DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
3800 NORTH CAMP CREEK PARKWAY SW
ATLANTA, GEORGIA 30331-5099
1 April 1997

USARC Regulation 380-4

Security

CONTROLLED CRYPTOGRAPHIC ITEM (CCI)

History. This is the initial publication of USARC Regulation 380-1.

Summary. This regulation provides the physical security standards and procedures to protect "**keyed"** or "**unkeyed"** CCI within the United States Army Reserve Command (USARC). The most common CCI held within the USAR is the Secure Telephone Unit, Third Generation (STU-III). Activity property book officers (PBO) have a complete inventory listing of CCI material/equipment currently held.

Applicability. This regulation applies to Headquarters, U.S. Army Reserve Command (USARC) and its Major Subordinate Commands (MSC), Direct Reporting Units (DRU) and subordinate units that are users of CCI. Local reproduction is authorized.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, Intelligence (DCSINT). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation.

Supplementation. Supplementation of this regulation is prohibited without prior approval from Commander, USARC, ATTN: AFRC-IN, 3800 North Camp Creek Parkway SW, Atlanta, GA 30331-5099.

DISTRIBUTION: A

Interim changes. Interim changes to this regulation are not official unless authenticated by the Deputy Chief of Staff, Information Management (DCSIM). Users will destroy interim changes on their expiration date unless superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Commander, USARC, ATTN: AFRC-IN, 3800 North Camp Creek Parkway SW, Atlanta, GA 30331-5099.

FOR THE COMMANDER:

ZANNIE O. SMITH
Brigadier General
Chief of Staff

OFFICIAL:

SIGNED
CAROLYN E. RUSSELL
Colonel, GS
Deputy Chief of Staff,
Information Management

CONTENTS *(Listed by paragraph number)*

Chapter 1
General

1-1. Purpose
This regulation standardizes the most critical requirements associated with the protection of CCI to ensure each USAR user is familiar with procedures for the use, control, and protection of CCI. It does not convey all requirements. Command/activity/unit USAR security managers are the designated monitors of CCI within their respective areas of operation. They are responsible for advising the activity property book officer (PBO), the communications security (COMSEC) officer, and the provost marshal (PMO) of any lost CCI or incidents involving CCI.

1-2. References

Required and related publications are listed in appendix A.

1-3. Explanation of abbreviations and terms
Abbreviations and terms used in this regulation are explained in the glossary.

1-4 Responsibilities

a. Overall responsibility for protection of CCI rests with each USAR user of CCI. The intent of this regulation is to assist both military and civilian users in executing this responsibility.

b. All assigned USAR personnel will protect CCI against loss, theft, sabotage, tampering, or unauthorized access. Personnel with access to CCI, key, operating instructions, and other sensitive or classified COMSEC materials will ensure that insecurities involving these materials are reported in accordance with DA Pamphlet 25-380-2. *[**NOTE**: Protection of CCI and COMSEC material is paramount over other considerations within a unit due to the highly damaging effects that compromised communications can produce, such as loss of life and negative impact on a unit's mission.]*

Chapter 2
Security

2-1. Access control
For clarity, “access” denotes the opportunity to obtain detailed knowledge through uncontrolled physical possession. External viewing of and "Controlled Proximity" to **unkeyed** CCI **does not** constitute access. The primary goal is to protect the cryptologic within CCI or its components. The cryptographic logic may be the hardware circuitry and key that converts information to or from an unintelligible form. The logic may also be determined from technical drawings, schematics and other technical literature.

a. **Keyed** CCI will be handled only by properly cleared personnel.

b. **Unkeyed** CCI may be handled by uncleared personnel who meet one of the following criteria:

(1) U.S. Citizen.

(2) Permanently admitted resident alien who is a U.S. Government employee, or Active or Reserve member of the armed forces.

(3) Foreign national (military or civilian) employed by his/her respective government, provided access is restricted specifically to the CCI for which formal release has been granted.

