial report, either directly to DIRNSA (S21), or, if keying material is in any way involved, to the appropriate controlling authority.

2. Evaluation Reports: Those that report on the evaluation of the insecurity, noting actions taken, corrections implemented, etc. These reports include those made by controlling authorities to DIRNSA and other Government entities when classified keying material is involved.

B. Insecurity Reports:

1. All initial reports of cryptographic, personnel, and physical insecurities should contain at least the following information:

a. Identification of the nature of the incident as a "COMSEC insecurity."

b. Any appropriate references (e.g., previously forwarded or related correspondence).

c. Complete identification of the materials involved (e.g., type of equipment, serial numbers, short titles, editions, copy numbers, ownership, quantities, etc.)

d. Identification (name, SSN, rank/grade, position, security clearance, cryptographic access status, etc.) of all personnel involved with the insecurity incident, to include:

(1) The reporting organization's point-of-contact (POC) for the incident.



(2) Personnel who committed, or were otherwise responsible for the insecurity.

(3) Personnel who discovered the insecurity.

(4) Any other persons who may be involved in any significant way.

e. Location of the incident, to include (as appropriate) geographical location, organizational name and address, unit identification codes, and COMSEC account numbers.

f. Circumstances surrounding the incident. The report should provide (if appropriate) 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 should include all relevant dates, times, places, including, as appropriate, the "who, what, when, where and why" of the insecurity. If sabotage, espionage, subversion, capture or defection are suspected or involved, identify as completely as possible the classified and cryptographic material to which the individual involved had access.

g. Local assessment of the possibility of unauthorized disclosure, compromise, theft, etc. Identify the person making the assessment by name and position. Assessments will be made as "compromise, (theft, unauthorized access, etc.) considered:

(1) Impossible"

(2) Improbable"

(3) Possible"

(4) Probable"

(5) Certain"

h. Local corrective actions taken or planned to limit the damage done, or to prevent a recurrence.

i. Any additional information deemed significant.

2. At least one report is required for each COMSEC insecurity which is detected. Later amplifying reports should be issued (referencing earlier reports) if circumstances change, new information is developed, etc. Contractors should be aware that additional information may be required in the process of evaluating reported insecurities, and will be requested by the organization charged with evaluating the incident.

### C. Evaluation Reports

1. Evaluation reports may be issued in a variety of forms. In general, however, they accomplish the following:

a. They summarize the nature and circumstances of the insecurity which was reported.

b. They make an assessment of the probability of compromise (or loss, theft, defection, etc.).

c. If necessary, they direct actions designed to limit the damage done, and to recover from the insecurity (e.g., emergency keying material supersession, skipping future editions, etc.).

2. When insecurities involving keying material are reported to a controlling authority, the controlling authority will perform the evaluation in accordance with the guidance contained in Appendix 1 to this Annex. It is the responsibility of the controlling authority, in such cases, to take or direct any necessary actions (e.g., extension of cryptoperiod, replacement of keying material), and to inform DIRNSA (S21) of the actions taken. Although an evaluation report will be addressed as action to DIRNSA (see paragraph III.A.1.d), it is the controlling authority's responsibility to take timely action, and to determine what coordination must be done (e.g., for resupply of keying material), or what further actions should be performed by DIRNSA, other Government organizations, or cryptonet members.

## APPENDIX 1 TO ANNEX G

### 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 their 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 DIRNSA 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 could have had access to must be inventoried.

e. If a controlling authority experiences difficulty in evaluating certain cryptographic insecurities of a technical nature, or any other difficulty in making an evaluation, assistance may be obtained from DIRNSA (Attention: 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 of spare key settings or 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 DIRNSA (Attention: 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 DIRNSA (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 specific 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 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, 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 DIRNSA 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 DIRNSA, Attention: S21 and Y1).

## **ANNEX H**

### **SYSTEM CERTIFICATION AND CONFIGURATION CONTROL**

#### **I. INTRODUCTION**

##### **A. General**

1. All applications of CCI equipment shall comply with the minimum applicable physical security and TEMPEST requirements contained in this document. Certification as to compliance must be accomplished prior to operational use of CCI equipment and any connected processing equipment for classified or national security related information.

2. In order to ensure the continued integrity of the CCI equipment/processing equipment configuration control of the installation must be maintained. This Annex describes the process and responsibilities for accomplishing certification and maintaining configuration control.

#### **II. CERTIFICATION**

##### **A. Introduction**

Certification can be accomplished in a logically phased manner and the following describes a three-phased approach which should be used. The certification section addresses physical security for the CCI equipment and TEMPEST for those situations which also involve processing equipment connected to the CCI equipment and which require TEMPEST countermeasures.

##### **B. Phase 1 - Site Survey**

A physical survey of the site which is to contain the CCI equipment and processing equipment, if applicable, should be made prior to the actual installation. A site survey is not required when there is already CCI equipment at the site and the upcoming installation merely consists of adding more CCI equipment to that site.

1. Physical Security - Prior to the installation of the CCI equipment, the contractor purchasing the equipment and the qualified entity responsible for installation (this could be the vendor or) another qualified entity, (see Annex D for qualifications) shall conduct a site survey to determine what, if anything, needs to be done to the area(s) which will contain the equipment, key and any classified material in order to meet the requirements of this document.

2. TEMPEST - For those situations where SECRET or higher information is to be processed, and there is a need to implement TEMPEST countermeasures, in accordance with the guidance and procedures in Annex E, a government Contracting Office, or its designated representative must determine which of the options presented in Annex E will be applied. The two appendices of Annex E can be of great value in making this determination.

#### C. Phase 2 - Site Preparation

Prior to the installation of the CCI equipment and any connected processing equipment, any site preparation that results from the site survey must be completed.

1. Physical Security - The contractor purchasing the CCI equipment is responsible for taking any corrective actions necessary to meet the physical security requirements.

2. TEMPEST - The contractor is also responsible for taking any corrective actions necessary to comply with the requirements of the TEMPEST countermeasure option selected. The vendor of the CCI equipment will be responsible for offering interconnection equipment (e.g., cables) for use between the CCI equipment and the processing equipment which, if installed properly, will not cause any TEMPEST problems. The interconnection equipment design must be approved by a certified TEMPEST person. This certification shall be sent to the NSA CCI equipment Program Manager and a copy retained by the vendor. The vendor shall provide the name and address of the NSA CCI equipment Program Manager to the certified TEMPEST person.

#### D. Phase 3 - Installation Inspection, Approval and Certification

Prior to the operational use of the CCI equipment (i.e., use with operational key) and any connected processing equipment, the installation must be inspected and approved as meeting all applicable requirements of this document.

##### 1. Physical Security

##### a. When the CCI equipment is to be used with classified key:

(1) Prior to installation the Facility Security Supervisor (FSS) shall inspect and approve that the area(s) which will contain the CCI equipment, the classified key, and other classified material, meets the applicable physical security requirements of this document. The FSS shall notify the COMSEC custodian and the CCI equipment vendor or the installer, as appropriate, of his approval.



## FOR OFFICIAL USE ONLY

(2) Prior to operational use, the FSS shall inspect and certify that the installation has been done in accordance with the applicable physical security requirements of this document. A copy of the certification shall be retained by the FSS and copies will be sent to the Defense Investigative Service Cognizant Security Office (DIS CSO), the COMSEC custodian, and if the equipment is owned by the Government, the appropriate Government Contracting Office(s).

b. When the CCI equipment is to be used only with unclassified key:

(1) Prior to installation the COMSEC custodian shall inspect and approve that the area which will contain the equipment and the unclassified key meets the applicable physical security requirements of this document and notify the CCI equipment vendor or the installer, as appropriate.

