

16 SEPTEMBER 2002



Communications and Information

**CONTROLLED CRYPTOGRAPHIC ITEMS
(CCI)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ AFCA/WFPC (MSgt Michael Jervis)

Certified by: HQ USAF/XICI
(Colonel. Linda K. McMahon)

Pages: 21

Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become “Information Assurance”) and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4001, (FOUO) *Controlled Cryptographic Items*. It provides the minimum Air Force standards for controlling and handling controlled cryptographic items (CCI). It consists of a basic instruction and provides a list of conditions for allowing foreign nationals access to CCI equipment and components; criteria for selecting a commercial carrier to transport CCI equipment and components; accounting requirements for CCI equipment and components; and modified requirements for CCI equipment and components used to support network security systems. The requirements of this instruction apply to all Air Force activities, departments and agencies, and their contractors and vendors that handle, distribute, account for, store, or use CCIs. Direct questions and comments on the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5234. Refer recommended changes and conflicts between this and other publications, to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**. Maintain and dispose of records created as a result of prescribed procedures in accordance with Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4). The *Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Forms Management Program*, affect this publication. See **Attachment 1** for a glossary of references and supporting information. See paragraph **16.1**, concerning report requirements exceptions.

NOTE: This AFI replaces Air Force Systems Security Instruction 4001, *Controlled Cryptographic Items*, dated 1 August 1997.

1.	General Information	3
2.	Definitions	3
3.	Responsibilities	3
4.	Control Requirements	4

Table 1.	Requirements for Access to Unkeyed CCIs.	5
5.	Preparing for Shipment	5
6.	Transporting Unkeyed CCIs	5
Table 2.	Transportation of Unkeyed CCIs.	6
7.	Using Commercial Passenger Aircraft as an Authorized Mode of Transportation ...	7
8.	Using Commercial Passenger Aircraft as an Authorized Mode of Transportation Outside the U.S., Its Territories, and Possessions	8
9.	Shipment Notification	8
10.	Use of Foreign Nationals	8
11.	CCI Accounting Requirements	9
12.	Inventories	9
13.	Maintenance	10
14.	COMSEC Deviations	10
15.	Disposition and Emergency Destruction	11
16.	Information Collections, Records, and Forms	11
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		12
Attachment 2—CONDITIONS FOR ALLOWING FOREIGN NATIONAL ACCESS TO CCI EQUIPMENT AND CCI COMPONENTS		15
Attachment 3—CRITERIA FOR SELECTING A COMMERCIAL CARRIER TO TRANSPORT CCI EQUIPMENT AND CCI COMPONENTS		18
Attachment 4—ACCOUNTING REQUIREMENTS FOR CCI EQUIPMENT AND CCI COMPONENTS		19
Attachment 5—MODIFIED REQUIREMENTS FOR CCI EQUIPMENT AND CCI COMPONENTS USED TO SUPPORT NETWORK SECURITY SYSTEMS		21

1. General Information .

1.1. Background and Purpose. In March 1985, the category of communications security (COMSEC) equipment and components known as CCI was formally introduced. Procedures were developed to facilitate the production, acquisition, and use of this new category of COMSEC material. The CCI concept was successful in promoting the broad use of secure telecommunications and information handling equipment. Today, CCIs are used to protect voice, record, and data communications processed by traditional national security telecommunications systems, and also to provide network security for automated information systems.

1.1.1. The secure telecommunications and information handling equipment and associated cryptographic components designated "Controlled Cryptographic Items (CCI)," employ a classified cryptographic logic in their design. However, the hardware or firmware embodiment of that logic is unclassified but controlled. The associated cryptographic engineering drawings, logic descriptions, theory of operation, computer programs, and related source data remain classified.

1.1.2. The control requirements set forth in this instruction are necessary to guard against preventable losses of unkeyed CCIs to an actual or potential adversary. See paragraph 14. for detailed procedures for reporting incidents involving unkeyed CCIs.

2. Definitions . Definitions contained in Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, apply to this instruction. Although AFDIR 33-303 contains separate definitions for the terms CCI assembly and CCI component, no such distinction is made within the scope of this instruction. Throughout this document, CCI component is used as a collective term and, in this context, a CCI component may refer to a single microcircuit or module, a module set or assembly, a printed circuit board, or any combination of these items.

3. Responsibilities .

3.1. The Director, National Security Agency (DIRNSA), as stated in NSA publications:

3.1.1. Designates which COMSEC equipment and components to select as CCI.

3.1.2. Maintains a complete listing of all COMSEC equipment and components designated CCI.

3.1.3. Ensures proper marking of all CCI equipment and components to show their status as controlled cryptographic items.

3.1.4. Establishes the minimum control requirements applicable to CCI equipment and components.

3.1.5. Issues new or revised national-level Operational Security Doctrine for COMSEC equipment, components, and systems designated CCI.

