

Security  
SECURITY PROCEDURES FOR CONTROLLED CRYPTOGRAPHIC ITEMS (CCI)

---

**SUMMARY.** This regulation explains the procedures for protecting UNKEYED CCI.

**APPLICABILITY.** This regulation applies to Army activities, units, and tenant agencies assigned or attached to III Corps and Fort Hood

**INTERIM CHANGES.** Interim changes to this regulation are not official unless they are authenticated by the Directorate of Information Management (DOIM). Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

**SUPPLEMENTATION.** Supplementation of this regulation is prohibited without prior approval from the Directorate of Counterintelligence and Security (DCIS), formerly the Directorate of Security (DSEC).

**SUGGESTED IMPROVEMENTS.** The proponent of this regulation is DCIS, III Corps and Fort Hood. Users are invited to send comments and suggested improvements to Headquarters, III Corps and Fort Hood, ATTN: AFZF-DS-S, Fort Hood, Texas 76544-5056.

---

OVERVIEW

	1
Purpose	1a
References	
	AR 190-51, Security of Army Property at Unit and Installation Level
	AR 380-40, Policy for Safeguarding and Controlling Communication Security (COMSEC) Material
	AR 735-5, Policies and Procedures for Property Accountability
	AFZF-DS-S memo, subject: Security Oversight for Controlled Cryptographic Items (CCI), 6 April 1992
	DA Pam 25-380-2, Security Procedures for Controlled Cryptographic Items
	FH Circular 380-92-3, Schedule of Security Inspections
	TB 380-41-3, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material, Vol 3, Accounting and Reporting Procedures
	TB 380-41-5, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material, Vol 5, Safeguarding COMSEC Material

---

(continued on next page)

References  
(cont)

Forms

DA Form 3964, Classified Document Accountability Record  
DA Form 5504, Maintenance Request

DD Form 173/1, Joint Message Form  
DD Form 1348-1, DOD Single Line Item Release/Receipt Document

SF 701, Activity Security Checklist

1b

Abbreviations

Abbreviations used in this regulation are explained in the glossary.

1c

General

This regulation

- directs the procedures for protecting UNKEYED CCI and
- standardizes the most critical procedures in the areas of
  - safeguarding,
  - handling,
  - accounting,
  - storage,
  - use,
  - maintenance, and
  - incidents.

CCI equipment and components are UNCLASSIFIED when UNKEYED but must still be controlled to protect against

- espionage,
- tampering, and
- loss.

The relaxed controls on CCI are to promote expanded, flexible use while saving resources.

CCI equipment, components, and fill devices will bear the designator "Controlled Cryptographic Item" or "CCI" which alerts the user to protect and safeguard items.

A component may be a CCI

- circuit board,
- modular assembly,
- microcircuit, or
- a combination of these items.

1d

Tampering

Tampering is ANY unauthorized modification altering the function of CCI to degrade the security it provides.

Only approved maintenance activities may disassemble CCI equipment and disturb its security integrity.

1e

RESPONSIBILITIES

2

Commanders Commanders have overall responsibility for protection of CCI.

CCI will be protected against

- loss,
- theft,
- sabotage,
- tampering, or
- unauthorized access.

Personnel with access to CCI, key, operating instructions, and other sensitive or classified COMSEC materials are personally responsible for ensuring that security incidents involving these materials are reported in accordance with (IAW) block 9.

2a

ACCESS CONTROL

3

Definition Access denotes the opportunity to obtain detailed knowledge through physical possession.

External viewing of and “controlled proximity” to UNKEYED CCI does not constitute access.

3a

Goal The goal is to protect the cryptologic within CCI or CCI components.

3b

Logic 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.

3c

Authorized Personnel UNKEYED CCI may be handled by personnel meeting one of the following requirements (provided they have a legitimate need-to-know and their duties require that access)

- US citizens who are US Government employees or are employed in support of the US Government.
- US resident aliens who are US Government employees, members of the US Armed Forces (either active or reserve), and US Government contractor employees.
- foreign nationals (military or civilian) employed by their respective governments, provided access is restricted specifically to CCI for which formal release has been granted to their respective governments.