(2) Prior to operation the COMSEC custodian shall inspect and certify that the installation has been done in accordance with the applicable physical security requirements of this document. A copy of this certification shall be retained by the COMSEC custodian.

### 2. TEMPEST

a. When it has been determined that TEMPEST countermeasures are needed, and prior to operation of the CCI equipment and connected processing equipment for SECRET or higher information, a certified TEMPEST person must inspect the installation and certify that these countermeasures have been applied properly. It is the responsibility of the Government contracting office or its designated representative to arrange for this inspection. Possible sources of TEMPEST expertise include Government cryptologic elements whose services could be obtained on an as available basis via an appropriate Government Contracting Office or a TEMPEST qualified contractor.

b. For those systems that constitute a standard configuration (i.e., systems using processing equipment that is listed on the Preferred Products List and vendor supplied interconnecting equipment, the design of which has been previously certified by a certified TEMPEST person), the certification of one system constitutes certification of all identical systems. In this situation the installer may act as the inspector and he need not be a TEMPEST certified person.

c. The person inspecting the installation must provide written certification that it meets applicable TEMPEST countermeasures requirements to an appropriate Government Contracting Office(s) with a copy provided to

## FOR OFFICIAL USE ONLY

the FSS of the contractor who purchased the CCI equipment. A copy should also be retained by the entity providing the certification. This installation will be subject to audit by an independent TEMPEST agency of the Government.

### E. Recertification

Recertification of compliance with the physical security and TEMPEST requirements must be accomplished whenever there are changes in the installation that can affect the security. Examples of changes that would affect security include moving the CCI equipment into another area, connecting a different model of processing equipment and CCI equipment with an interconnect system that is different than the original. Recertification is not required for maintenance actions such as replacing a defective CCI or processing equipment with a like model.

### F. Reinspection

For CCI equipment applications employing classified key, an inspection of the CCI equipment and any connected equipment by representatives of the Government (e.g., an agent of the Government) will be conducted at least once within two years from the date of the initial certification and will be conducted aperiodically thereafter. These reinspections will look for continued compliance with the requirements of this document.

## III. CONFIGURATION CONTROL

A. Introduction - In order to ensure the continued security integrity of the CCI equipment and any connected processing equipment, it is important that configuration control be maintained. The Memorandum of Understanding and/or Memorandum of Agreement with the vendor of the CCI equipment provides strict requirements for the configuration and modification control of the equipment. In general, all modifications to stand-alone CCI equipment and all modifications to the embedded cryptographic subsystem of endorsed CCI equipment must be approved by NSA. This requirement extends to the contractor purchasing the CCI equipment. The remainder of this section provides direction on the configuration control of the installation of the CCI equipment and any connected processing equipment.

B. CCI Equipment Applications using Classified Key - For CCI equipment application using classified key, control shall be maintained over the installation configuration. The certified installation shall be documented (e.g., equipment model numbers, location of cable runs between the CCI equipment and connected processing equipment, the location of the processing equipment in an approved TEMPEST zone). The FSS shall be responsible for

## FOR OFFICIAL USE ONLY

retaining this documentation and ensuring that it is kept up-to-date (the entity that certified the installation should also retain a copy). The configuration documentation must be made available, if requested, to the persons conducting Government audits.

C. CCI Equipment Applications using Unclassified Key - For CCI equipment applications using unclassified key there are no control requirements for the configuration of the installation. However, the configuration control requirements for the CCI equipment itself described in paragraph A. above apply.

## **ANNEX I**

### **AUTHORIZED VENDOR EQUIPMENT**

A. The Appendices to this Annex provide brief descriptions of the equipment that is available from vendors authorized by NSA to directly sell CCI equipment, the names of the vendors and the points of contact, and any access and physical security or other (e.g., key ordering) requirements for these equipments which, because of their unique nature, are not covered in the other Annexes.

B. As additional CCI equipment becomes available additional appendices to this Annex will be supplied.

# APPENDIX 1 TO ANNEX I

## KY-71

### I. Introduction

A. This appendix provides a brief description of the KY-71 Secure Telephone Unit (STU-II); the vendor name, address and point of contact; unique access and physical security requirements; and method(s) of keying and, the procedures for ordering material.

### II. General Description

A. The KY-71 is a CCI equipment which provides clear as well as secure voice through standard (non-conditioned) Government and commercial switched telephone networks. These include two-wire systems such as the Direct Distance Dial (DDD) system and GSA's Federal Secure Telephone Service Telecommunications System (FSTS), and four-wire systems such as the DoD AUTOVON.

B. The KY-71 operates at 9600 bps and at 2400 bps in the secure voice mode and also has a secure data capability at 2400 bps.

C. In terms of cryptonet operation, the KY-71 can operate in the net mode (all members have the same key) or in the Key Distribution Center (KDC) mode (all secure calls on a different key).

D. Key is inserted in the KY-71 via the KOI-18 paper tape reader or the KYK-13 electronic transfer device.

### III. Vendor

A. The International Telephone and Telegraph Corporation (ITT) is an authorized vendor of the KY-71. Inquiries concerning the purchase of the KY-71 should be made to:

The ITT Corporation  
Defense Communications Division  
492 River Road  
Nutley, NJ 07110  
Telephone: (201) 284-3168

#### IV. KY-71 Unique Access and Physical Security Requirements

##### A. Application

The KY-71 provides full security for all applications of voice and data when used with an appropriately classified key (e.g., when used with TOP SECRET key it may be used to secure TOP SECRET information).

##### B. Access and Physical Security

1. General - The KY-71 is an unclassified Controlled Cryptographic Item (CCI), and it must be accounted for by serial number (i.e., Accounting Legend 1) in accordance with the requirements of Annexes B and C. In addition to the access and physical security requirements of Annex D, the following applies to the KY-71.

##### 2. Crypto-Ignition Key

a. The KY-71 includes a KYK-71 Crypto-Ignition Key (CiK) which provides a convenient method for unkeying and rekeying the KY-71 on a frequent basis without requiring access to actual keying material.

b. The CiK must be inserted in the KY-71 whenever a key is being loaded and wherever secure mode operation is required. When the CiK is inserted the KY-71 is considered keyed and must be protected in accordance with the requirements for a keyed CCI equipment.

c. When the CiK is removed, the KY-71 is considered unkeyed and must be protected in accordance with the requirements for unkeyed CCI equipment.

d. The CiK is an unclassified CCI device and must be protected in accordance with the requirements for unkeyed CCI equipment. However, when not inserted in its associated KY-71, the CiK should be protected in a manner that provides physical separation from the associated KY-71 (e.g., locked in a separate room, kept in the pocket of an authorized KY-71 user).

e. The CiK is an accounting legend 2 item and therefore accountable by quantity in accordance with the procedures of Annexes B and C.

### 3. KY-71 Deskset

a. The KY-71 can have between one and six desksets remotely located up to 1000 feet from the KY-71 via a junction box (Z-AMX). These desksets can be individually enabled/disabled via a user action at the deskset.

b. The desksets are not considered CCI equipment. However, use of an enabled deskset shall be limited to the positive control of persons who are cleared to the self-authentication level of the system (e.g., SECRET for FSTS). Desksets shall be disabled when not under the positive control of appropriately cleared individuals.

#### c. Safeguarding Desk Sets, Junction Boxes, and Wirelines.

(1) All desk sets, junction boxes, and interconnecting wirelines comprise a secure subscriber facility and must be installed to meet the requirements outlined in Annex E. A one meter separation is not required between the KY-71 desk set and a black commercial telephone. These two instruments may be co-located as close as desired, provided the black commercial telephone has a hook switch that disconnects its internal circuitry from the handset when it is on-hook. A 50mm separation is not required around the cable from the STU-II desk set, regardless of its length, provided that the KY-71 desk set so installed is only used to process analog voice signals and is never used to process digital signals. Cables and desk sets so installed must be appropriately labeled so as to preclude their use to process digital data. The restriction against placing the KY-71 desk set and a black commercial telephone on the same metallic surface does not apply.