3.1.6. Promulgates specific guidelines to use during the development and manufacture or assembly of all CCIs and ensures these guidelines are provided to affected United States (U.S.) GOVERNMENT CONTRACTORS and VENDORS. Accomplish this by providing appropriate design specifications directly to the contractor or vendor, or by incorporating applicable portions of such specifications in the contractual document or commercial agreement.

3.2. Headquarters United States Air Force, Deputy Chief of Staff, Warfighting Integration (HQ USAF/XI). Implements the control requirements set forth by National Security Agency (NSA), and

delegates certain responsibilities to HQ AFCA/WF and Headquarters Cryptologic Systems Group (HQ CPSG).

3.3. HQ AFCA/WF.

3.3.1. Develops, and recommends to HQ USAF/XI, new or revised Air Force Operational Security Doctrine for COMSEC equipment, components, and systems designated CCI.

3.3.2. Develops, and recommends to HQ USAF/XI, Air Force procedures for maintaining minimum control requirements applicable to CCI equipment and CCI components.

3.4. HQ CPSG.

3.4.1. Maintains a complete listing of all COMSEC equipment and components designated CCI within the Air Force inventory.

3.4.2. Act as the CENTRAL CCI AUTHORITY to provide oversight for managing all CCI assets held in the Air Force.

4. Control Requirements .

4.1. Control of CCI Equipment and Components. This section sets forth the minimum standards for controlling UNKEYED CCI equipment and components. Control keyed CCI equipment and components according to the requirements set forth in AFKAG-1, *Air Force Communications Security (COMSEC) Operations*, and AFI 33-211, *Communications Security (COMSEC) User Requirements*. The requirements of this instruction also apply to any otherwise unclassified information processing equipment modified through integration of a CCI component. When such equipment is so modified, the equipment becomes a CCI in its entirety. The information processing equipment remains a CCI as long as it continues to serve as a host for the CCI component. If the CCI component is subsequently removed, the host equipment reverts to its previous status as an unclassified information processing equipment. Refer to [Attachment 4](#), for accounting requirements applicable to CCI equipment described in this paragraph. See [Attachment 5](#) for modified requirements for CCI equipment and CCI components used to support network security systems.

4.2. Access. Use [Table 1](#). to determine requirements when granting U.S. and non-U.S. citizens access to unkeyed CCIs.

Table 1. Requirements for Access to Unkeyed CCIs.

The following requirements apply when granting access to unkeyed CCIs. For:		
A	B	
Access by U.S. Citizens	Access by Non U.S. Citizens	
A security clearance is not required.	Employed by the U.S. Government.	Employed by a U.S. Government Contractor or Vendor.
Normally grant access only to U.S. citizens who require this access to perform their regular duties.	The Commander may decide to grant access to permanently admitted RESIDENT ALIENS who are employees of the U.S. Government, or are active duty or reserve component members of the U.S. Armed Forces based on a determination that the official duties of the resident alien require this access.	Grant access only to permanently admitted resident aliens, and any other non-U.S. citizens, employed by a U.S. Government contractor or vendor with the prior written approval of the appropriate NSA program office. Submit requests for granting such access through Command COMSEC channels. Requests must be fully justified and based on operational need.
See Attachment 2 for specific conditions allowing FOREIGN NATIONALS access to CCIs.		

4.3. Protection of Unkeyed CCIs. Afford unkeyed CCIs protection at least equal to that normally provided to other high value/sensitive material. In addition, protective measures employed must reasonably guard against attempts by individuals to gain access to unkeyed CCIs with the intent of committing acts of theft, sabotage, or tampering. **NOTE:** When CCIs contain a key, make sure protective measures are consistent with the classification of the key, its purpose and/or the sensitivity of the information or function being protected by the key. The Operational Security Doctrine for a specific CCI equipment, component, or communication system will contain any unique or special controls applicable to that equipment, component, or system.

5. Preparing for Shipment .

5.1. Package unkeyed CCIs in any manner that:

5.1.1. Provides sufficient protection from damage.

5.1.2. Provides evidence of any attempt to penetrate the package while the material is in transit.

5.2. Mark the packages externally to identify the contents as CCI whenever the shipping activity determines that such marking is necessary to facilitate special handling during transit.

5.3. Ship CCIs only to AUTHORIZED ACTIVITIES. Address packages in a manner that ensures delivery of the material to an individual's unit who is designated to accept custody of it at the recipient activity. Address packages to a functional designator (e.g., unit/office symbol, duty position title [i.e., COMSEC manager], or account number), rather than addressed to an individual's name.

6. Transporting Unkeyed CCIs . Regardless of the mode of transportation selected, prepare unkeyed CCIs for shipment as set forth in paragraph [5](#).

6.1. Modes of Transportation. Use **Table 2.** to determine an authorized mode of transportation when transporting unkeyed CCIs.

Table 2. Transportation of Unkeyed CCIs.

