HEADQUARTERS
U.S. EUROPEAN COMMAND

USEUCOM Directive 25-1

HEADQUARTERS U.S. EUROPEAN COMMAND
INFORMATION SECURITY
SOP

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
APO AE 09128-4209

TABLE OF CONTENTS

I. General Information
1. Summary 4
2. Applicability 4
3. Internal Control Systems 4
4. Suggested Improvements 4
5. Points of Contact 4
6. Responsibilities 5
7. Security Policy 5
8. Declassification and Information Requests 5

II. Administrative Requirements
1. Appointment Letters 6
2. Security Books/Files 6
3. Classified Cover Sheets 7
4. Travel/TDY 8
5. Directorate Administrative Guidelines 9
6. In-Processing/Out-Processing 11
7. Required Reports 11

III. Training
1. Training on Security Equipment 11
2. Security Training 11

IV. Security Procedures
1. Classification 12
2. Accountable Documents and Media 13
3. Procedures for Controlling Accountable Documents/Media 13
4. Transporting Classified Documents and Media 15
5. Destruction Procedures 16
6. Document Review/Clean out 17
7. Reproduction Procedures 17
8. Storage of Classified Material 18
9. Working Papers Control Procedures 19
10. Area and Container Security 19

V. Automated Information Systems (AIS) Security
1. General Guidance 21
2. AIS Marking 22
3. AIS Configuration &Location 25
4. AIS Access Control 26
5. Incidents 27
6. Official Use 29
7. Publishing Information 29

VI. STU-III Security
1. General Information 30
2. Physical Security Considerations 31
3. Responsibilities 32
4. STU-III Guidelines and Reference 33

VII. Conclusion 34

I. General Information

1. Summary. To establish policies and procedures for Physical, Information, and Personnel Security Programs for military and civilian personnel (including contractors) assigned to HQ USEUCOM. (NOTE: While security measures should not encumber day-to-day operations, proper documentation of some actions are required. These actions are **highlighted** and/or annotated with an asterisk.)

2. Applicability. This document applies to all personnel assigned to Headquarters, U.S. European Command. It does not apply to SCIFs, which are covered by separate instructions published by the Headquarters SSO.

3. Internal Control Systems. This Directive contains no internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. Suggested Improvements. The proponent for this Directive is the USEUCOM Special Assistant for Security Matters. Suggested improvements should be forwarded to HQ USEUCOM/ECSM, Unit 30400, Box 1000, APO AE 09128.

5. Points of Contact.

a. USEUCOM Special Assistant for Security Matters, ECSM, 430-8167.

b. Information/Physical Security, ECSM-SP, 430-8172.

c. Special Security Office, ECJ2-SSO, 430-8563/7189.

d. Personnel Security, ECJ2-SOI, 430-5365/7448.

e. AIS Security, ECJ2-SSO for SCI Systems, 430-5672/7189.

f. Foreign Disclosure, ECJ25-TB, 430-5478.

g. AIS Security, ECJ6-I, 430-5341/7300

6. Responsibilities.

a. The Special Assistant for Security Matters has been designated at the Headquarters U.S. European Command "Information Security Program Manager (ISPM)".

b. The HQ USEUCOM Security Manager, is assigned to the Special Assistant for Security Matters (ECSM); working in conjunction with OPRs of specific security programs, oversees all aspects of security within the headquarters, except SCIFs, which fall under ECJ2-SSO. ECSM-SP is the OPR for Information and Physical Security, as it pertains to protection of collateral, non-SCI, information and materials, and is the Office of Supporting Responsibility (OSR) for all other related areas.

c. **Directors will appoint Directorate Security Managers, in writing, and provide a copy to ECSM-SP.** Directorate Security Managers shall be the Director's representative for all internal security matters. He/she shall develop, implement and enforce security procedures within the directorate, and respond to the needs of the organization.

d. Division Chiefs are responsible for security within their respective divisions. In larger organizations, it may be appropriate to assign Division Security Managers. If so, they shall be appointed, in writing, to perform security duties and will perform duties in support of the directorate Security Manager. **Directorate Security Managers will maintain current copies of all appointment letters.**

7. Security Policy.

a. Security is an inherent responsibility. Anyone observing security violations/deviations or suspicious behavior or activities shall immediately bring them to the attention of the Division Security Officer who, in turn, shall notify the Directorate Security Manager. While security regulations do not guarantee protection and cannot be written to cover all conceivable situations, use of basic security principles, common sense, and a logical interpretation of directives will enhance security for the directorate.

b. This SOP shall remain a part of each security manager's continuity book, and made available to directorate personnel. Personnel shall review this SOP annually as part of the HQ USEUCOM and directorate's continuing security education program.