(2) Within CONUS, Hawaii, Alaska, and U.S. territories, where the threat of technical surveillance is generally minimal, STU-II desk set distribution lines which run outside of controlled areas must be visually inspectable (i.e., either hidden or visible, but easily accessible for aperiodic inspection). Conduit is generally not required for physical security reasons, however, technical risks do remain and conduit may be advisable to protect classified information in vulnerable areas. In those cases this walled conduit (electrical metallic tubing (EMT)) will suffice. Wirelines processing compartmented information (SI/SAO) must comply with appropriate security regulations. All PDS installations must meet the requirements of applicable department or agency documents pertaining to PDSs for the classification of information being protected. Appropriate department or agency COMSEC authorities should be consulted for specific secure distribution system installation guidance.

d. The desksets and junction box are Accounting Legend 4 items.

#### 4. Keying Material

a. Introduction - The KY-71 can operate in either of two basic cryptographic modes, the Key Distribution Center (KDC) mode or the Net mode.

##### b. KDC Mode

(1) A unique key (Vu) is required to be loaded into the KY-71 for KDC mode operation. The Vu is a paper tape key unique to each KY-71. It is used only for protecting the call keys (Vcall) and is held by the KY-71 and its associated Key Distribution Center (KDC). (The KDC is a computer based facility which provides, as a result of an automatic phone call from the KY-71, call keys to the KY-71.) The Vu is never used to protect traffic. Individual Vus may not be used on more than one KY-71 without specific approval of the Controlling Authority. Vu's are classified to the highest level of information authorized to be transmitted on a specific KY-71 but are classified SECRET as a minimum.

(2) Net Sizes - KDC mode operation permits cryptographic interoperability with the majority of other KY-71's operating in the KDC mode. As such there are no net size restrictions per se.

(3) Cryptoperiod - The normal cryptoperiod of a Vu is three months.

(4) Authentication - In the KDC mode the KY-71 is self authenticating to the SECRET level. When discussing TOP SECRET or compartmented information, it is each user's responsibility to determine the clearance of the other party receiving the information. This may be done by positive voice recognition, where the individual's clearance level is already known or through the use of other acceptable authentication means (e.g., NSA-approved authentication systems).

(5) The Vu is an Accounting Legend 1 item.

##### c. Net mode

(1) A net key (Vn) is required to be loaded into the KY-71 for net mode operation (i.e., when multiple KY-71's all contain a common key). The Vn is a paper tape Traffic Encryption Key (TEK) held in common with a number of KY-71's. Only one net key can be stored in a KY-71 at a time. Vn's are classified to the highest level of information authorized to be transmitted over a given cryptonet. Vn's can be UNCLASSIFIED, CONFIDENTIAL SECRET, and TOP SECRET.



(2) For classified and unclassified Vns the normal cryptoperiod is one month with a daily update.

(3) Net sizes - Classified Vn cryptonets will be no larger than 30 holders (members). Exceptions to cryptonet size restrictions may be approved only by NSA, on a case-by-case basis. Unclassified cryptonets can be any size. However, the vulnerability to compromise and the subsequent impact of a compromise increase as the net gets larger. Contingency cryptonets which may be activated only by the Controlling Authority may be as large as operationally required.

(4) The Vn is an Accounting Legend 1 item.

## V. KY-71 Keying Method

A. KDC Mode vs Net Mode - The KY-71's primary mode of operation is KDC-mode, although the terminal can also accommodate a net mode for either special applications or contingency use. In net mode, traffic is protected by keying material that is held by all net members in hard copy form. The KDC-mode offers greater security than the net mode and its use is encouraged in preference to net-mode operations for the KY-71.

### B. System Operation

1. The KY-71 is assigned a Vu key which is held only by that particular KY-71 and by the KDC. The KDC has stored in its data base the Vu keys of all KY-71 terminals worldwide. Using the key the KDC encrypts Vcall keys and passes them securely to the KY-71's. The Vu keys are distributed on paper tape in protective canisters, and are manually changed.

2. For purposes of using KDC service, each KY-71 terminal is assigned a five-digit identification number. This terminal ID number uniquely identifies a KY-71 both to the KDC and to other KY-71s.

3. When a KY-71 calls the KDC to request a Vcall key, it automatically passes to the KDC both its unique five-digit ID number and the ID of the terminal being called. This data is sent to the KDC in the clear. The KDC then uses these two terminal IDs to identify the unique keys in which Vcall keys should be encrypted before they are returned to the calling terminal.

4. The KDC must maintain files showing the terminal ID numbers of all terminals in the system and the current association of unique keys to terminal ID numbers. The contents of the latter file normally changes, as KY-71 terminals are rekeyed. The process of constructing this file is called "binding," and the data that associates terminals with their unique keys for any given cryptoperiod is called "binding data."

## VI. Obtaining Key Distribution Center Service

A. The General Services Administration (GSA) has been designated the Controlling Authority and System Manager for the Federal Secure Telephone Service (FSTS) and the KDC. As such, GSA is responsible for assigning KY-71 terminal ID numbers, maintaining the KDC data base, collecting binding data and inputting it to the KDC, and placing orders with NSA for the production and distribution of sufficient keying material for all terminals. GSA also operates trouble assistance and directory assistance services for subscribers who are having difficulty with terminal operations or in placing secure calls.

B. In order to provide effective and efficient system management, GSA requests that two points of contact be designated for each KY-71 terminal. One of these is the Terminal Coordinator, who handles the administrative details of initial installation, KDC data base registration, and keying. The second of these is the Binding Coordinator, who handles the recurring requirement to report to GSA the identity of the unique key to be used in the terminal during the next cryptoperiod. For Government-owned equipment (Government Purchased or Contractor-acquired property), the responsible Government contracting officer should designate the Terminal and Binding coordinators. For contractor-owned equipment the contractor should designate these coordinators. In all cases the number of Terminal Coordinators and Binding Coordinators should be kept to an absolute minimum.

### C. The Terminal Coordinator

1. The Terminal Coordinator acts as a point of contact for GSA regarding terminal data. Appointment of a new Terminal Coordinator must be requested by letter or message to GSA. The Terminal Coordinator is responsible for requesting new terminal ID numbers and providing terminal input information. Requests for KY-71 ID numbers should be directed to the GSA Terminal ID point-of-contact on terminal ID 00188 telephone number COMM (202) 245-3496 or FTS 245-3496.

2. In order for a KY-71 terminal to make or receive secure calls using electronic per-call keys, it must be entered in the KDC data base. This is accomplished by the Terminal Coordinator completing the FSTS User Worksheet (see Appendix 2 to this Annex). Information on the FSTS User Worksheet is provided to GSA via electronic message or registered mail. GSA will accept User Worksheets only from the designated Terminal Coordinator. Only the Terminal Coordinator can authorize terminal additions, deletions, or modifications which must be submitted on the FSTS Users Worksheet.

3. The initial FSTS User Worksheet should be completed in full. However, any subsequent worksheets which update the original need only include: Section 1 -Administrative Data; Section 2 - Agency Terminal Coordinator; and any information which has changed since the previous

worksheet. A worksheet format with instructions is included in Appendix 2 of this Annex. Questions pertaining to FSTS User Worksheets should be directed to the GSA worksheet point-of-contact on terminal ID 00188 telephone number COMM (202) 245-3496 or FTS 245-3496. Completed worksheets should be submitted to this message address: GSA Berryville//KDC SF//; or mailing address (via registered mail): P.O. Box 129, Berryville, VA 22611. Allow 30-60 days for data input and verification before operation in KDC mode.