Transport unkeyed CCIs through U.S.-controlled channels using a mode of transportation that provides both continuous accountability and reasonable protection against theft or loss of the material while it is in transit. Accordingly, the following modes of transportation are approved:		Within the U.S., Its Territories, and Possessions	Outside the U.S., Its Territories, and Possessions
1	Authorized U.S. Government department, service, or agency couriers.	X	X
2	Authorized U.S. Government contractor or company couriers. (Note 1)	X	X
3	U.S. Postal Service (USPS) Registered Mail, provided the material does not, at any time, pass out of U.S. control. (Note 2, 4, and 5)	X	X (Note 8)
4	USPS Express Mail, provided the material does not, at any time, pass out of U.S. control. (Note 3, 4, and 5)	X	
5	Commercial carriers certify they utilize a system accurately reflecting a continuous chain of accountability for the material while it is in transit. (Note 6)	X	
6	U.S. military or military-contract air service carriers (e.g., Air Mobility Command, Logair, Quicktrans) provided there is a continuous chain of accountability for the material while it is in transit.	X	X (Note 9)
7	Defense Courier Service (DCS), on a case-by-case basis, when there is no other approved mode of transportation servicing the destination. (Note 7)	X	X
8	U.S. Diplomatic Courier Service		X

NOTES:

1. Couriers must satisfy the requirements of **Table 1.**, Column A.
2. Obtain a recipient's signature when using registered mail. Introduce material into the postal system "across-the-counter" at an USPS facility; do not use postal drop boxes.
3. When using express mail, the shipper must obtain assurance from USPS authorities that the material will receive continuous electronic or manual tracking to the point of delivery. Obtain a recipient's signature when using express mail. Introduce material into the postal system "across-the-counter" at a USPS facility; do not use postal drop boxes.
4. There are certain restrictions governing the size and weight of packages shipped via USPS registered or express mail. Individuals responsible for shipping CCIs should check with their local USPS facility to obtain information regarding these restrictions.

5. USPS first class, fourth class, parcel post, certified, and insured mail are not approved for shipping unkeyed CCIs because these mail services do not provide continuous accountability.
6. As there is no formal listing of approved commercial carriers for CCIs, [Attachment 3](#) contains detailed criteria for selecting an appropriate commercial carrier. The shipper shall select a commercial carrier based on the carrier's compliance with these criteria.
7. Obtain prior authorization from DCS before introducing any unkeyed CCIs into the DCS system.
8. Package containing the CCI must not pass through any foreign postal system or be subject to any foreign postal inspection. You can use USPS registered mail to ship unkeyed CCIs to/from locations overseas, but only if the location is serviced by a Fleet Post Office or Army/Air Force Post Office authorized to process USPS registered mail.
9. To the maximum extent possible, material shipped to/from locations outside the U.S., its territories, and possessions should remain under continuous U.S. control. Although some limited handling of the material by foreign nationals may be unavoidable during aircraft loading and unloading operations, the material must be returned to U.S. control upon completion of these operations. Should the material subsequently show any evidence of unauthorized access or tampering, submit a COMSEC incident report according to AFI 33-212, *Reporting COMSEC Deviations*.

7. Using Commercial Passenger Aircraft as an Authorized Mode of Transportation . Follow the guidelines below when using authorized couriers to transport unkeyed CCIs aboard commercial passenger aircraft.

7.1. Whenever required by routine airport security procedures, inspect unkeyed CCIs in the presence of the courier. This inspection is normally limited to external viewing of the CCI; however, the CCI may be X-rayed if necessary.

7.2. The courier must always carry official documentation designating the individual as a courier. When applicable, this documentation must also state that the material in the courier's possession is property of the U.S. Government.

7.3. To the maximum extent possible, carry CCIs in the passenger compartment of the aircraft so the courier can keep the storage location under observation. However, if the equipment is bulky or configured so that the entire CCI cannot reasonably be carried in the passenger compartment, consider the following options:

7.3.1. If the equipment consists of an INTEGRATED CCI COMPONENT installed within an otherwise unclassified information processing equipment, the responsible activity shall, where authorized, have a QUALIFIED TECHNICIAN remove the CCI component from the equipment. The courier may then carry the CCI component on board the aircraft. Transport the remaining equipment, packaged in a manner that protects it from damage, in the hold of the aircraft.

7.3.2. If the equipment is treated as a CCI in its entirety, or the equipment has no removable CCI component, make prior arrangements with the airline to ensure the CCI can receive special handling by the airline prior to having the equipment transported in the hold of the aircraft. If the courier needs to change aircraft at an intermediate stop, they will ensure the CCI always accompanies

them on the same aircraft. All reasonable measures shall be taken to ensure the courier and the CCI arrive at the final destination on the same aircraft.

7.4. If a situation occurs where the courier and the CCI become separated, the courier must immediately notify the airline to initiate recovery actions. Also notify the shipping activity and inform them of the situation. Document all facts concerning the separation.

7.4.1. If the CCI is recovered, thoroughly examine it for signs of unauthorized access or tampering. If none are found, the courier resumes control of the CCI and continues to the destination.