(4) Non-U. S. Citizen employed by or in support of the U.S. Government, including U.S. commercial carriers, provided there is a constant U.S. presence or the CCI is packaged in an adequately protected container.

2-2. Control and handling of CCI
This regulation contains procedures for protecting **keyed/unkeyed** CCI and prevent tampering. Tampering is any unauthorized modification that alters the function of CCI to degrade the security it provide**s.** Only approved maintenance activities will disassemble CCI equipment and disturb its security integrity.

a. Control. CCI is unclassified, but access control of CCI is essential to assure users of its functional integrity. Enforcing proper handling and access controls during the use, repair, transport, storage, and disposition of CCI, will prevent or deter attempts to degrade functional integrity through tampering.

b. When there is no chance or opportunity for viewing of cryptovariables, tampering, or internal examination exist, then no restrictions are imposed upon external viewing or other exposure involving CCI.

c. Handling. When **unkeyed**, CCI equipment and components are unclassified, but must be controlled against espionage, tampering, and loss. The relaxed controls on CCI are intended to promote their expanded, flexible use while saving resources. CCI equipment, components, and fill devices will bear the designator "Controlled Cryptographic Item” or "CCI” to alert the user to execute the controls required by this regulation. A component may be a CCI circuit board, modular assembly, microcircuit, or a combination of these items.

d. Users will protect **keyed** CCI in accordance with requirements in AR 380-40 and TB 380-41**. Keyed** CCI denotes that it contains a sequence of random binary digits **(key)** used to encrypt or decrypt electronic signals. Protection of CCI when **keyed** must be consistent with the classification of the key it contains.

e. Keying material is often referred to simply as “**key**.” Some COMSEC equipment has the capability for electronic entry and dissemination of key (e.g., KY-57), while other equipment requires manual entry of the key (e.g., KW-7 and KG-27). *[**NOTE**: The CCI may be in two operational states, **keyed and unkeyed.** It is only when **unkeyed** (or when unclassified key is used) that CCI is unclassified.]*

2-3. Accountability

a. Accountability of CCI goes hand in hand in the handling of CCI. Users must apply the following procedures for positive control and accountability:

(1) Account for CCI End Items (Class VII) by serial number.

(2) Common fill devices (Class VII) are the only items tracked locally by quantity, **not** by serial number.

(3) Account for uninstalled CCI components (Class IX) by quantity.

(4) Account for lost/damaged CCI in accordance with AR 735-5.

b. Logistics supply procedures at command levels provide for--

(1) Accountability down to individual CCI users.

(2) End-to-end audit trail of transactions.

(3) Quarterly inventory of CCI.

(4) End items accountable by serial number.

(5) Uninstalled components (accountable by quantity).

2-4. Storage of CCI

a. Storage denotes the state of CCI when it is not in use by, in the physical possession of, or continuously attended by an authorized person where its adequate protection is assumed.

b. Users must store **unkeyed** CCI under the "**double-barrier"** protection rules (meaning two separate physical containment structures) to deter unauthorized access to the degree required by AR 190-51.

c. Examples of double-barrier protection are--

(1) A locked wall locker inside a locked room.

(2) **Unkeyed** CCI secured inside a vehicle that is locked with a padlock and inside a motor pool, or inside a chain-link fence, that is secured at night or when unoccupied. *[**NOTE:** Doors of tracked vehicles and vans with installed CCI must be locked by a series 200 padlock (NSN 534000-158-3805) or a series 5200 padlock (NSN 5340-00-158-3807)]*.

d. Each USAR activity having any CCI will prepare a regulation or a numbered publication memorandum.

e. Where there is limited storage space for **unkeyed** CCI within a USAR activity, the activity commander (under the authority of AR 190-51 and USARC Pamphlet 190-1) may authorize, in writing, storage of **unkeyed** CCI within an arms vault/room. The CCI double-barrier protection rule must be in place and storage area should be constructed as a separate, locked cage or container within the arms vault/room.