3d

CCI MAINTENANCE

4

Guidelines

Guidelines for access by maintenance personnel and access to maintenance work areas are

- a responsible maintenance supervisor will have a security SOP for limiting the handling of or access to CCI which is in for repair (the SOP will include the need for CCI to be "ZEROIZED" before it is accepted for repair).
- US citizens, who are authorized access after completing an NSA approved training course or certified under AR 640-15, may perform any level of maintenance for which they have been trained.
- foreign nationals employed by or in support of the US Government, either continental United States (CONUS) or outside continental United States (OCONUS) or its territories and possessions who have completed an NSA approved training course on the equipment or on the equipment's crypto-components, may perform limited maintenance when they are
  - a citizen of a nation to which the equipment has been released,
  - supervised by a US citizen authorized to have access and to perform maintenance.
  - given limited access authorization (LAA) when they need access to classified COMSEC information to perform their jobs.

4a

Storage

Storage and use of classified CCI manuals will meet AR 380-5 requirements.

4b

CCI EMERGENCY PLANS

5

General

Procedures for ensuring access control of CCI during emergencies (natural disasters and hostile actions) at Fort Hood will be the same as for COMSEC materials.

Units will prepare emergency plans to protect CCI against any emergency caused by

- natural disasters, such as a fire or flood;
- civil disturbances, such as mob action;
- or hostile actions, such as enemy or terrorist attack.

5a

Natural Disaster

During natural disasters, protection will continue through evacuation or secure storage.

5b

Civil Disturbance

During civil disturbances and hostile actions, protection continues through evacuation or destruction.

5c

- 
- Procedures      Emergency procedures must be detailed in writing and provide
- authority for the US person in charge to implement the procedures.
  - locations of all CCI material.
  - specific destruction responsibilities.
  - locations of destruction devices.
  - instructions to remove and destroy installed and spare components designated as CCI before destroying other installed and spare unclassified components.
  - instructions for recovering lost or abandoned CCI.
  - instructions for a post emergency inventory of CCI.

5d

---

## ACCOUNTABILITY

6

- 
- Procedures      Account for CCI End Items (Class VII) by serial number.
- Common fill devices (Class VII) are the only items not tracked locally by serial number, but by quantity.
- Account for uninstalled CCI components (Class IX) by quantity.
- Procedures under AR 710-2 provide for the identification of lost CCI.
- The manual supply procedures at Fort Hood provide for
- accountability down to individual CCI users.
  - end-to-end audit trail of transactions.
  - quarterly inventory of CCI.
  - end items accountable by serial number.
  - uninstalled components (accountable by quantity).
- Primary hand receipt holders record serial numbers of all common fill devices (the primary hand receipt holder hand receipts each common fill device to the user by serial number).
- Inventory CCI sensitive items quarterly IAW AR 710-2.
- When CCI cannot be accounted for under these supply procedures, an Incident Report must be generated.

6a

Unserviceable  
CCI/Turned  
In/Shipped

Unserviceable CCI or CCI to be turned in/shipped is taken to the designated direct support unit (DSU) or Directorate of Logistics (DOL) COMSEC Maintenance, building 4617, with a DA Form 5504, for technical inspection and to ensure equipment is zeroized.

DCIS will provide each DSU and the COMSEC Maintenance Division a pre-inked stamp to be used on the DA Form 5504.

In the technical inspection process, unserviceable CCI or CCI to be turned in/shipped are zeroized and, whenever practicable, the fill batteries are removed.

When the technical inspection is completed, the DA Form 5504 is

- stamped,
- dated, and
- initialed by the authorized inspector.

Unserviceable CCI or CCI to be turned in/shipped will be returned to the unit for turn-in.