7.4.2. If the CCI is recovered and shows signs of unauthorized access or tampering, or if the CCI is not located, the shipping activity must report this incident in accordance with requirements in paragraph 14. In cases of unauthorized access or tampering, the shipping activity must also provide instructions to the courier regarding proper handling of the suspect CCI.

8. Using Commercial Passenger Aircraft as an Authorized Mode of Transportation Outside the U.S., Its Territories, and Possessions .

8.1. In addition to complying with the guidelines contained in paragraph 7., make every attempt to use a commercial U.S. flag carrier as the method of choice whenever a courier transports CCIs outside the U.S., its territories, and possessions. When this is not possible, contact HQ AFCA/WFP for assistance in selecting an acceptable non-U.S. carrier.

8.2. In all cases, prepare an itinerary identifying the specific airline used; whether the flight is non-stop or whether any intermediary stops are required; and the estimated times of departure and arrival.

8.3. In addition to having the required documentation described in paragraph 7.2., the courier must possess any customs documents needed to permit the material to enter the destination country and, when necessary, to permit the material to re-enter the U.S.

NOTE: Couriers subject to customs inspection should contact HQ AFCA/WFPC to obtain the necessary customs documentation. Applicable forms issued by the Department of State for this purpose are Form DSP-5, **Application/License for Permanent Export of Unclassified Defense Articles and Related Technical Data**, and Form DSP-73, **Application/License for Temporary Export of Unclassified Defense Articles**.

9. Shipment Notification . Whenever unkeyed CCIs are transported by USPS registered mail or express mail, commercial carriers, and U.S. military or military-contract air service carriers, the shipping activity must provide the intended recipient with advance notification of the impending shipment. This advance notification helps to readily identify any shipment unduly delayed or lost en route. If a shipment of CCIs is not received by the intended recipient within five working days following the expected delivery date, contact the shipping activity. Initiate a tracer action unless there is a valid explanation for the delay. If tracer actions fail to locate the shipment, consider the CCI lost and report the incident in accordance with paragraph 14.

10. Use of Foreign Nationals . **Attachment 2** provides guidance regarding using foreign nationals when transporting unkeyed CCIs in certain specified locations overseas.

11. CCI Accounting Requirements . DIRNSA, in coordination with the developing/producing department or agency (where applicable), determines the minimum accounting requirements for each CCI. **Attachment 4** contains general guidelines used in determining these accounting requirements.

11.1. Centralized Oversight Responsibility.

11.1.1. HQ CPSG at Lackland AFB TX, is designated as the Central CCI Authority. They provide oversight for managing all CCI assets held by the Air Force.

11.1.2. HQ CPSG must ensure all CCI assets belonging to the Air Force are controlled in either the Standard Base Supply System (SBSS) or COMSEC material control system (CMCS). These systems must satisfy the CCI accounting requirements set forth in **Attachment 4**.

11.1.3. Upon request from DIRNSA, the HQ CPSG provides information concerning any CCI asset charged to the Air Force.

11.1.4. HQ CPSG develops procedures to ensure all inventories of CCI assets are conducted in accordance with the requirements in paragraph **12**.

11.2. Local Accounting Responsibilities. Local accounting procedures must be able to readily identify a responsible individual should any CCI become lost or otherwise discovered outside of proper channels, and must reflect the ultimate disposition of each CCI, when appropriate.

11.3. Responsibility for Accounting Functions. Conduct accounting functions by individuals who satisfy the requirements of **Table 1**, Column A.

12. Inventories . Each activity having local accounting responsibility for CCIs must perform a complete physical inventory of its CCI holdings at periodic intervals according to the requirements applicable to the system in which the CCIs are accountable. Perform inventories for CCIs accountable within the CMCS every six months. Perform inventories for CCIs accountable within the SBSS every 12 months. The periodic interval between successive inventories may never exceed 12 months regardless of accounting system. This inventory must include all CCI equipment and uninstalled CCI components. The individual responsible for conducting the inventory (e.g., supply equipment custodian, COMSEC manager, COMSEC responsible officer, etc.) must physically view each CCI. However, this requirement can be waived for those CCIs resident at distant locations provided the REPORTING ACTIVITY has a signed receipt for the material and all information contained on the receipt is current since the last scheduled inventory. Report the results of the inventory, to include any discrepancies, according to applicable procedures relevant to the system in which they are accountable. If unkeyed CCI equipment or uninstalled CCI components cannot be accounted for, report it in accordance with the requirements of AFI 33-212. In addition:

12.1. Inventory all CCIs described in paragraph **A4.2**, by serial number.

12.2. Perform inventories of CCIs at reporting activities whenever there is a change of personnel having local accounting responsibility and whenever so directed by HQ CPSG.

12.3. Only U.S. citizens who require this access to perform their regular duties shall certify the accuracy of inventory reports reflecting CCI assets. The reporting requirements in this instruction are exempt from licensing in accordance with AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.