2-5. Relocating CCI

The activity commander may approve the reloaction of CCI used in an office environment or other fixed location whenever there is an operational need. Before moving the CCI, a knowledgeable person must check the CCI for possible tampering and report any findings. That individual will prepare an access discrepancy report under the provisions of DA Pamphlet 25-380-2, appendix B, if the CCI in question shows signs of tampering. The device will not be used pending disposition instructions from NSA.

2-6. Protection of unattended CCI

a. Prior to selecting physical and security protection measures for any unattended CCI, the activity/unit commander must initiate a risk assessment for review by the unit/command PMO (per provisions of AR 190-51). Protection measures must be the same as afforded to protect other unclassified, sensitive, high value equipment in the same environment. Unattended and uninstalled CCI is considered to be in storage when it is in logistics channels.

b. Unattended CCI installed in a fixed location, or in a mobile or transportable configuration, are not considered to be in storage.

2-7. Shipment of CCI

The responsibility for shipment of CCI from any USAR activity rest with the activity/unit PBO. The PBO must prepare the CCI for shipment as follows:

a. A shipment of CCI requires only one wrapper.

b. Packages must be clearly marked outside with **"CCI"** in 2-inch letters.

c. All transaction documents must also reflect the CCI designation and any other markings required to facilitate processing during shipment.

d. Each shipment of CCI will contain a shipping document or record as required to effect transaction accounting and maintain an audit trail; e.g., DD Form 1348-1.

2-8. Shipping methods

a. The PBOs will ensure only authorized shipping methods are used for CCI and that each package is under the DOD constant surveillance service (CSS) procedure for protection purposes.

b**.** The following are authorized means of shipping CCI:

(1) U.S. Postal Service registered mail.

(2) U.S. military, military-contractor, or private air service.

(3) U.S. Diplomatic Courier Service.

2-9. Restrictions

a. When shipping CCI, the shipper must ensure--

(1) Batteries are removed from CCI prior to shipment.

(2) "Zeroization" of CCI equipment is completed prior to shipment.

(3) CCI is not transported in privately-owned vehicles.

b**.** Packaging of CCI for shipment.

(1) Shippers will package CCI in a sturdy metal, wood, fiberboard, or heavy duty cardboard container suitably constructed to prevent damage or undetectable examination of the contents.

(2) Shipments of small or fragile CCI components will be packaged to reduce susceptibility to loss or damage, and to prevent detectable tampering or opening.

2-10. Disposition of CCI

a. Users will obtain disposition instructions for excess CCI from the USAR activity PBO, who will coordinate disposition actions with his/her supporting supply activity or wholesale supply source.

b. The activity/unit PBO will retrograde non-repairable CCI under routine automatic-return-item procedures. (See AR 710-1 for guidance.) *[**NOTE:** National Security Agency (NSA) is the central destruction facility for integrated circuits designated CCI.]*

2-11. Emergency protection for CCI

a. Users must continue protection of CCI to the fullest during any emergency, such as:

(1) Fire or flood.

(2) Civil disturbances.

(3) Hostile actions or terrorist attack.

b. This protection must continue through either evacuation or secure storage during any natural disasters.

c. When civil disturbances or hostile actions are involved, protection of CCI must continue through evacuation or destruction.

d. Each unit/activity must have a regulation or numbered publication memorandum outlining procedures to follow during an emergency situation. It will include the following:

(1) Authority for the U.S. person in charge to implement the procedures.

(2) Specific locations of all CCI material.

(3) An outline of specific destruction responsibilities.

(4) Locations of workable destruction devices.

(5) Local procedural instructions to remove and destroy installed/spare components designated as CCI before actually destroying other installed and spare unclassified components.

(6) Detailed instructions for recovering lost or abandoned CCI.

(7) The requirement to complete a post-emergency inventory of CCI.

(8) Instructions and examples of any required reports as directed by DA Pamphlet 25-380-2.