The unit will take unserviceable CCI or CCI to be turned in/shipped to the Security Warehouse, building 90031, West Fort Hood, for turn in/shipment within 72 hours.

This warehouse is the ONLY authorized turn-in point for accountable CCI.

CCI will not be accepted at the warehouse

- without the “stamp” on the DA Form 5504 or
- after the 72-hour time frame.

NOTE: The only exception to this rule is for “Installation” STU-III telephones which will be turned in to DOL Installation Property Book Office, building 4630, 287-3490. These STU-IIIs must also have the stamped DD Form 5504 and be turned in within the 72-hour time frame.

CCI not turned in to the security warehouse or to DOL Property Book Office within 72 hours will be reinspected by the support unit to ensure it is still “zeroized.”

6b

CCI STORAGE

7

General

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.

UNKEYED CCI will be stored under the DOUBLE-BARRIER protection rules.

Each unit and activity at Fort Hood will publish by SOP the units in-place “double-barrier protection,” specifying specific locations where personnel may use storage facilities.

CCI will not be stored inside arms rooms because personnel who have access to weapons may not meet CCI access requirements.

(continued on next page)

---

General (cont) “Double-barrier protection” denotes two separate physical containment structures which deter unauthorized access to the degree required by AR 190-51, paragraph 3-6.

The following are examples of double-barrier protection

- a locked wall locker inside a locked room.
- UNKEYED CCI locked in a vehicle by a padlock with the radio secured by a chain inside a motor pool or inside a chain link fence secured at night or when unoccupied.
- UNKEYED CCI locked in a tracked vehicle with the tracked vehicle locked.

CCI may be stored locked in its operational configuration; there must be a second barrier such as a motor pool fence to comply with the double-barrier rule or a roving guard at least every 2 hours for security checks.

The preferred method of storage of UNKEYED CCI at Fort Hood is in an operational configuration that meets double-barrier protection requirements such as in

- aircraft,
- vehicles,
- vans, or
- buildings.

Doors to tracked vehicles and vans with installed CCI will be locked by

- a series 200 padlock, national stock number (NSN) 5340-00-158-3805 or
- a series 5200 padlock, NSN 5340-00-158-3807.

CCI storage security requirements for vehicles that lack manufacturer installed locking devices are

- vehicles without door locks or ignition key locks, with CCI in the operational mode (UNKEYED), parked in the motor pool after duty hours.
  - CCI equipment will be stored in the mounted rack and secured with a series 200 padlock.
  - motor pool will be bound by a perimeter fence or barrier meeting the standards outlined in AR 190-51, appendix E, and gates and openings closed and locked.
  - vehicle parking areas will be lighted within the motor pool.
  - each vehicle will be secured with an approved locking device (such as, activate manufacturer installed ignition locking device or immobilize steering wheel with a chain and series 200 padlock).
  - remove easily accessible or exposed equipment or items that are not securable and subject to theft.
  - where the above criteria cannot be met, dedicated guard personnel will be used.

---

(continued on next page)

General (cont)

- vehicles without door locks or ignition key locks parked outside the motor pool during duty hours with CCI in the operational mode (UNKEYED).
  - CCI equipment will be secured in the mounted rack with a series 200 padlock.
  - activate manufacturer installed locking device (ignition key) or immobilize steering wheel with a security chain and series 200 padlock.
  - a security check should be conducted on each vehicle not less than once every 2 hours by the driver or other responsible person.
  - the vehicle will be returned to the motor pool and secured when no longer operationally needed.
  - M880 and M1000 series vehicles will not only activate manufacturer door and ignition locking devices but will also secure the steering wheel with a chain and series 200 padlock.

UNKEYED CCI installed in open vehicles will be secured by padlocks with the radio secured by a security chain and a series 200 lock.

Immobilize steering wheel with a security chain and series 200 lock.

A vehicle not in use will be stored inside a fenced and lighted motor pool that has a roving guard (passing every 2 hours) for security checks.