12.4. HQ CPSG shall determine the need to conduct any reconciliation of records between itself and a reporting activity.

13. Maintenance . Only qualified technicians may maintain CCIs. The requirements of AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*, apply to personnel who perform maintenance on CCIs. However, commanders may authorize certain non-U.S. citizens to perform limited maintenance on unkeyed CCIs when both of the following conditions are satisfied:

13.1. Maintenance is performed in the U.S., its territories and possessions, or in a foreign country as allowed by **Attachment 2**.

13.2. Non-U.S. citizens are granted access in accordance with the guidelines contained in **Table 1**, column B. In addition, these individuals must have successfully completed a NSA-approved limited maintenance training course for the CCI, and appropriately cleared if access to classified information or material is required. **NOTE**: When an unclassified information processing equipment (e.g., Single Channel Ground to Air Radio System [SINCGARS/RT-1523]) contains an integrated CCI component, a non-U.S. citizen who qualifies under the above criteria may perform all levels of maintenance on the host equipment after removal of the CCI component.

14. COMSEC Deviations . Report COMSEC deviations involving unkeyed CCIs according to AFI 33-212.

14.1. A COMSEC deviation report is not required for the loss of a CCI that does not have a cryptographic capability (e.g., certain unkeyed common fill devices; an unclassified host equipment from which an integrated CCI component was removed under authorized conditions; etc.). However, if such a device or equipment is lost and subsequently recovered, inspect the device or equipment for signs of tampering or unauthorized modification. If such signs are present, submit a report in accordance with the requirements of AFI 33-212.

14.2. Report any other deviations involving an unkeyed CCI as a Practice Dangerous to Security (PDS) according to AFI 33-212. PDSs include, but are not limited to, the following types of situations:

14.2.1. Shipping CCIs by means of certified, first or fourth class, parcel post, or insured mail.

14.2.2. Shipping CCIs by a commercial carrier that has not agreed in writing to provide either signature/tally service or electronic tracking service.

14.2.3. Movement of CCIs (e.g., transfer) not accompanied by the proper documentation or the documentation contains significant errors.

14.3. Ensure contractual documents or Memorandums of Understanding/Memorandums of Agreement (MOU/MOA) include instructions for the contractors or vendors to follow for reporting COMSEC incidents and PDSs.

15. Disposition and Emergency Destruction .

15.1. See AFKAG-1 and AFI 33-211 for requirements governing emergency destruction of CCIs.

15.2. Routine destruction of unkeyed CCIs by individual users is NOT AUTHORIZED.

15.3. Process unserviceable/not repairable, or no longer required CCIs for turn-in according to applicable procedures relevant to the system in which they are accountable.

15.4. Return CCIs accountable within the CMCS to the issuing COMSEC manager for return to the depot.

16. Information Collections, Records, and Forms .

16.1. Information Collections. No information collections are created by this publication.

16.2. Records. Retain and dispose of records (paragraph 12.4., A2.10., and A3.2.2.) according to AFMAN 37-139 (will convert to AFMAN 33-322, Volume 4), Table 33-22.

16.3. Forms (Adopted and Prescribed).

16.3.1. Adopted Forms: Department of State Form DSP-5, **Application/License for Permanent Export of Unclassified Defense Articles and Related Technical Data**; DSP-73, **Application/License for Temporary Export of Unclassified Defense Articles**; DD Form 1907, **Signature Tally Record**; and AF Form 847, **Recommendation for Change of Publication**.

16.3.2. Prescribed Forms: No forms are prescribed by this publication.

LESLIE F. KENNE, Lt Gen, USAF
DCS, Warfighting Integration

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

The Paperwork Reduction Act of 1995

AFPD 33-2, *Information Protection*

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Deviations*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information*

AFI 33-360, Volume 2, *Forms Management Program*

AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

NSTISSI 4001, (FOUO) *Controlled Cryptographic Items*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

CCI—Controlled Cryptographic Item

CE—Communications-Electronic

CMCS—COMSEC Material Control System

COMSEC—Communications Security

DCS—Defense Courier Service

DIRNSA—Director, National Security Agency

HQ AFCA—Headquarters, Air Force Communications Agency

HQ CPSG—Headquarters, Cryptologic Systems Group

HQ USAF—Headquarters, United States Air Force

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

NSA—National Security Agency

PDS—Practice Dangerous to Security

SBSS—Standard Base Supply System

U.S.—United States

USPS—United States Postal Service

Terms

Authorized Activities—Responsible to the HQ CPSG either through SBSS or CMCS channels.

Central CCI Authority—HQ CPSG is designated with maintaining oversight and management responsibility for all CCIs charged to the Air Force.

Combined Facility—A property consisting of a structure, building, or a fixed or mobile shelter or platform, occupied and operated by U.S. personnel in conjunction with personnel from one or more allied nations.

Combined Operation—An operation conducted by U.S. personnel in conjunction with personnel from one or more allied nations. These personnel must act together to accomplish a specific mission.