2-12. Maintenance of CCI

a. The U.S. Army Communications Command Security Logistic Activity's (USACCSLA's) current policy is to only replace CCI/STU-III(s) with a turn-in CCI. Any individual turning in a STU-III or other CCI must notify their activity USAR PBO prior to turning in the item.

b. Users will turn in any CCI that needs repair to the property book officer (PBO) for coordination in shipping the equipment to the maintenance depot at Tobyhanna Army Depot (TYAD). Shipping documents for turn-in of CCI equipment must reflect a valid DOD Activity Address Code (DODAAC) to confirm the shipper is authorized to turn in CCI to TYAD. Any CCI equipment turned in for repair must have all accompanying components shipped with it; e.g., manuals and power supplies. If the shipment is not complete, a shortage list signed by either the unit commander or PBO must be attached to the turn-in document.

c. Requisition/replacement of CCI (specifically, for STU-III equipment) is very restricted, primarily due to severe limitations of wholesale procurement funds for purchase of secure STU-IIIs.

Chapter 3
Access Discrepancy/Incident Reporting

3-1. General

a. Users will report any CCI incident, physical loss, and/or loss of access control under unknown or unexplainable circumstances in accordance with DA Pamphlet 25-380-2.

b. Minor lapses in CCI control procedures, where unauthorized access is improbable, only requires local reporting, as a matter of administrative procedure.

c. Commanders should consider disciplinary action against any person who knows of and fails to report a possible access discrepancy/incident.

3-2. Types of reportable discrepancies/incidents

a. Physical loss of CCI.

b. Discrepancies of inventory between an activity's accountable property record and a physical inventory count.

c. Losses of control which leads to probable loss of access control.

d. Any unauthorized release of CCI or deliberate falsification of control documents.

e. Any CCI not on accountable records and turned-in as "found on installation."

3-3. Discrepancies/incident reports

Reports are official correspondence which the USAR activity Security Manager should prepare for **unkeyed** CCI discrepancies/incidents, with an information copy to the activity PMO. When the incident involves **keyed** CCI, the USAR activity COMSEC Officer must prepare the report. Reports may be forwarded by message or memorandum. The two types of required reports are:

a. **Initial report.** This report is required for all discrepancies/incidents.

b. **Final report.** When all required information is not given in the initial report, then a final report will be required.

*[**NOTE:** The initial report may be considered as the final report if all pertinent information is submitted in the initial report.]*

3-4. Classification of reports
Under normal conditions, reports are prepared as **UNCLASSIFIED, FOR OFFICIAL USE ONLY (FOUO);** however, the originator should examine **all** information before making a determination on the classification. This will mainly ensure that no classified information is included in the report, otherwise the report must be classified at a minimum of **CONFIDENTIAL**. Classification guidance for CCI information is in DA Pamphlet 25-380-2, table B-1. Distribution of reports will only be internal, on a need-to-know basis.

3-5. Routing of reports

a. Routing of USAR CCI discrepancy/incident reports involving **unkeyed** or **keyed** CCI will be routed as follows:

ACTION ADDRESSEE(S)
DIRNSA FT GEORGE G MEADE MD//V5 1A//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-KP-IN//

INFORMATION ADDRESSEE(S)
CDRFORSCOM FT MCPHERSON GA//AFIN-IS//
CDRUSARC FT MCPHERSON GA//AFRC-INS/IMO-T/PRM//
OTHER APPROPRIATE COMMAND CHANNELS

b. When a discovered discrepancy/incident reveals that the CCI was **keyed** with cryptographic key, the USAR activity COMSEC account custodian or security manager will telephonically notify the HQ, USARC, COMSEC Officer (DCSIM), COMSEC Program Manager, and PMO. This procedure will assist USAR activities in properly reporting incidents and ensuring proper agencies/chain of command are addressed in the report.

c. In the event the preparer of the incident report cannot contact a HQ, USARC representative, as stated in paragraph 3-5b above, they should contact the USACCSLA COMSEC incident monitoring office, Fort Huachuca, AZ for assistance at commercial (520) 538-8189.

3-6. Report contents/format
The message format for preparing a CCI discrepancy/ incident report is in appendix B (RCS exempt, AR 335-15, para 5-2e(2)).