D. The Binding Coordinator

1. Binding is the process of creating a data file within the KDC which associates each KY-71 terminal number with Vu key. The Binding Coordinator is responsible for executing this procedure when instructed by GSA, and for providing GSA with the assignment information. Key is identified by a short title (normally USKAT-500 or USKAT-501 in the FSTS), an edition designator (e.g., AB, AC, ...) and a unique five-digit Vu ID number. Examples of the prompt message and the Binding response message are included in Appendix 2.

2. The Terminal Coordinator will perform the initial binding of terminal-unique key to a new terminal's ID number. Afterwards, GSA will send the Binding prompt message to the Binding Coordinator listed on the FSTS User Worksheet. Questions regarding binding information should be directed to the GSA Binding point of contact on the KY-71 ID number 00188 telephone number COMM (202) 245-3496 or FTS 245-3496.

## APPENDIX 2 TO ANNEX I

### KEY ORDERING FORMS

#### Contact List

General Services Administration

Mailing Address: GSA, CDMF  
P.O. Box 129  
Berryville, VA 22611

Message Address: GSA Berryville//KDC SF//

Phone Number: KY-71/STU-II:

Terminal ID 00188  
COMM (202) 245-3496  
FTS 245-3496

#### Questions Regarding:

Terminal ID Numbers: Merle A. Robertson  
Jamie S. Lichliter

FSTS User Worksheet: George D. Bradford  
Jamie S. Lichliter

Binding Information: George D. Bradford  
Jamie S. Lichliter

Program Information Questions should be directed to:

GSA: General Services Administration  
NCR ATTN WKIE  
7th & D Streets SW  
Washington, DC 20407

Phone Number: Commercial (202) 453-3978

KY-71/STU-II: Terminal ID 01145  
COMM (202) 453-4069  
FTS 453-4069

NSA: DIRNSA, V21  
9800 Savage Road  
Ft George G. Meade, MD 20755-6000

Phone Number: COMM: (301) 859-6783

KY-71/STU-II: Terminal ID 00028  
COMM (301) 850-5893

COMSEC Account questions should be directed to:

NSA: DIRNSA, Y131  
9800 Savage Road  
Ft. George G. Meade, MD 20755-6000

Phone Number: COMM (301) 688-8110

## FSTS User Worksheet Format

1. Administrative Data

Agency or Contractor:

Sponsoring Agency if Contractor:

2. Terminal Coordinator

Full Name	Secure	Mailing	Classified
Phone Number	Address	Msg Address	

If requested, may we release this data to other agencies? Y/N

3. Binding Coordinator

Full Name	Secure	Mailing	Classified
Phone Number	Address	Msg Address	

4. Terminal Data

Term ID	No	Type	Short	Ed	Vu ID	Remarks
	of Svc	Title				

5. COMSEC Depot Data

Account Number

Custodian's Name

Telephone Number (Secure)

Mailing Address

Message Address (Classified)

6. STU-II Directory Assistance

Agency

Telephone Numbers:

Department

COMM

Office

FTS

Terminal ID Number

AUTOVON/ETS

7. Technical Assistance Data

Term ID No.	Location	Area	Area Main Ofc
	Main Ofc		Telephone No.

FSTS User Worksheet Instructions

1. Administrative Data

To complete administrative data, list the name of your agency. If user is a contractor, list contractor's name and sponsoring agency.

2. Agency Terminal Coordinator

List your Terminal Coordinator's name, secure telephone number, mailing address and classified message address including the routing indicator (if none, please indicate).

3. Binding Coordinator

List the Binding Coordinator's name, secure telephone number, mailing address and classified message address including the routing indicator (if none, please indicate).

4. Terminal Data

TERM ID NO. - Specific ID number assigned to your terminal by GSA, CDMF.

TYPE OF SVC - Delete, add, modify, listed in this order.

DELETE - Request to remove a terminal from service. List all deletes before listing adds.

ADD - Request to activate a terminal. List all adds before going to modify.

MODIFY - Request to change present terminal input data.

SHORT TITLE - Any identifying combination of letters and numbers assigned to COMSEC material for identification.

ED (Edition) - One or more alpha characters which identify a series of COMSEC material.

VU ID (Variable Unique ID) - A COMSEC key held by one CRYPTO equipment and uniquely associated with one terminal ID number.

REMARKS - List any significant events such as moving and transferring of equipment and any other changes not listed.

5. COMSEC DEPOT DATA

ACCOUNT NUMBER - Assigned COMSEC account number.

CUSTODIAN'S NAME - Designated COMSEC Custodian.

TELEPHONE NUMBER (Secure) - Secure telephone number where COMSEC Custodian can be reached.

MAILING ADDRESS - Address for COMSEC Custodian.

MESSAGE ADDRESS (Classified) - Provide address used to receive classified message including the routing indicator. If none, please indicate.

6. STU-II Directory Assistance

If supplied, the following information will only be used at the KDC to provide Directory Assistance for your terminal.

Your FSTS Telephone Directory Listing requirements will be solicited by a message to all Terminal Coordinators.

List your Agency, Department and Office.

TERM ID NO. - Assigned Terminal ID Number.

COMM - Commercial Telephone Number.

FTS - FTS Telephone Number.

AUTOVON/ETS - AUTOVON/ETS Telephone Number.

7. Technical Assistance Data

GSA can provide guidance for technical assistance for terminals if desired.



TERM ID NO. - Assigned Terminal ID Number.

LOCATION - The physical location of the terminal which may require technical assistance.

AREA MAIN OFC (Area Servicing Maintenance Office) -The GSA area or office responsible for maintaining the terminal.

AREA MAIN OFC TELEPHONE No. - The telephone number for the GSA office responsible for maintaining the terminal.

Example of prompt message sent to terminal coordinator

SUBJ:Projected Future FSTS Key Material Requirements (U)

(C) In order to provide all agencies with sufficient amount of future KY-71/STU-II keying material (USKAT-500 or USKAT-501), request that each agency submit an annual report projecting future requirements from \_\_\_\_\_ to \_\_\_\_\_. The annual report should be submitted in a cumulative amount for each quarter. The quarters for this reporting period are as follows:

first quarter - \_\_\_\_ through \_\_\_\_, second quarter - \_\_\_\_ through third quarter - \_\_\_\_ through \_\_\_\_, fourth quarter - \_\_\_\_ through \_\_\_\_.

(U) If there are no projected increases, negative reports are requested. Your response should be received by this office no later than \_\_\_\_\_.

(U) Questions concerning this message may be addressed to Merle A. Robertson on ID number 00188 telephone number COMM (202) 245-3496 or FTS 245-3496.

(C) The following is an example format for you to follow when submitting your response:

Example

SUBJ: Projected Future FSTS Key material Requirements Response

Reference: MSG DTG \_\_\_\_\_ CITE NUMBER \_\_\_\_\_.

Listed below is the cumulative projected key material requirements data information for the period \_\_\_\_\_ through \_\_\_\_\_ for each quarter.

First quarter	Second quarter
Third quarter	Fourth quarter

Declass \_\_\_\_\_.

Example of prompt message sent to terminal coordinators and binding coordinators.

SUBJ: FSTS Rekey (Binding) Data/rekey window notification (U)

(C) USKAT-500 (USKAT-501) Edition \_\_\_ will be superseded at 2400 hours ZULU on \_\_\_\_\_ by USKAT-500 (USKAT-501) edition \_\_\_\_.