Controlled Cryptographic Item (CCI) Assembly—Device embodying a cryptographic logic or other communications security design approved by NSA as a Controlled Cryptographic Item. It performs the entire communications security function, but depends upon the host equipment to operate.

Controlled Cryptographic Item (CCI) Component—Part of a CCI that does not perform the entire communications security function but depends upon the host equipment, or assembly, to complete and operate the communications security function (see paragraph 2.).

Controlled Cryptographic Item (CCI) Equipment—Telecommunications or information handling equipment embodying a CCI component or assembly and performs the entire communications security function without dependence on host equipment to operate.

Foreign National—A person who is not a natural born or naturalized citizen of the U.S. and who is not categorized as a resident alien.

Integrated CCI Component—A CCI component designed to be incorporated with an otherwise unclassified communication or information processing equipment or system to form a CCI equipment or system. **NOTE:** The integrated CCI component cannot perform any function by itself. It obtains power from the host equipment. An integrated CCI component may take a variety of forms (See paragraph 2.).

Qualified Technician—An individual who satisfies the training requirements of AFI 21-109, and is authorized to perform a specified level of maintenance on CCIs.

Reporting Activity—An activity with accounting responsibility for a specific number of CCIs charged to that activity. Under CMCS channels, the COMSEC manager is responsible. Under SBSS channels, the equipment supply custodian is responsible.

Resident Alien—a citizen of a foreign country, legally residing in the U.S. on a permanent basis, who is not yet a naturalized citizen of the U.S.

Unkeyed—A cryptographic equipment that contains no keying material and has all of its internal key storage registers in a zeroized state.

U.S. 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.

Vendor—A company executing a MOU/MOA with NSA, or with a NSA-authorized government department or agency, for the development, production, sale, installation, or maintenance of a CCI equipment or CCI component.

Attachment 2

CONDITIONS FOR ALLOWING FOREIGN NATIONAL ACCESS TO CCI EQUIPMENT AND CCI COMPONENTS

A2.1. Commanders may authorize certain foreign nationals to have access to CCIs provided such access is granted in accordance with the conditions set forth in this Attachment. These conditions only apply in those foreign countries where the U.S. Government occupies property of the foreign government as a tenant (e.g., a military base, an embassy, a consulate, etc.).

A2.2. Access to Unkeyed CCIs. Irrespective of the release status of the CCI, foreign nationals may be admitted without escort to areas containing installed CCIs when:

A2.2.1. The commander has determined the potential risk of tampering with the CCI is acceptable considering the local threat, vulnerability, and sensitivity of the information being protected; and

A2.2.1.1. Admittance to the area is required in conjunction with building maintenance, custodian duties, or other operational responsibilities normally performed by unescorted foreign nationals before CCI was installed in the area; and

A2.2.1.2. The CCI is installed in a facility either U.S.-controlled or is a COMBINED FACILITY with a permanent daily U.S. presence.

A2.2.2. The applicable Operational Security Doctrine does not specifically prohibit admittance to such areas by unescorted foreign nationals.

A2.3. Access to Keyed CCIs. In addition to satisfying the requirements set forth above, foreign nationals may also be admitted without escort to areas containing keyed CCIs when:

A2.3.1. The foreign national is a civilian employee of the U.S. Government or a military member of the U.S. Armed Forces, or is a foreign national assigned to a combined facility.

A2.3.2. The foreign national holds a security clearance acceptable to the U.S. and is appropriate for the highest classification of the keying material being used.

A2.3.3. The CCI remains the property of the U.S. Government and an employee of the U.S. Government is responsible for the integrity of the CCI. (Follow procedures in paragraph [A2.6](#) if no U.S. Government employee is assigned to the area containing the keyed CCI.)

A2.3.4. The communications being protected are determined essential to the mission of either a U.S. operation or a COMBINED OPERATION.

A2.4. At activities where foreign nationals have unescorted access to keyed CCIs:

A2.4.1. U.S. personnel at distant locations, who are communicating with the CCI equipment at such an activity, must be made aware of the nature of this foreign national access prior to initiating secure communications.

A2.4.2. Only appropriately cleared U.S. personnel will key CCI equipment with U.S.-classified keying material. Submit waivers to this requirement through command COMSEC channels. Only DIRNSA/I41 may grant waivers to this requirement. Authorized foreign nationals may key CCI equipment with classified allied or unclassified (either U.S. or allied) keying material.

A2.5. CCI Equipment Installed in Facilities With No U.S. Presence. Where there is an operational need to install and operate CCI equipment in an unmanned facility in a foreign country or in a facility staffed entirely by foreign nationals, the commander responsible for the CCI equipment must approve the **installation** in advance. The installation must meet requirements set forth in AFKAG-1, AFI 33-211, and this instruction. The CCI equipment must be installed by, and must remain under the control of, authorized U.S. personnel who verify the presence of the CCI equipment at regular intervals. These types of installations shall employ additional security measures (e.g., equipment lock bars, alarms, security containers, etc.) to prevent unauthorized foreign national access to the CCI equipment. For CCI equipment located in facilities with no U.S. presence, following keying requirements in paragraph **A2.4.2**. The commander verifies the continuing need to retain CCI equipment at such facilities at periodic intervals, but not less than once every six months.