8. Declassification and Information Requests.

a. Directors are the reviewing authority for Freedom of Information Act (FOIA) and Mandatory Declassification Review (MDR) packages, and the authorities for declassification and retention of classification on documents and media for which the directorate is OPR.

b. Directorate XOs shall coordinate with the appropriate division for all FOIA & MDR packages. A "memorandum of reply" to ECJ1-AXR (tasking office) will be attached to the directorate tasker for use by the division OPR. Once complete, coordinate packages with the Directorate Security Manager for a final review of declassification procedures and return the package to ECJ1-AXR.

II. Administrative Requirements

1. Appointment Letters.

a. **Directors shall appoint, in writing, a Directorate Security Manager and Alternate. A copy of appointment letter for the primary and alternate Directorate Security Manager shall be forwarded to ECSM-SP.** (NOTE: Those personnel appointed to security manager duties will attend the HQ USEUCOM "Security Manager Training Course" as soon as possible, but not later than 6 months from the date of appointment.)

b. **Directors shall appoint, in writing, the Directorate TOP SECRET Control Officer (TSCO) and Alternate, and Directorate COSMIC/ATOMAL Control Officer and Alternate for the directorate NATO Control Point.** Directors should strive to maintain program continuity through critical review of changes to administrative processes brought about by personnel assignments to these billets.

2. Security Books/Files. **Directorate and division Security Managers shall maintain a security manager's continuity book on file.** It may be in paper form, saved to a computer disk (to include one backup copy), or a combination of the two. The book/file must include, as a minimum, the following:

a. Copies of their Security Manager appointment letters.

b. Copies of division personnel arrival dates, initial security briefing dates, annual re-briefing dates, and quarterly training.

c. Directorate and division security policy letters.

d. Copies of the following publications:

e. DOD 5200.1R, Information Security Program, with USEUCOM Supplement 1.

f. DOD 5200.1-PH, A Guide to Classified Documents.

g. USEUCOM Directive 25-5, Automated Information Systems Security Policy.

h. USEUCOM Directive 25-14, Personnel Security Program.

i. USEUCOM Pamphlet 25-2, Security Awareness.

j. USEUCOM Staff Memorandum 25-11, Exchange and Safeguarding of ATOMAL Information.

k. USEUCOM Staff Memorandum 25-13, Control of NATO Classified material.

l. HQ USEUCOM NATO Security Briefing for NATO SECRET and COSMIC.

m. ATOMAL Security Briefing

n. A copy of the Directorate "Emergency Destruction and Evacuation Procedures".

3. Classified Cover Sheets.

a. Classified cover sheets **ARE REQUIRED** on all classified documents when they are not secured in a safe (when visual access is available to persons not having the proper clearance or need to know). Personnel should assume that visual access is available any time classified material is outside of its secure storage container.

b. Use the following classified cover sheets:

(1) CONFIDENTIAL: Standard Form 705.

(2) SECRET: Standard Form 704.

(3) TOP SECRET: Standard Form 703.

(4) COSMIC TOP SECRET: ACE Form 76.

4. Travel/TDY.

a. Carrying Classified Material.

(1) Courier Orders: If there is a requirement to carry classified material while traveling off post on official business, the carrier must be designated as a "courier." A designated courier must hold a **courier letter** authorizing the conveyance of classified material. The letter must be signed by the Director or designated representative. DD Forms 2501 may also be used, in lieu of courier letters for travel **within Germany only**.

(2) Directorate Hand-carried Material Log: **Maintain a log to indicate what classified material is being carried by personnel on official travel.** The purpose of this log is to facilitate preparing a damage assessments in emergency/accident situations.

b. Passing Clearances to TDY Destinations:

(1) Personnel traveling on official business and needing to pass collateral security clearances to destinations must send a memo to the security manager. As a reminder, SCI clearances can only be passed from SSO to SSO. Collateral clearances may be passed by the Security Manager. Regardless of who passes the clearance, include the following information in the memo request:

(a) Name (LN, FN, MI):

(b) Rank:

(c) SSN

(d) DOB:

(e) POB:

(f) Destination:

(g) Organization/Location:

(h) Dates of Visit:

(i) Purpose of Visit:

(j) POC for Visit:

(k) GENSER Message Address:

(l) Telephone (Commercial and DSN):

(m) STU III (Commercial and DSN):

(n) FAX:

(2) ONLY the **Director** may authorize conveyance of classified material aboard commercial airlines outside CONUS. This practice will be kept to the absolute minimum. Every effort will be made to use U.S. Flagged carriers. However, when traveling **on commercial airlines** the orders must be annotated with the following statement: **"Individual Performing as an Official Courier for the United States Government"**. This authorization is in addition to following administrative requirements for transmittal of accountable documents.