(U) We require your binding data response by \_\_\_\_\_. the following data must be provided to his message address: "RUCFAAA GSA Berryville VA//KDC SF//".

1. Short title and edition. (list only once)
2. Binding coordinator's name, telephone number and agency. (list only once)
3. Term ID No.                      Vu ID No.

It is imperative that this information be correct and submitted on a timely basis.

(C) You may rekey your terminal any time from \_\_\_\_\_ through \_\_\_\_\_. If your terminal is not rekeyed within this period, you will be unable to go secure in the KDC mode until you perform the rekey.

(U) Any questions concerning this message may be addressed to STU-II ID number 00188 telephone number COMM (202) 245-3496 of FTS 245-3496.

Declass \_\_\_\_\_.

Example of Binding Response Message sent by Binding Coordinators.

SUBJ: Binding Data Response

REFERENCE: MSG DTG \_\_\_\_\_ CITE \_\_\_\_\_

(C) This binding data information required for the CRYPTO-period beginning \_\_\_\_\_.

1. Short title and edition:
2. Binding Coordinator's name, telephone number, agency
3. Term ID No.                      Vu ID No.

## **APPENDIX 3 TO ANNEX I**

### **KG-84A**

#### **I. Introduction**

This appendix provides a brief description of the KG-84A General Purpose Encryption Equipment; the vendors names; and unique access and physical security requirements.

#### **II. GENERAL DESCRIPTION**

A. The KG-84A is an on-line cryptographic equipment which is used to secure digital data and teletype traffic. It can be used in the duplex mode of operation with the capability of receiving and transmitting at different selectable rates simultaneously. It can also be operated in the half-duplex or the simplex modes.

B. In the synchronous mode, it can operate at all standard data rates from 50 bps to 32000 bps, using its internal clock, or from DC to 64000 bps using an external clock.

C. In the asynchronous mode, it operates at all standard rates from 50 baud to 9600 baud.

D. The KG-84A is keyed via the KOI-18 or the KYK-13 fill devices.

#### **III. Vendors**

Inquiries concerning the purchase of the KG-84A should be directed to:

Allied Bendix Aerospace	Director of Marketing
Bendix Communications Division	TRW/EPI
1300 E. Joppa Road	or 3450 N. Nevada Avenue
Baltimore, MD 21204	Colorado Springs, CO 80907
Telephone: (301) 583-4000	Telephone: (303) 475-0660

#### **IV. KG-84A Unique Access and Physical Security Requirments**

##### **A. Application**

The KG-84A provides full security for all applications of data when used with an appropriately classified key (e.g., when used with TOP SECRET key it may be used to secure TOP SECRET information).

##### **B. Access and Physical Security**

The KG-84A is an unclassified Controlled Cryptographic Item (CCI). It must be accounted for by serial number (i.e., Accounting Legend 1) in accordance with the procedures of Annexes B and C. In addition to the access and physical requirements of Annex D, the following requirements apply to the KG-84A.

#### 1. Keying Material

The KG-84A can operate in the common net mode (i.e., all members of the cryptonet use the same key), and in the point-to-point mode (a special net mode case where there are only two members). The KG-84A can be rekeyed manually using the KOI-18 or KYK-13 fill devices or it can be remotely rekeyed by another KG-84A. Key stored in the KG-84A can also be "updated" (i.e. a currently loaded key is irreversibly modified by an internal KG-84A process).

a. Traffic Encryption Key (TEK), also referred to as the "X" Key, used to encrypt/decrypt digital information (i.e., traffic). The KG-84A can hold up to four different traffic keys simultaneously. Future traffic key variables may be loaded into the KG-84A prior to becoming operational; however, this should be done as close as possible to the end of the current cryptoperiod (e.g., one hour prior to the change of the current key). This key is an Accounting Legend 1 item.

#### 1) Cryptoperiod

a) For classified and unclassified TEK operating in the point-to-point mode (where the operation is 24 hours a day, seven days a week), the cryptoperiod is one month with a daily update. This means that a new key variable is loaded once a month and an update performed each day. The update period may be delayed for up to two hours to complete the processing of an urgent message.

b) The cryptoperiod for classified and unclassified TEK used in netted or part-time point-to-point applications is 24 hours. This means that a new key is loaded (possibly by remote rekeying) each day. The cryptoperiod may be extended for up to two hours to complete the processing of a message. Cryptoperiods longer than 24 hours may be used where it is operationally difficult to accommodate the 24 hour cryptoperiod but can be employed only after written NSA approval. When such extensions are approved the key shall be updated daily. Requests for approval should describe all the operational particulars and be sent to NSA, ATTN: S04.

#### (2) Cryptonet size

(a) For classified TEK the number of KG-84A's in any given net should be as small as possible and for classified key the number should not exceed 30. Cryptonet sizes larger than 30 may require more stringent physical security and access control procedures than described in Annex D. All cryptonet sizes that are to be larger than 30 must be approved by NSA.

(b) For unclassified TEK there are no restrictions on the size of the cryptonet, however the vulnerability to compromise and the impact of a compromise both increase as the net gets larger.

b. Key Encryption Key (KEK), also referred to as the "U" Key. The KG-84A can remotely rekey a distant KG-84A by encrypting the traffic or TEK with the KEK and transmitting it to the distant KG-84A. Remote rekeying is not operationally advantageous as a normal means of replacing the TEK. However, in those cases where it is operationally difficult to rekey manually and remote rekeying is deemed advantageous by NSA, then it can be used. This key is an Accounting Legend 1 item.

(1) The KG-84A must contain the current TEK and its unique KEK in order to perform remote rekeying's therefore, remote rekeying is only usable in full-time, continuous applications.

(2) The KEK must be unique from and equal to or higher in classification than the TEK. Only those keys specified for use as KEK may be loaded into the KEK position.

(3) Cryptoperiod - For classified and unclassified KEK the cryptoperiod is one month.

(4) Cryptonet size - KEK are "two-holder" keys (i.e., there can be only two parties in the cryptonet). Also, KEK may not be distributed electronically (i.e. remote distribution via another KEK is not permitted).

c. For all applications updates should be limited to once a day.

## **APPENDIX 4 TO ANNEX I**

### **KOI-18, KYK-13, and KYX-15 FILL DEVICES**

#### **I. Introduction**

This appendix provides a brief description of the KOI-18 General Purpose Tape Reader and the KYK-13 Electronic Transfer Device; the vendor name, address, and point of contact and any unique access and physical security requirements.

#### **II. General Description**

A. The KOI-18 is a CCI equipment used to load cryptographic key into a number of other cryptographic equipment. It is a hand-held, battery operated device which reads eight-level punched paper tape which contains the key. The KOI-18 reads the paper tape and converts the key to a serialized electronic output for transfer into the other cryptographic equipment, or a KYK-13. The KOI-18 does not store the key read from the paper tape.

B. The KYK-13 is a CCI equipment used to temporarily store and subsequently load cryptographic key into a number of other cryptographic equipment. The KYK-13 is small and battery operated and receives the cryptographic key via a KOI-18 paper tape reader. The KYK-13 can store up to six cryptographic keys and is used as a convenient means to load the same set of key into a number of equipment.

C. The KYX-15 is a CCI equipment used to remotely rekey a number of cryptographic equipment. The KYX-15 is small and battery operated and receives the cryptographic key via a KOI-18 paper tape reader. The KYX-15 can store up to 16 cryptographic keys, and is a necessary fill device for remotely loading the same set of keys into a number of equipment.