A2.6. Use of CCI Equipment in Sensitive Environments. Do not move CCI equipment from an environment where foreign national access was authorized, to a more sensitive environment where the risk is unacceptable. If operational needs require such a move, it must first receive the commander's approval. To ensure no tampering has occurred, a qualified technician must perform an examination of any CCI equipment involved before moving the equipment to the new location. If any evidence of possible or actual tampering is detected, report this fact as a COMSEC incident in accordance with paragraph **14**. Remove the affected CCI equipment from operational use pending disposition instructions from NSA.

A2.7. Handling CCIs at Storage Facilities. Foreign nationals can handle unkeyed CCIs in conjunction with receiving, shipping, and storage duties performed at warehouses or other logistics facilities, provided they are employed by the U.S. government or a U.S. government contractor, and they are under the direct supervision of an individual who satisfies the access requirements of this instruction.

A2.8. Transporting CCIs. Under the following conditions, foreign nationals employed by the U.S. government or a U.S. government contractor may be used to transport unkeyed CCIs that are the property of the U.S. government or a U.S. government contractor or vendor.

A2.8.1. The carrier must use a system providing continuous accountability and custody for the material from pick-up to ultimate destination.

A2.8.2. There must be a constant U.S. presence (e.g., a foreign driver is accompanied by a U.S. person who satisfies the access requirements of the basic instruction); or

A2.8.3. The material must be contained in a closed vehicle or shipping container (e.g., CONEX, dromedary) that has been locked by an individual who satisfies the access requirements of the basic instruction. In addition, the closed vehicle or shipping container must have a high security shipping seal affixed to provide evidence of unauthorized attempts to access the enclosed material.

A2.9. Issuing and Inventory Functions. Foreign nationals employed according to the requirements in paragraph **A2.7**, may also perform the issuing and inventory functions below.

A2.9.1. Foreign nationals may issue CCIs to individuals whose identity and authorization to receive the CCIs was verified by a U.S. government employee at the facility.

A2.9.2. During an inventory conducted according to the requirements in paragraph **12**, foreign nationals may count or read serial numbers of CCIs comprising the shelf stock of the facility.

A2.10. Do not grant foreign nationals access to inventory records, property books, or other documents reflecting total quantities of CCIs within a particular geographic area, or reveal the location of these CCIs outside the warehouse or logistics facility.

A2.11. Installation and Maintenance.

A2.11.1. You can use foreign nationals to install unkeyed CCI equipment provided:

A2.11.1.1. They are directly supervised by a U.S. citizen employed either by the U.S. government or a U.S. government contractor or vendor.

A2.11.1.2. Their access is limited to only the external portion of the CCI equipment. They may not perform any installation functions that require access to internal components of the equipment.

A2.11.2. The commander may allow foreign nationals to perform some maintenance on unkeyed CCI equipment provided all of the following conditions are satisfied. The foreign nationals:

A2.11.2.1. Must be employed by the U.S. government or a U.S. government contractor or vendor.

A2.11.2.2. Must be citizens of the country where the CCI equipment is maintained and was released.

A2.11.2.3. Must successfully complete an NSA-approved limited maintenance training course for the equipment.

A2.11.2.4. Must not require access to classified information or material, or otherwise be appropriately cleared.

A2.11.2.5. Must restrict their maintenance capability to direct replacement of CCI components. Foreign nationals may not perform any repair work on a CCI component or the COMSEC portion of a CCI equipment.

A2.11.3. Whenever foreign nationals perform maintenance of CCI equipment entirely or in part; a qualified technician shall check the equipment prior to returning it to service. This technician must be a U.S. citizen capable of detecting any unauthorized modifications to the CCI equipment or a CCI component thereof.

Attachment 3

CRITERIA FOR SELECTING A COMMERCIAL CARRIER TO TRANSPORT CCI EQUIPMENT AND CCI COMPONENTS

A3.1. CCIs may be transported by any commercial carrier warranting, in writing to the shipping activity, they can satisfy all of the following requirements. The carrier must:

A3.1.1. Be a firm incorporated in the U.S. and provide door-to-door service.

A3.1.2. Guarantee delivery within a reasonable number of days based on the distance traveled.

A3.1.3. Have a means of tracking individual packages within its system to the extent, should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the package's last known location.

A3.1.4. Guarantee the integrity of the vehicle's contents at all time.

A3.1.5. Guarantee the package is afforded a reasonable degree of protection against theft (e.g., use of a security cage, video surveillance, etc.) should it become necessary for the carrier to make a prolonged stop at a carrier terminal.