(3) Classified material travel restrictions shall be part of the initial/recurring security training for directorate personnel.

5. Directorate Administrative Guidelines. **Directorates shall establish written procedures to document emergency evacuation and destruction, reproduction of classified material, control of uncleared personnel in the work area, and room/area/ safe inspections and checks for their divisions.** All personnel must be knowledgeable of these procedures. Guidelines for the EMERGENCY PORTIONS of these plans are listed below:

a. Emergency Plans: These plans shall be labeled "FOUO" and kept in the front of individual security container's locking drawer or on the exterior of one or two safes in a series of security containers. Each division shall include a review of these plans as part of their continuing security education training.

b. Safe Marking: Mark the interiors of the drawers with the appropriate level of classified material contained therein and marked with its priority of destruction, (e.g.: 1, 2 or 3). Destroy classified material in this order of priority:

(1) Priority 1: All TOP SECRET, COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and classified COMSEC Material.

(2) Priority 2: All SECRET, NATO SECRET and NATO SECRET ATOMAL material.

(3) Priority 3: All CONFIDENTIAL and NATO CONFIDENTIAL ATOMAL information.

c. Responsibilities: Individuals listed on the Classified Container Information Form (Standard Form 700), or directorate Duty Officer, shall be responsible for implementing emergency destruction procedures when required. If sufficient time exists:

(1) When ordered to implement emergency evacuation or destruction, Security Officers shall supervise the emergency plan implementation.

(2) The Directorate Security Manager shall coordinate with the divisions involved and supervise the directorate security issues pertaining to the operation.

d. Evacuation:

(1) Evacuate Priority 1 classified material with deploying sections in sturdy lockable boxes if time permits. If capture is imminent, destroy Priority 1 classified material as prescribed in paragraph e, below.

(2) Place Priority 2 classified material in burn bags; evacuate if time permits. If time does not permit evacuation, destroy Priority 2 classified material as prescribed in paragraph e, below. Do not retire or ship Priority 2 classified material to a rear area or records center.

(3) Destroy Priority 3 material as time permits.

e. Destruction Procedures: The destruction official shall destroy classified material, according to priority, in a shredder approved for classified destruction. If time permits, the destruction official, and witness officials, if available, shall execute certificates of destruction.

f. Civil Disturbances: All classified material shall be secured until orders are issued to implement emergency destruction. If an order to destroy material is given, or if a sufficient threat of compromise (as determined by military personnel present) exists, personnel shall proceed to destroy material by priority as prescribed.

g. Evacuation: Where fire, natural disaster, or any condition requiring evacuation (not related to deployment or dispersal) exists, evacuate classified material in order of priority to a safe place as determined by the senior military individual on-scene. There, place the area and the classified material under armed guard. If possible, the guard shall have a security clearance at least as high as the material being guarded.

h. Drills: Emergency evacuation or destruction training should take place during fire drills and practice exercises. **These exercises shall occur at least annually.** During fire drills and exercises, classified material shall not be removed from the building or destroyed. Instead, drills should include a walk-through to rehearse the material destruction precedence, time involved in moving back and forth between the destruction and evacuation points, and the volume of material that would require movement. Directorate Security Managers will document and maintain records of semiannual exercises.

i. Last Resort: In the event personnel listed on Standard Form 700 cannot be contacted, the Directorate Duty Officer shall be notified. The Duty Officer shall obtain combinations and work with other directorate personnel to complete the emergency destruction or evacuation.

6. In-Processing/Out-Processing. Departing (PCSing) personnel and sponsors of newly arrived personnel shall report to both the Directorate Security Manager, and the Security Clearance Office. Any badges obtained from these offices, or the SSO office, shall be protected as a valuable personal possession and returned prior to PCS.

7. Required Reports. A summary of security issues (including audit findings) shall be provided annually by the Directorate Security Manager to the Director. Additionally, the Directorate Security Manager shall immediately notify the Director of any significant security incidents.

III. Training.

1. Security Equipment Training. Security Managers are responsible for changing safe and door combinations, training personnel on proper procedures for operating the shredder, and for training/assisting personnel in the proper planning and conduct of the "shredding detail."

2. Security Training.

a. The Directorate Security Manager shall complete the HQ USEUCOM Security Manager's Course, prior to or as soon as possible (within 6 months), after appointment of this duty. Division Security Officers shall complete this course as soon as practical following their nomination to the position of Security Manager.

b. Division Security Officers shall ensure each newcomer receives division security training within seven working days of assignment. Recurring training for all assigned division personnel shall be provided on a regular basis, but no less than quarterly.