#### **III. Inquiries concerning these fill devices should be directed to:**

Systems Development Corporation  
A Burroughs Company  
P.O. Box 517  
Paoli, PA 19301  
Telephone: (215) 363-4627

#### IV. KOI-18 and KYK-13 Unique Access and Physical Security Requirements

##### A. Application

1. These fill devices can be used to load all classification levels of cryptographic key as well as unclassified key.

##### B. Access and Physical Security

1. Both of these fill devices are unclassified Controlled Cryptographic Items (CCI). However, when the KYK-13 is loaded and temporarily storing key, it assumes the classification level of the stored key, and should be controlled accordingly. Both devices must be accounted for by quantity (Accounting Legend 2) in accordance with the procedures of Annexes B and C.

2. Although the KYK-13 can store keys, it shall not be used for long term storage but rather for facilitating the loading of key in multiple CCI equipment during the normally brief period of time when these CCI equipment are being rekeyed. The KYK-13 must be zeroized (i.e., all key erased) when this period is over.

3. There may be "commercial versions" of these fill devices which are not labeled as "CCI equipment". These commercial versions shall not be used to key any CCI equipment.

4. Since these fill devices process key, it is therefore very critical that any evidence of suspected or actual tampering be reported to the NSA, ATTN: S21.

## **Annex J**

### **Glossary**

The following glossary contains definitions of terms as used in the U.S. Government Contractors Controlled Cryptographic Items (CCI) Manual. As far as possible, definitions have been coordinated with other official COMSEC glossaries and other documents.

A1721: COMSEC Material Hand Receipt.

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

ACCOUNTABLE COMSEC MATERIAL: See COMSEC Material.

ACCOUNTING LEGEND CODE (AL): A numeric code used within the COMSEC Material Control System to indicate the minimum accounting controls required for items of COMSEC material. (May also be abbreviated ALC.)

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

AL-1: The accounting legend code indicating continuous accountability by accounting number.

AL-2: The accounting legend code indicating continuous accountability by quantity.

AL-4: The accounting legend code indicating that initial receipt is required for an item so listed, but thereafter accountability to a COR may be dropped.

ALC: See Accounting Legend Code.

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



**APPROVED COMSEC CARRIER:** A trustworthy, U.S. owned and established firm or organization with a sound reputation which has been entrusted and approved by NSA to carry/transport CCI materials.

**ARFCOS:** See Armed Forces Courier Service.

**ARFCOS FORM 1:** The receipt for material shipped via ARFCOS.

**ARFCOS FORM 10:** Armed Forces Courier Authorization Record which authorizes contractor personnel to receipt for ARFCOS shipped material.

**ARMED FORCES COURIER SERVICE (ARFCOS):** The joint military courier organization authorized to transport all types and classifications of Government materials, including cryptographic equipment and keying materials.

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

**AUTHENTICATION:** Measures designed to provide protection against fraudulent transmission and imitative communications deception by establishing the validity of a transmission, message, signal, or individual. Authentication is also a means of identifying individuals and verifying their eligibility to receive specific categories of information.

**AUTHORIZED COMMERCIAL CARRIER:** A trustworthy, U.S. owned and established firm or organization with a sound reputation which has been entrusted and authorized by NSA to carry or transport COMSEC materials.

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

**AUTHORIZED VENDOR PROGRAM:** A program authorizing a manufacturer of existing/developed COMSEC equipment to produce excess quantities to sell directly to eligible buyers.

**BINDING:** The process of associating a specific terminal with its unique key encryption key for a given cryptoperiod.

**BINDING COORDINATOR:** For the KY-71/71A, the government contracting officer or contractor employee who is responsible for reporting to GSA the ID of the key encryption key to be used in the next cryptoperiod.

**BLACK:** A term applied to all telecommunications circuits, components, equipments, and systems which handle only encrypted or non-national security-related signals, and to telecommunications areas in which no national security or national security-related signals occur.

**CA:** See Controlling Authority.

**CALL KEY:** See Per Call Key.

**CANISTER:** A type of protective packaging for key in tape form.

**CAP:** See Contractor Acquired Property.

**CCEP:** See Commercial COMSEC Endorsement Program.

**CCI:** See Controlled Cryptographic Item.

**CCI CONTROL AGREEMENT:** An agreement binding the contractor/user of CCI equipment to the requirements of the CCI Manual regarding control, accounting, etc., and prescribing conditions for the financing, resale, and final disposition of the CCI equipments.

**CENTRAL OFFICE OF RECORD (COR):** The activity at NSA or other government department or agency, responsible for establishing and closing primary COMSEC accounts, maintaining records of all COMSEC accounts and custodians, maintaining master records of all issued accountable material and performing inventories and providing guidance and COMSEC briefings.

**CERTIFICATION OF ACTION STATEMENT:** A statement attached to the audit report being returned to the COR certifying that all actions have been completed by the COMSEC account.

**CERTIFIED INSTALLATION:** An installation that has been determined by NSA to meet minimum applicable physical and technical security requirements when installing COMSEC equipment.

**CIK:** See Crypto-Ignition Key.

**CLEARED COURIER:** See Authorized Company Courier.

**CO:** See Contracting Officer.

**COGNIZANT AGENT:** See Hostile Cognizant Agent.

**COGNIZANT SECURITY OFFICE (CSO):** The Defense Investigative Service Director for Industrial Security having industrial security jurisdiction over the geographical area in which a facility is located.

COMMERCIAL CARRIER: See Authorized Commercial Carrier.

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

COMMUNICATIONS SECURITY (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government and its contractors. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emission security) to electrical systems generating, handling, processing or using national security or national security related information. It also includes the application of physical security measures to communications security information and materials.

COMPONENT (CRYPTOGRAPHIC): See Cryptographic Component.

COMPROMISE: Any occurrence which results or can result in unauthorized persons gaining access to information equipment or other materials for which they are not authorized.

COMPROMISING EMANATIONS: Unintentional, intelligence-bearing signals which, if intercepted and analyzed, disclose the national security information transmitted, received, handled, or otherwise processed by any information-processing equipment.

COMPUSEC: See Computer Security.

COMPUTER SECURITY: The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer as well as measures designed to prevent denial of authorized use of the system.

COMSEC: The abbreviation of Communications Security.

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.

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

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

COMSEC AIDS: All COMSEC material, other than equipments or devices, that perform or assist in the performance of cryptographic functions or relate to associated functions and equipments, and are required in the production, operation, and maintenance of cryptosystems and components thereof. Some examples are: COMSEC keying material and supporting documentation, such as operating and maintenance manuals.

COMSEC CONTRACTOR: See COMSEC Vendor.

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

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, as well as equipment designed specifically to aid in or as an essential element of the conversion process. Cryptoequipment, crypto-ancillary equipment, crypto-production equipment and authentication equipment are all COMSEC equipment.

COMSEC FACILITY: A facility which contains classified COMSEC material.

COMSEC FUNCTION: A function of a cryptographic equipment or device providing purely cryptographic process, such as encryption or decryption.

COMSEC INSECURITY: Any occurrence which jeopardizes the security of COMSEC material or of the secure electrical transmission of national security or national security related information.

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

COMSEC MATERIAL: Any material in physical form whose intended purpose is to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security, or to ensure the authenticity of such communications. It includes, but is not limited to: (a) COMSEC keying material in any form to protect or authenticate national security or sensitive information which must be transmitted, communicated, or processed by electrical, electromagnetic, electromechanical, or electro-optical means; (b) those items which embody, describe, or implement a cryptographic logic; and (c) other items produced by or for the Government for COMSEC purposes.

**COMSEC MATERIAL CONTROL SYSTEM (CMCS):** A logistic system through which accountable COMSEC material is distributed, controlled, and safeguarded. It consists of all COMSEC Central Offices of Record, cryptologic depots and COMSEC accounts/subaccounts.

**COMSEC MEASURES:** All cryptographic, transmission emission and physical security techniques employed to protect telecommunications.