Appendix A
References

Section I
Required publications

AR 190-51 (Security of Army Property at Unit and Installation Level). Cited in para 2-4.
AR 380-40 (Policy for Safeguarding and Controlling Communications Security (COMSEC) Material). Cited in para 2-2d.
AR 710-1 (Centralized Inventory Management of the Army Supply System). Cited in para 2-10b.
AR 735-5 (Policies and Procedures for Property Accountability). Cited in para 2-3a(4).
DA Pam 25-380-2 (Security Procedures for Controlled Cryptographic Item (CCI)). Cited in paras 1-4b, 2-5, 3-1a, 3-4.
TB 380-41 (Security Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material). Cited in para 2-2d.

Section II
Related publications

AR 15-6 (Procedure for Investigating Officer and Boards of Officers)
AR 380-5 (Department of the Army Information Security Program)
AR 380-19 (Information System Security)
AR 380-19-1 ((C) Control of Compromising Emanations (U))
AR 710-2 (Supply Policy Below the Wholesale Level)
DA Pam 25-16 (Security Procedures for the Secure Telephone Unit, Third Generation (STU-III))
USARC Reg 380-3 (Safeguarding and Control of Communications Security (COMSEC) Material)
USARC Reg 380-6 (Secure Telephone Unit-Third Generation (STU-III))
USARC Pam 190-1 (Physical Security)

Appendix B
Message Format For CCI Discrepancy/COMSEC Incident Report

FROM: REPORTING ORGANIZATION
ACTION: DIRNSA FT GEORGE G MEADE MD//V5 IA//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-KP-IN//
INFORMATION: CDRFORSCOM FT MCPHERSON GA//AFIN-IS//
CDRUSARC FT MCPHERSON GA//AFRC-INS/AFRC-IMO-T/PRM//
OTHER APPROPRIATE COMMAND CHANNELS
BT
UNCLAS E F T 0 (**CLASSIFICATION BASED UPON CONTENT**)
SUBJECT: INITIAL/FINAL CCI DISCREPANCY/COMSEC INCIDENT REPORT
(**NOTE: DEPENDING UPON WHETHER CCI WAS KEYED OR UNKEYED WILL DETERMINE WHAT INFORMATION MUST BE REFLECTED. ENTER INFORMATION AS APPLICABLE TO DISCOVERED INCIDENT.)**
A. AR 380-40, CHAPTER 7
B. TB 380-41, PARAGRAPH 5.28.12
C. DA PAM 25-380-2
1. COMSEC ACCOUNT NUMBER (**IF CCI KEYED**)
UIC AND DODAAC OF THE UNIT INVOLVED: (**IF UNKEYED/LOST/STOLEN**)
2. CCI IDENTIFICATION:
A. NOMENCLATURE
B. SERIAL NUMBER:
C. QUANTITY:
D. NATIONAL STOCK NUMBER (NSN):
E. OWNING UNIT OF CCI (PROPERTY BOOK):
F. KEYED OR UNKEYED CCI:
3. BRIEF INCIDENT DESCRIPTION: THE DATE AND TIME OF DISCOVERY, AS APPROPRIATE; IDENTIFICATION (NAME, SSN, RANK/GRADE, POSITION, ETC.) OF PERSONS WHO HAD ACCESS TO THE ITEM; **ANSWER TO QUESTIONS "WHO?, WHAT?, WHEN?, WHERE?, WHY?, AND HOW?"** CATEGORIES TO GIVE CLEAR PICTURE OF THE OCCURRENCE.
4. POINT OF CONTACT: GIVE NAME, TELEPHONE NUMBERS, FAX NUMBER.
5. FINAL REPORT: (**TO BE SUBMITTED ONLY IF ALL INFORMATION IS NOT INCLUDED IN INITIAL REPORT**). IF REQUIRED, GIVE THE FOLLOWING:
A. A SUMMARY OF THE RESULTS OF ALL INQUIRIES AND INVESTIGATIONS.
B. REFLECT THE CORRECTIVE MEASURES TAKEN OR PLANNED TO PREVENT A RECURRENCE.
C. EVALUATION BY LOCAL SECURITY MANAGER OF THE ACCESS DISCREPANCY WITH AN ASSESSMENT AS TO WHETHER UNAUTHORIZED ACCESS IS CONSIDERED IMPOSSIBLE, IMPROBABLE, POSSIBLE, PROBABLE, OR CERTAIN.
BT