(1) Indoctrination training: Given by Security Managers to ensure new personnel receive initial briefings about security awareness and protection of classified material. Security Managers will review this SOP with the new individual during this training.

(2) Recurring training: The Directorate Security Manager shall publish an annual training plan. Although a majority of the training will be conducted by the Directorate Security Manager, divisions shall ensure that security training occurs on a quarterly basis. The computer Local Area Network (LAN) may be used in this effort. Training shall be annotated in the division security notebook or kept in a computer file. Items available as references for training are: this SOP, security regulations and directive reviews, SSO newsletters, Headquarters' policy letters, sanitized and unclassified security incident reports, and the annual security training plan disseminated by the Directorate Security Manager.

c. The Directorate Security Manager shall contact Division Security Officers on a quarterly basis to review past, continuing, and new directorate/division security training and practices.

IV. Security Procedures

1. Classification.

a. If personnel find documents and media that appear to be improperly classified, they shall notify the Division or Directorate Security Managers for follow-up action.

b. Directors are authorized to make original classification authority determinations for information up to and including SECRET.. In the absence of the Director, the Deputy Director is authorized to make such determinations. Only the CINC, DCINC, and Chief of Staff are authorized as Original Classification Authorities for Top Secret.

c. All personnel should have a copy of DOD 5200.1-PH, "A Guide to Classified Documents," for reference when marking documents. When using derivative classification (single-source or multiple-source), maintain a hand-written bibliography on a piece of paper attached to the file copy of the document for future classification reviews. If the document is stored only on disk, add a section on the disk listing source(s) for that document.

d. Classification Guides. A classification guide shall be issued for each classified system, program, plan, or project as soon as practical before the initial funding or implementation of the

system, program, plan or project. Guidance may either be published as a formal classification guide or included in plans or directives.

2. Accountable Documents and Media.

a. The Directorate TOP SECRET Control Officer (TSCO) shall manage the day-to-day operation of the accountable documents/media security program.

b. Definitions:

(1) Accountable Documents and Media: Documents and media classified as TOP SECRET, COSMIC TOP SECRET, ATOMAL, and NATO SECRET.

(2) NATO Documents and Media: Classified material originated by NATO. (NOTE: HQ USEUCOM cannot originate or stamp a document with a NATO caveat/classification unless it is jointly written and published--see SM 25-13.)

(3) COSMIC: The NATO term for TOP SECRET.

(4) ATOMAL: The NATO term for Formerly Restricted Data or Restricted Data (FRD/RD).

c. Individuals responsible for accountable documents and media shall not be relieved of their duties until a complete inventory is performed and total accountability has been assured and documented. Personnel on ETS/PCS shall turn in all classified documents and media assigned to them **seven working days** prior to their departure date. Personnel departing on leave/TDY for **more than 45 days** shall turn in or transfer their accountable documents and media through the TSCO.

3. Procedures for Controlling Accountable Documents and Media.

a. Accountable electronic messages are received at the VTCC and through various computer systems. Accountable paper documents are received via courier at the ECJ1-AC (Blue Room) or the directorates.

b. Receipts for U.S. SECRET materials are not required within the Headquarters. Receipts (DA Form 3964) **are required** for U.S. SECRET material being transferred outside HQ USEUCOM. (Maintain the returned signed receipt for two years and then destroy).

c. Under all circumstances, process and control every accountable document (as defined in para. 2.b.(1)) through the Top Secret Control Officer (TSCO).

(1) The TSCO is responsible for the initial receipt of accountable documents and media addressed to the directorate. Appropriate control forms shall be completed for each document before they are accepted and stored or given to another division for review. The TSCO normally also holds the position of ATOMAL Control Officer and is responsible for reviewing, dispatching, and maintaining accountability registers of TOP SECRET, COSMIC TOP SECRET, NATO SECRET & ATOMAL documents and media (the TSCO shall issue specific guidance).

(2) An original control register shall be maintained by the TSCO.

(3) Use the HQ USEUCOM Form 23-15, USEUCOM Classified Material Register to control the following accountable documents and media within the Directorate:

(a) COSMIC TOP SECRET Documents and Media

(b) TOP SECRET Documents and Media

(c) ATOMAL Documents and Media

(d) NATO SECRET

(4) Cover sheets are required on all controlled documents. Maintain access records, if required by classification level, for two full calendar years after the document has been destroyed. Affix the following forms to the appropriate documents:

(a) TOP SECRET documents - AF Form 144, TOP SECRET Access Record and Cover Sheet.