**COMSEC REGISTER FILE:** An accounting file of L6061 forms for each COMSEC device or equipment accountable by a contractor.

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

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

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

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

**CONFIGURATION CONTROL:** Ensuring that the security integrity of COMSEC equipment and any connected information processing equipment be maintained when considering modifications to a telecommunications system.

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

**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.

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

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

**CONTRACTOR-OWNED EQUIPMENT:** See Plant Equipment.

**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".

**CONTROLLED SPACE:** The area surrounding equipments that process national security or national security-related information in which unauthorized personnel must be either escorted by authorized personnel or be under constant physical or electronic surveillance. Unauthorized is defined as uncleared or, in the case of CCI equipment, not requiring access to the equipment.

**CONTROLLING AUTHORITY (CA):** The supervisor of a cryptonet whose responsibilities include cryptonet management, logistics, and security.

**COR:** See Central Office of Record.

**CRYPTO:** A marking or designator indentifying all COMSEC keying material used to protect or authenticate telecommunications carrying national security and national security-related information.

**CRYPTO-ANCILLARY EQUIPMENT:** Equipment designed specifically to facilitate efficient or reliable operation of a crypto-equipment, especially equipment designed specifically to convert information to a form suitable for processing by crypto-equipment, but which does not itself perform cryptographic functions.

**CRYPTO-EQUIPMENT:** Any equipment employing a cryptographic logic.

**CRYPTOGRAPHIC COMPONENT:** The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or information handling equipment. A cryptographic component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items.

**CRYPTOGRAPHIC INSECURITY:** Use of 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.

**CRYPTOGRAPHIC SECURITY:** That component of communications security which results from the use of technologically sound cryptosystems and from their proper use.

**CRYPTOGRAPHY:** (a) The art or science which treats the principles, means, and methods for rendering plain information unintelligible and for recovering

encrypted information into intelligible form. (b) The designing and use of cryptosystems. (c) The function which confirms the validity of data, messages, commands, or users.

**CRYPTO-IGNITION KEY (CIK):** A device, which can be removed from a crypto-equipment, used to protect key from physical compromise.

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

**CRYPTONET:** A collection of crypto-equipments operating on the same traffic encryption key.

**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.

**CRYPTOPERIOD:** A specific time period during which a particular key is used.

**CRYPTOSEcurity:** See Cryptographic Security.

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

**CS:** See Controlled Space.

**CSO:** See Cognizant Security Office.

**DD250:** Material Inspection and Receiving Report to receipt for COMSEC and CCI material shipped from vendor.

**DEPOT MAINTENANCE:** See Full Maintenance.

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

**DIRECT SHIPMENT:** Transportation of COMSEC material from one account to another with no intervening stops, such as at a GSA or military depot.

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

**DIS:** Defense Investigative Service.

**DROP ACCOUNTABILITY:** An accounting procedure by which a COMSEC account or subaccount receiving accountable COMSEC material assumes all responsibility after initial receipt and provides no further accounting to the COR. AL-4 items are drop accountable.

**EMISSION SECURITY:** That component of communications security which results from all the measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

**FACILITY:** A physically definable area consisting of a controlled space which contains national security or national security-related information processing equipment.

**FACILITY CLEARANCE:** The determination that from an administrative standpoint, a facility is eligible for access to classified information of a specific category.

**FACILITY SECURITY SUPERVISOR (FSS):** That employee in an office possessing a classified COMSEC account who is responsible for protecting the COMSEC equipment and keying material.

**FAR:** Federal Acquisition Regulation.

**FEDERAL SECURE TELEPHONE SERVICE:** The secure telecommunications system utilizing the KY-71/71A, commercial telephone system and the GSA operated Key Distribution Center.

**FILL DEVICE:** See Common Fill Device.

**FOCI:** See Foreign Ownership Control or Influence.

**FOREIGN OWNERSHIP CONTROL OR INFLUENCE (FOCI):** An administrative determination of the nature and extent of foreign dominance over the contractor's management and/or operations.

**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.

**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.



FSSO: See Facility Security Supervisor.

FSS: See Facility Security Supervisor.

FSTS: See Federal Secure Telephone Service.

FULL MAINTENANCE: All component diagnostic repairs, equipment modifications, and overhauls which are beyond the scope of limited maintenance.

GFE: See Government Furnished Property.

GFP: See Government Furnished Property.

GOVERNMENT CONTRACTOR: An individual, corporation, partnership, association, or other entity performing work under a U.S. Government contract, either as a prime contractor or as a subcontractor.

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

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.

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.

HARD COPY KEY: Physical keying material such as printed key lists or punched key tapes.

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

HAZARD (TEMPEST): The measure of the potential existence of compromising emanations at a point beyond the controlled space.

HOSTILE COGNIZANT AGENT: A person who is authorized access to national security or sensitive information and who intentionally makes it available to an unauthorized party whose goals are inimical to the interests of the U.S. Government.

**IMITATIVE (COMMUNICATIONS) DECEPTION:** The introduction, by unauthorized parties, of signals or traffic which imitate valid messages into communications channels to deceive authorized users.

**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.

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

**INTRUSION DETECTION SYSTEM (IDS):** A system to detect and signal the entry of unauthorized persons into a protected area (e.g., security alarms, sensor systems, video systems).

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

**INVENTORY REPORT:** A report submitted to the COR reporting those items of COMSEC material that were physically sighted in accordance with inventory procedures.

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

**ITP:** See Industrial TEMPEST Program.

**KDC:** See Key Distribution Center.

**KEY:** Data (usually a sequence of random binary digits) used to initially set up and periodically change the operations performed in a crypto-equipment. Examples of the forms key may take are key lists, punched tape, etc.

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

**KEY ENCRYPTION KEY:** A key used in the encryption and/or decryption of other keys.

**KEY LIST:** A printed series of key settings for a specific cryptonet at a specified time, which is produced in list, pad, or tape form.

**KEY MANAGEMENT:** The total process by which keys are generated, stored, protected, transferred, loaded, and destroyed.

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

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

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

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

**KMSP:** See Key Management Support Plan.

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

**LIMITED ACCESS AREA:** See Controlled Space.

**LIMITED MAINTENANCE:** Maintenance performed by maintenance activities responsible for direct support of user organizations. Limited maintenance includes disassembly, trouble isolation to a removable subassembly (i.e., printed circuit assembly, etc.), and replacement of the faulty subassembly without soldering. It also provides technical assistance to user organizations.

**LONG TITLE:** The descriptive title of a item of COMSEC material. (e.g., General Purpose Encryption Device for the KG-84/84A).

**MAINTENANCE KEY:** Key intended only for off-the-air, in-shop, use.

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

**MODIFICATION:** Any change to the electrical, mechanical, or software characteristics of an COMSEC end item.

**NATIONAL SECURITY AGENCY CENTRAL OFFICE OF RECORD (NSA COR):** The activity within NSA charged with the responsibility for maintaining records of accountability of all accountable COMSEC material entrusted to or generated by or for NSA, the Military Departments or Civil Agencies.

**NATIONAL SECURITY INFORMATION:** Information related to the national defense or foreign relations of the United States that was determined to be classified pursuant to Executive Order 12356 or any predecessor order.

**NATIONAL SECURITY-RELATED INFORMATION (UNS-R):** Information that is not classified but that would be detrimental if acquired by unauthorized persons.

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

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

**NET KEY:** A key held in common by all members of a given net.

**NET VARIABLE:** See Net Key.

**OPERATIONAL KEY:** Key intended for use on-the-air for the protection of mission-related, operational traffic.

**PAGE CHECK:** A check of the pages contained within an accountable COMSEC publication against the list of effective pages of handling instructions to ascertain the presence of each page and to determine if any pages are missing or duplicated.