Keys for padlocks will be maintained under local key and lock control procedures.

The Physical Security Branch, Office of the Provost Marshal, will inspect key control during physical security inspections to ensure the integrity of locks used to protect CCI.

7a

TRANSPORTATION

8

Control

There must be continuous control of CCI during transportation.

CCI cannot be transported in privately owned vehicles (POVs) without advance written approval from the appropriate commander or accountable officer.

CCI in operational configurations are permitted off-post subject to the following conditions

- movement must be part of command approved missions specifically approved by the responsible commander.
- CCI must be under constant surveillance, this applies to road, rail, and air transport, such as
  - rail movement to the National Training Center requires that CCI be under constant surveillance during transport (guards must be present to observe and control all access to the train when it is not moving).

(continued on next page)

---

**Control (cont)**

- CCI cannot be left in a locked unattended vehicle, unless it meets the double-barrier protection requirements stated above.

During air transport, a unit guard must be present to control access to CCI.

When CCI is flown in an aircraft without unit guards, a formal hand receipt transfer must take place to ensure that the air crew accepts responsibility for the CCI.

Preferred shipment other than registered mail or military vehicle is by the Department of Defense Constant Surveillance Service (DODCSS).

The DOL Transportation Division will provide the procedures to follow for shipment under the DODCSS.

All outbound CCI will be processed through DOL ensuring

- CCI is properly packaged for shipment.
- KEYED equipment is not shipped.
- batteries are removed prior to shipment.
- CCI is packaged in sturdy metal, wood, fiberboard, or heavy duty cardboard containers suitably constructed to prevent damage or undetectable examination of the contents.
- CCI is not shipped in a shelter unless it is a mounted integral part of the shelter.
  - Shelters will be processed through the designated support unit for technical inspection if there is CCI mounted inside.
  - Shelters will be unlocked when taken to DOL in order to ensure there is no CCI inside the shelter that is not an integral part of the shelter.
  - If there is mounted CCI in a shelter, there must be a "stamped" DA Form 5504 indicating the CCI is zeroized.
- shipping containers weighing over 40 pounds use nylon reinforced tape or are banded if a banding machine is available.
- small or fragile CCI components are packaged to reduce susceptibility to loss or damage and to prevent undetectable tampering or opening.
- CCI markings are clearly marked outside of packages in 2-inch letters or larger.
- "CCI" appears on all transaction documents.
- package wrapping contains "TO" and "FROM" information obtained from the Department of Defense Activity Address Directory (DODAAD) and other markings required to facilitate processing during shipping.
- each shipment of CCI contains a shipping document or record as required to effect transaction accounting and maintain an audit trail, for example, DD Form 1348-1.

---

(continued on next page)

NOTE: If the shipment consists of more than one package, each separate package will be assigned the same control or document number and will be identified by the individual package number, for example, WW70835, package No. 2 of 3. The total number of packages will be indicated on the shipping document. The shipping document will accompany package number 1.

- only authorized shipping methods are used.

Control (cont)

Shipment of CCI by registered mail will be processed through the DOL, then through the Fort Hood Post Office.

- The transaction will be recorded on DA Form 3964.
- The suspense copy will be held until the receiver's copy is returned.
- The receiver's copy completes the transaction.

KEYED equipment WILL NOT be shipped.

Shipment by means other than the above must be approved by the III Corps and Fort Hood DCIS.

All inbound CCI shipments will be received by the DOL Transportation Officer, building 49015.

When receiving CCI shipments,

- examine for signs of tampering,
- verify contents, and
- return signed receipts.

8a

INCIDENT REPORTING

9

Security Incidents and Reporting Procedures

It is essential that personnel who use or handle CCI be completely aware of security incidents and reporting procedures.

Report any incident of

- loss,
- loss of control,
- unauthorized access,
- transport by unauthorized means,
- unreconciled inventory,
- known or suspected espionage, and
- tampering.