Glossary

Section I
Abbreviations

CCI ..... controlled cryptographic item
COMSEC ..... communications security
CSS ..... constant surveillance service
HQ ..... headquarters
NSA ..... National Security Agency
DOD ..... Department of Defense
DODAAC ..... DOD activity address code
FORSCOM ..... U.S. Army Forces Command
FOUO ..... For Official Use Only
NSN ..... national stock number
PBO ..... property book officer
PMO ..... provost marshal office
POC ..... point of contact
STU-III ..... Secure Telephone Unit, Third Generation
SOP ..... standing operating procedure
SSN ..... social security number
TYAD ..... Tobyhanna Army Depot
UIC ..... unit identification code
USACCSLA ..... United States Army Communications Command, Security Logistic Activity
USARC ..... U.S. Army Reserve Command

Section II
Terms

Access
The capability and opportunity to obtain detailed knowledge through authorized physical possession. Handling, external viewing of, and controlled proximity to CCI does not constitute access.

Access discrepancy
Known or suspected access to CCI by unauthorized persons. An access discrepancy may result in a COMSEC incident.

CCI designated assembly
A device which embodies a cryptographic logic or other COMSEC design which performs the entire COMSEC function, but depends upon the host equipment for its function.

CCI designated component
A device which embodies a cryptographic logic or other COMSEC design which does not perform the entire COMSEC function. It is dependent upon the host equipment or assembly for its function or to complete the COMSEC function.

CCI designed equipment
Telecommunications or information-handling equipment which embodies a CCI-designated assembly **or** component, and which performs the entire COMSEC function without dependence on a host equipment to function.

COMSEC incident (formerly COMSEC insecurity)
Any occurrence which jeopardizes the access control of COMSEC material.

Controlled cryptographic items (CCI)
An unclassified COMSEC equipment, assembly, or component which embodies classified cryptographic logic and is approved by NSA for safeguarding classified information or authenticating identification Friend or Foe signals.

Cryptographic logic
A deterministic logic by which information may be concerted to an unintelligible form and reconverted to an intelligible form. Logic may take the form of engineering drawings, schematics, hardware, or firmware circuitry.

Foreign national
A person who is not native to, or naturalized in, the United States, and who is not categorized as a U.S. resident alien.

Government installation or facility
A U.S. Government-owned or leased commercial facility in a fixed location. This includes the facility's building, building equipment, and subsidiary facilities such as perimeter fencing. A commercial facility, when wholly or partially leased, is considered to be a Government installation.

Handling
Controlled physical possession of CCI by persons who require possession in the performance of their duties, but who do not require, or are not authorized access. Giving the option to handle CCI assumes that the risk of persons gaining detailed knowledge is acceptable.

Mobile configuration
Capable of being moved from one location to another and configured for operations while in motion.

Physical protective measures
Permanent structural safeguards such as walls and fences, and physical security equipment such as surveillance system. (See AR 190-51.)

Security procedures
Measures which include administrative actions involving the workforce which can usually be changed immediately, such as security checks. (See AR 190-51.)

Tampering
An unauthorized modification which alters the proper functioning of an equipment and degrades the security the equipment is designed to provide. Tampering includes unauthorized alteration, attachment or removal of parts, and the unauthorized extraction of the cryptokey using probes or bugs.

U.S. resident alien
A citizen of a foreign country who is legally residing in the United States on a permanent basis.

U.S. military presence
Two or more U.S. military installations in a country other than the United States, its territories and possessions, where U.S. military personnel are stationed.