**PDS:** See Protected Distributed System.

**PER CALL KEY:** A Traffic Encryption Key generated on command.

**PERSONNEL INSECURITY:** Any occurrence (e.g., loss, theft, loss of control, capture, recovery by salvage, tampering, unauthorized viewing, access or photographing) which results in jeopardy to COMSEC material.

**PERSONNEL SECURITY:** Determining an applicant's or an employee's loyalty and trustworthiness by ensuring that personnel investigations are completed in sufficient scope, commensurate with position sensitivity designations and according to the degree and level of access to classified and sensitive information.

**PHYSICAL INSECURITY:** Any occurrence (e.g., loss, theft, loss of control, capture, recovery by salvage, tampering, unauthorized viewing, access, or photographing) which jeopardizes or could jeopardize COMSEC material.

**PHYSICAL SECURITY:** The component of communications security which results from all physical measures necessary to safeguard COMSEC material and information from access by unauthorized persons.

**PLANT EQUIPMENT:** Contractor property of a capital nature (including equipment, machining tools, test equipment, telecommunications security and protection equipment, furniture, vehicles, and accessory and auxiliary items).

**POSSESSION REPORT:** To record on an SF153 the possession of COMSEC material when such material is received from another account without an accompanying SF153.

**PPL:** See Preferred Products List.

**PREFERRED PRODUCTS LIST:** A periodically published list of commercially produced, TEMPEST-approved equipments which meet the requirements of NACSIM 5100A, "Compromising Emanations Laboratory Test Standard, Electromagnetic (U)".

**PRIMARY COMSEC ACCOUNT:** A contractor COMSEC account which reports to the appropriate COR and which is administratively accountable for all its subaccounts.

**PROTECTED DISTRIBUTION SYSTEM (PDS):** An approved wire line and/or fiber optics system to which adequate acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for the transmission of unencrypted classified information.

**PROTECTIVE PACKAGING:** Packaging techniques for keying material which discourage penetration 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.

**QUALIFIED MAINTENANCE TECHNICIANS:** Individuals who have satisfactorily completed an NSA approved full or limited maintenance training course.

**RECONCILIATION STATEMENT:** The document which compares a subaccounts' holdings with the primary account's master records and/or preprinted inventory.

**RED:** A term applied to wirelines, components, equipments and systems which handle national security and national-security-related signals, and to areas in which national security signals occur.

**RED/BLACK CONCEPT:** The concept that electrical and electronic circuits, components, equipments, systems, etc., which handle national security or national security-related plain language information in electric signal form (RED) be separated from those which handle encrypted or non-national security-related information (BLACK).

**REGULARLY SUPERSEDED KEYING MATERIAL:** The keying material designated for use during a specified period of time and superseded whether or not the key is used.

**RE-INSTALLATION:** The connection of a previously installed equipment which has been moved to a new location at a COMSEC account.

**REMOTE REKEYING:** The secure electronic transmission of a key from a remote source.

**RESERVE KEYING MATERIAL:** Uncommitted keying material held to satisfy unplanned keying material requirements.

**RISK:** The probability that a hostile entity will successfully exploit a particular telecommunications or COMSEC system for intelligence purposes.

**SCOCE:** See Subcommittee on Compromising Emanations.

**SELF-AUTHENTICATION:** In general, implicit authentication of transmission on a secure telecommunications system or cryptonet to a predetermined classification level.

**SENSITIVE INFORMATION:** See National Security-Related Information.

**SF153:** The government form used for documenting transfer, possession, discrepancy in transfer, destruction, and inventory reports supplemental to preprinted reports for CCI and COMSEC equipment and materials.

**SHIELDED ENCLOSURE:** An area (room or container) specifically designed to attenuate electromagnetic radiation or acoustic emanations, originating either inside or outside the area.

**SHORT TITLE:** An identifying combination of letters and numbers assigned to COMSEC material for the purpose of brevity (e.g., KAM-1211A/TSEC, TSEC/KW-76). Each item of accountable COMSEC material is assigned a short title to facilitate handling and control.

**SPECIAL SECURITY AGREEMENT (SSA):** An agreement to be executed in the case that a contractor has been determined to be under foreign ownership, control or interests which will reasonably and effectively preclude access and/or transfer of CCI equipment and associated materials to foreign interests.

**SPP:** See Standard Practice Procedures.

**SSA:** See Special Security Agreement.

**STANDARD PRACTICE PROCEDURES (SPP):** A document written by the contractor which specifically implements all applicable security controls required by the CCI Manual, DD Form 441 and the Industrial Security Manual.

**SUB-ACCOUNT:** A COMSEC account established at a subordinate contractor facility (e.g., subcontractor) which reports to aid in the operation of the prime account and reporting to the prime account.

**SUBCOMMITTEE ON COMPROMISING EMANATIONS:** This subcommittee, of the National Telecommunications and Information Systems Security Committee (NTISSC) composed of representatives from various government organizations, is charged with specific responsibilities designed to implement Government-wide programs for the control and suppression of compromising emanations. In carrying out these responsibilities it is an instrument for exchanging technical TEMPEST information, techniques, and criteria among Government organizations and their contractors.

**SUPERSESSION:** Scheduled or unscheduled replacement of keying material with a different edition.

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

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

**TAMPERING:** An unauthorized modification which alters the proper functioning of a COMSEC equipment or system in a manner which degrades the security it provides.

**TEMPEST:** A short unclassified name referring to investigations and studies of compromising emanations. It is often used synonymously for the term "compromising emanations".

**TERMINAL COORDINATOR:** For the KY-71/71A, that government contracting officer or contractor employee responsible for handling the administrative details of initial installation, KDC data base regulation and keying.

**TEST KEY:** Keys intended for "on-the-air" testing of crypto-equipments.

**THREAT:** The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly telecommunications and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

**TRAFFIC ANALYSIS:** The study of communications characteristics which are external to the encrypted text.

**TRAFFIC ENCRYPTION KEY:** A key that encrypts and/or decrypts plaintext or previously encrypted information.

**TRAINING KEY:** Key intended for on or off-the-air use in support of mission-related operational training.

**TRANSFER OF ACCOUNTABILITY:** The process of transferring accountability for COMSEC material from the COR of the shipping organization to the COR of the receiving organization or between COMSEC Custodians.

**TRANSMISSION SECURITY:** That component of communications security designed to protect transmissions from unauthorized intercept, traffic analysis, imitative deception, and disruption.

**TSEC NOMENCLATURE:** A system for identifying the type and purpose of items of COMSEC material over which NSA exercises configuration control. (Note: TSEC is an abbreviation for Telecommunications Security.)

**UNCLASSIFIED COMSEC ACCOUNT:** A COMSEC account established for a user who will handle only unclassified equipment and keying material.

**UNCLASSIFIED NATIONAL SECURITY RELATED INFORMATION:** See National Security-Related Information.

**UNIQUE KEY:** See Key Encryption Key.

**UNIQUE VARIABLE:** See Key Encryption Key.

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

**UNS-R:** See National Security-Related Information.

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

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

**VENDOR:** See COMSEC Vendor.

**VULNERABILITY:** Characteristics of a telecommunications system or cryptosystem which are potentially exploitable by hostile intelligence entities.



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

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

ZONING: An approach which uses RF attenuation measurements to characterize the TEMPEST protection inherent to a facility, including both the free space attenuation associated with the facility's controlled space and the additional attenuation provided by the physical building structure. TEMPEST security is achieved by locating equipment/systems in appropriate TEMPEST zones. Similarly, equipment/systems are given zone assignments based on TEMPEST test data.