The inability to account for or control CCI denotes a CCI incident, including those situations related to accidents in which control is temporarily or permanently lost.

Incidents which involve classified key in any form will be reported under AR 380-40 and TB 380-41-5 as a COMSEC incident.

Deviations from the procedures prescribed herein are reportable incidents.

(continued on next page)

Physical  
Security  
(cont)

Deviations will be reported to the

- unit or activity security manager,
- unit commander, and
- DCIS, 287-4706.

Incidents will be reported immediately.

The reporting channel for CCI incidents at Fort Hood is

- report to the unit/activity security manager or the unit commander/director.
- notify the DCIS, 287-4706, during normal duty hours.

NOTE: On nonduty hours, unit and activity security managers must notify the DCIS "On-Call" person. This individual can be contacted through the III Corps and Fort Hood Corps Operation Center (COC), telephone number 287-2520/2506.

An initial written report will be prepared within 24 hours and forwarded to DCIS by the unit/activity in which the incident occurred or as otherwise directed by the DCIS.

DCIS will make a determination as to whether a formal report to United States Army Intelligence and Security Command (INSCOM) is required.

NOTE: If it is reportable to INSCOM, it must be reported within 36 hours after the discrepancy is discovered and the need for a report is verified (the report will be in the format shown at appendix A).

Report to the CI Covering Agent for your activity.

A CCI incident is reportable under Subversion and Espionage Directed Against US Army and Deliberate Security Violations (SAEDA) as a Category VI investigation.

Any unit/organization who is reporting an incident must also report the incident to the assigned Covering Agent Team representative.

If a tenant organization has the incident, they should report the incident to the local 902d MI Group Resident Office.

Failure to report a CCI incident as a Category VI, SAEDA will generate a directive from the INSCOM Subcontrol Office to conduct the investigation (this directive is based on INSCOM receiving the report of incident from the respective unit).

Non-United States Army Forces Command (FORSCOM) organizations located at Fort Hood may report according to their local procedures except when FORSCOM CCI items are involved.

DCIS will fully coordinate reports of lost or missing CCI with the Provost Marshal.

- Reports will be marked as a minimum "FOR OFFICIAL USE ONLY," if it clearly does not contain classified information (classification guidance is contained in DA Pamphlet 25-380-2).

---

(continued on next page)

Physical Security (cont)

- If necessary facts cannot be gathered within 24 hours, all available information will be sent in an initial report.
- A copy of all reports to INSCOM, in message or memorandum format, will be sent to DCIS.
- Follow-up reports will normally be required.

The unit with jurisdiction of the incident will appoint an Investigating Officer, in writing, per AR 15-6.

The Investigating Officer will determine the facts surrounding the incident.

Fact finding will follow the informal procedures of AR 15-6.

DCIS will be provided a copy of appointment orders of Investigating Officer.

A copy of the completed inquiry will be forwarded to the DCIS, ATTN: AFZF-DS-S.

Relief from property accountability will be contingent upon the completion of a Report of Survey under AR 735-5.

9a

INSPECTIONS

10

Annual Command Inspections

Inspections will be conducted in conjunction with the Command Security Inspections IAW FH Circular 380-92-3, Schedule of Security Inspections.

The interval between command inspections will not exceed 24 months.

DCIS will inspect

- FORSCOM commercial/contractor COMSEC accounts and temporary contractor accounts.
- all CCI hand-receipt holders on the installation (units/activities).

10a

Unit/Activity Inspections

Each division/brigade, directorate, or other activity will inspect all CCI hand-receipt holdings in their subordinate units for accountability and security requirements annually as a minimum.

The DCIS will inspect all division/brigade headquarters and may inspect one or all units subordinate to that headquarters.

Directorates and activities that have CCI will be inspected by the DCIS (inspection checklist at appendix B.)

10b

---

Inspection Results/Reports DCIS is available to perform courtesy and assistance visits to all activities that are CCI hand-receipt holders.