A3.2. In addition to satisfying the requirements set forth above, the carrier must either:

A3.2.1. Utilize a signature/tally record accurately providing a continuous chain of accountability and custody by each individual who assumes responsibility for the package/shipment while in transit (the carrier may either provide its own signature/tally record form or agree to use DD Form 1907, **Signature Tally Record**); or

A3.2.2. Utilize an electronic tracking system providing a chain of accountability and custody similar to that provided by a manually prepared signature/tally record. Delivery records must show the name of the individual who receipts for the material at the final destination. Information must be available (e.g., a hard-copy printout, a readable computerized database, an "800" telephone number service, etc.) providing those points, during transit, where electronic tracking of the package/shipment occurred.

A3.3. In addition to the foregoing, the shipping activity must ensure documentation accompanying the shipment includes an emergency telephone number of an individual authorized to receipt for the shipment. Include this emergency telephone number in the event the carrier attempts to make delivery during other than normal duty/work hours.

Attachment 4

ACCOUNTING REQUIREMENTS FOR CCI EQUIPMENT AND CCI COMPONENTS

A4.1. All CCIs within the Air Force are reportable to an accounting point designated by HQ CPSG. Minimum accounting requirements for the different categories of CCIs are specified below.

A4.2. Accounting by serial number is required for:

A4.2.1. All CCI equipment designed solely to perform a cryptographic function. This equipment is identified by an external nameplate containing the short title and the serial number of the equipment (e.g., KG-84, KL-43G, KY-57, STU-III, NES).

A4.2.2. Any unclassified information processing equipment serving as a host for an installed integrated CCI component. The integrated CCI component provides the information processing equipment with a cryptographic capability. The host equipment may process voice, data, or record communications. This type of CCI equipment may be identified either by a short title-type nomenclature (e.g., PRC-112A(C), RT-1523(C)/U, etc.) or by its descriptive name (e.g., GRID Model 1117, Secure Network Server, etc.). **NOTE:** Normally the integrated CCI component is embedded within the host equipment and is not readily identifiable by the user. For this reason, use the serial number of the host equipment for accounting purposes. Only qualified technicians are authorized to remove the CCI component from the host equipment.

A4.2.3. Certain CCI modular components (e.g., KGV-46) or microcircuit devices (e.g., MYK-6) where the sensitivity of the CCI or its application warrants separate serial number traceability. Always use the serial number of the CCI component or microcircuit device for accounting purposes even when it is installed in a host equipment. **NOTE:** Whenever CCIs described in the paragraphs above are moved/transferred outside the Air Force; the accompanying shipping documents must reflect the serial number of the CCI equipment, component, or microcircuit device, as appropriate.

A4.3. Accounting by quantity is permitted for:

A4.3.1. Those CCI devices not cryptographic in nature, but performing critical key processing or other ancillary functions (e.g., certain common fill devices).

A4.3.2. Uninstalled or spare CCI components intended for use in equipment described in paragraph [A4.2.2](#). Separate accounting is not required for components installed in a host equipment since these components are included as part of the larger CCI configuration (see paragraph [4](#)).

A4.4. When a host equipment contains an integrated CCI component (see paragraphs [A4.2.2](#) and [A4.2.3](#)), recommend affixing a label to the host equipment to identify it as a CCI. In addition, this label may also reflect identifying information regarding the integrated CCI component.

A4.5. Never open CCI equipment for the sole purpose of verifying the presence of any integrated CCI component.

A4.6. As an exception to the accounting requirements set forth in paragraph [A4.2](#), the following only applies to CCIs operating in an airborne environment or as part of a major weapons or communica-

tions-electronics (CE) system. This exception notwithstanding, the accounting system must still be able to trace each CCI equipment by its serial number.

A4.6.1. Account for CCIs installed as part of a weapons/CE system or onboard an aircraft as part of the overall weapons/CE system or as part of the aircraft mainframe.

A4.6.2. Account for CCIs retained solely for direct replacement of like CCIs installed in configurations described in paragraph [A4.6.1](#), by quantity upon authorization from HQ CPSG.

Attachment 5**MODIFIED REQUIREMENTS FOR CCI EQUIPMENT AND CCI COMPONENTS
USED TO SUPPORT NETWORK SECURITY SYSTEMS**

A5.1. The control requirements set forth in paragraphs 4. and **Attachment 2** are designed for CCIs used to protect communications processed by traditional national security telecommunications systems. However, when using CCIs to provide network security for automated information systems, commanders may choose to follow the alternative guidelines set forth in this Attachment.

A5.2. Network Security Oversight Responsibilities. The individual or activity designated as having network security oversight:

A5.2.1. May be designated to ensure the proper reporting of COMSEC incidents involving CCI assets associated with the network.

A5.2.2. May be tasked with ensuring appropriate corrective actions are taken with respect to any COMSEC incident considered a PDS.

A5.3. Administrative Oversight Responsibilities. The individual or activity designated as having administrative oversight for the network:

A5.3.1. May be responsible for local accounting and inventory of CCI assets associated with the network.

A5.3.2. May be tasked with reporting certain information to one or more central CCI authorities depending on the network configuration.