Inspection reports will be forwarded to the unit inspected within 7 working days after DCIS has completed the inspection.

Unsatisfactory findings of CCI inspections will receive immediate attention.

Units/activities receiving unsatisfactory inspections may be reinspected within 90 days.

---

10c

SECURITY TRAINING

11

---

Training Class The Fort Hood DCIS will provide training classes as requested by a unit/activity security manager.

Commanders will ensure that all personnel who handle CCI are trained on the security requirements contained in this regulation.

Training will include all security standards and procedures contained in this regulation.

---

11a

Appendix A  
CCI SECURITY INCIDENT REPORT

(Use DD Form 173, Joint Message Form)

PAGE 1 OF

	TIME	MM	YY	PP	RR	UUUU	TIME
FROM	CDR	UR	UNIT	FT	HOOD	TX//UR	OFC SYM//
TO	CDR	INSCOM	FT	BELVOIR	VA//IAOPS	CI-OI//	
				DIRNSA	FT	MEADE	MD//X71A//
				CDR	902MIGP	FT	MEADE MD//IAGPA-OP-T//
INFO	CDR	FORSCOM	FT	MCPHERSON	GA//FCJ2	CIS//	
				CDR	CCSLA	FT	HUACHUCA AZ//SELCL-NICP-OR//
ZEN	FHRO	902MIGP	FT	HOOD	TX//IAGPA	C-FH//	
ZEN	CDR	III CORPS	FT	HOOD	TX//AFZF	DS-S//	
ZEN	(UNIT PROPERTY RECORD ACCOUNT IF NOT OWN)						

UNCLAS FOUO

QQQ

SUBJECT: CCI INCIDENT REPORT - INITIAL

A. DA PAM 25-380-2, SECURITY PROCEDURES FOR CCI, 10 JAN 91.

1. IAW REF A THE FOLLOWING INFO IS FORWARDED AS REQUIRED:

A. PHYSICAL LOSS OF UNKEYED CCI, STU III, 5810-01-230-1486, SERIAL NUMBER XXXXX, INSTALLED IN ROOM XXX, BLDG XXXX, FT HOOD, TX. CCI OWNED BY XXXXXXXXXXXXXXXXXXXX (UIC XXXX) AND ON HAND RECEIPT TO (UNIT), FT HOOD, TX.

B. CHRONOLOGICAL SEQUENCE OF EVENTS: AT APPROX 0730 ON 25 MAR 92, SFC DOE, JOHN E., 123-45-6789, AN NCO ASSIGNED TO XXXXXX, DISCOVERED THE STU III MISSING FROM HIS DESK. A THOROUGH SEARCH WAS CONDUCTED WITHIN THE BLDG AND A CHECK WAS MADE WITH ALL INDIVIDUALS WHO MAY HAVE HAD ACCESS TO THE ROOM. THE DEVICE WAS UNKEYED

AND VERIFIED AS PRESENT AT 1630 LOCAL ON 24 MAR 92 (SF 701, END OF DAY SECURITY CHECK). THE CRYPTO IGNITION KEY (CIK) FOR THAT STU III WAS SECURED IN A GSA APPROVED SECURITY CONTAINER WITHIN ROOM XXX. THE AC POWER ADAPTER AND CONNECTION CABLES ARE ON HAND. LOCAL CIDC ARE CURRENTLY INVESTIGATING THE CIRCUMSTANCES SURROUNDING THE INCIDENT.

2. AS INFORMATION BECOMES AVAILABLE, FOLLOW-UP/FINAL REPORT WILL BE FORWARDED.

3. POC IS XXXXXX XXXXX, DSN XXX-XXXX.

---

NOTE: The originator is responsible for assigning the proper classification and should examine all information furnished in the report before making a determination.

Mark reports that do not contain classified information "FOR OFFICIAL USE ONLY" and distribute internally on a need-to-know basis.

**Appendix B  
CCI SECURITY CHECKLIST**

	YES	NO	NA
Has the unit/organization developed an SOP which outlines procedures for physical protection and control of access to CCI equipment? (AR 380-40, para 2-1)			
In the event of an actual or possible compromise, are the commander's responsibilities outlined in the unit CCI SOP? (DA Pam 25-380-1, app B)			
Are transportation requirements for CCI outlined? (DA Pam 25-380-2, para 2-9)			
Does the SOP outline the following:  Access requirements for CCI? Double barrier storage requirements? Access control for storage area? Incident reporting requirements? Security training for personnel handling CCI? The conducting of quarterly inventories?	_____ _____ _____ _____ _____ _____	_____ _____ _____ _____ _____ _____	_____ _____ _____ _____ _____ _____
Does the unit/organization supply have copies of  AR 190-51, Security of Army Property at Unit and Installation Level, 30 Apr 86? AR 380-5, DA Information Security Program? AR 710-2, Supply Policy Below the Wholesale Level? FH Regulation 380-8, Security Procedures for Controlled Cryptographic Items? DA Pam 25-380-2, Security Standards for Controlled Cryptographic Items? TB 380-41-3, Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material? TB 380-41-5, Safeguarding COMSEC Material?	_____ _____ _____ _____ _____ _____ _____	_____ _____ _____ _____ _____ _____ _____	_____ _____ _____ _____ _____ _____ _____
Is there adequate security for CCI when unattended? (DA Pam 25-380-2, para 2-7)			
Is CCI afforded protection commensurate with the level of classification assigned? (AR 380-40, paras 8-2 and 8-4)			
Are unkeyed CCI stored under the double-barrier protection rules? (AR 190-51, para 3-6c(1)(a))			
Does the unkeyed CCI equipment meet the standards of AR 190-51 when installed in an operational configuration in an aircraft, vehicle, or other special conveyance? (AR 190-51, para 3-5d, e, and f)			
Does monthly inventory establish an audit trail? (AR 710-2, para 9-10, table B-1)			
Does the unit maintain proper accountability in the handling and storage of the Master CIK for STU IIIs? (AR 380-40, para 2-14)			
Are STU IIIs and CIKs inventoried quarterly?			
Are the Master CIKs being stored in a GSA approved security container? (AR 380-40, para 2-14)			
Is CCI ZEROIZED prior to storage, shipment, or turn-in? (FH Reg 380-8, para 7g)			
Does the unit SOP contain instructions for turn-in of CCI to the Security Warehouse, bldg 90031, West Fort Hood? (FH Reg 380-8, para 7g)			
Is there FORSCOM approval for STU-III telephones that are installed in on-post or off-post residences?			

## Glossary

## ABBREVIATIONS

---

CCI	Controlled Cryptographic Items
COC	corps operation center
COMSEC	Controlling Communication Security
CONUS	continental United States
DA	Department of the Army
DCIS	Directorate of Counterintelligence and Security
DODAAD	Department of Defense Activity Address Directory
DODCSS	Department of Defense Constant Surveillance Service
DOIM	Directorate of Information Management
DOL	Directorate of Logistics
DSU	direct support unit
FORSCOM	United States Army Forces Command
IAW	in accordance with
INSCOM	United States Army Intelligence and Security Command
LAA	limited access authorization
NSN	national stock number
OCONUS	outside continental United States
POVs	privately owned vehicles
SAEDA	Subversion and Espionage Directed Against US Army and Deliberate Security Violations

---

1 January 1993

III CORPS & FH REG 380-8

The proponent of this regulation is DCIS

FOR THE COMMANDER:



STEPHEN J. BERTOCCHI  
LTC, SC  
DOIM

ROBERT S. COFFEY  
Brigadier General, USA  
Chief of Staff

DISTRIBUTION:  
IAW FH Form 1853,  
PLUS: IM-AO (5)  
IM-ARL (2)  
IM-Pubs (100)  
DCIS (25)