(b) COSMIC and ATOMAL documents - ACE Form 78, Access Control Record.

(5) Division personnel shall hand-carry accountable documents and media to the directorate TSCO for dispatch to organizations outside the Directorate. All accountable documents transferred temporarily or permanently shall be transferred through the directorate TSCO and **NEVER DIRECTLY FROM HOLDER TO HOLDER**.

(6) When accountable documents and media are being permanently transferred to another organization, route the document through the TSCO. Use USEUCOM Form 23-15 to show change of accountability. When a signature on the control register is not practical, annotate the control register with "see DA Form 3964" in the signature section as evidence the document was transferred. The TSCO shall ensure the signed receipt (DA Form 3964) is maintained with the register.

(7) Return all TOP SECRET Material (including working papers) to a GSA approved safe at the end of each duty day for safekeeping and for subsequent destruction when required.

(8) Do not place classified documents, including TOP SECRET documents, and media into "in/out" baskets or in distribution boxes. Always hand carry classified documents and physically turn them over to properly cleared individuals.

(9) TOP SECRET documents and media shall not be left unattended.

(10) TOP SECRET material created within Directorates shall be given a control number and controlled on HQ USEUCOM Form 23-15 by the TSCO. TOP SECRET material that is to be transferred outside HQ USEUCOM shall be hand carried by the TSCO to ECJ1-AAC for control and dispatch.

4. Transporting Classified Documents and Media.

a. Authorization to pick up classified material from the VTCC shall be approved by the Director or designated representative. Individuals authorized for this duty shall be appointed by letter, signed by the Director. Hand carry the original letter to the VTCC and a copy to the Directorate Security Manager, who should also retain a copy for his/her files.

b. Division personnel shall hand-carry accountable documents and media to the directorate TSCO for dispatch to organizations outside the Directorate.

c. Removal of Classified Material from facilities: In accordance with the USEUCOM Chief of Staff policy, **DO NOT** remove classified material from HQ USEUCOM installations (e.g., Patch Barracks) for the purpose of working on such material during off-duty hours or for other purposes involving personal convenience. See paragraph II.4 for procedures concerning the conveyance of classified material.

d. Personnel are authorized to carry classified material to/from other offices on Patch Barracks without a special authorization letter, however, they must receive a briefing on how to properly hand-carry classified materials. Whenever classified materials/media are being carried

between offices and outside of Patch Barracks, cover the material by the appropriate cover sheet and enclose in an opaque envelope or a more substantial closed container (i.e., double-wrapped, suitcase).

e. If directorate personnel are unfamiliar with the rules governing the transportation of classified material at HQ USEUCOM, they shall contact the Directorate Security Manager for guidance.

5. Destruction Procedures.

a. The following documents may be destroyed by any division personnel: SECRET, CONFIDENTIAL, and UNCLASSIFIED.

b. The Directorate TSCO shall accomplish destruction of TOP SECRET and NATO SECRET documents and media. Upon destruction of NATO Secret documents, using the Document control number, immediately notify ECJ1-AAC, NATO Sub-registry.

c. Return all COSMIC and ATOMAL documents and media to the directorate TSCO for destruction by ECJ1-AAC.

d. Destroy all classified material as soon as it is no longer required. Certificates of destruction are not normally required for SECRET or CONFIDENTIAL material.

(1) Divisions having shredders may use them for destruction of all but accountable/controlled documents and media.

(2) Individual offices shall secure their classified waste in authorized containers at the end of each duty day. Burn bags shall not be used for any other purpose than to hold classified waste and shall be marked on both sides of the bag as follows:

NAME
OFFICE SYMBOL
PHONE NUMBER
CLASSIFICATION (Only within SCIFs)

e. Maintain inactive register pages of TOP SECRET accountability records for two years in the inactive register. Maintain inactive NATO Secret register pages for two years.

6. Document Review/Cleanout.

a. Each division shall review at least 25 percent (or three linear feet, whichever is less) of classified holdings each quarter to determine whether or not they may be destroyed, declassified, or downgraded. In conjunction with this review, accountable documents shall be forwarded to the administrative staff for downgrading or destruction, as required. Staff officers should continually review files for these purposes during the course of normal duties.

b. The HQ USEUCOM CLASSIFIED MATERIAL CLEANOUT DAY will occur annually during the first Wednesday in February. Notice will be made early enough to allow divisions time to schedule at least one-half day to review and clean out classified material. TOP SECRET material shall be transferred, returned, or disposed of through the directorate TSCO.

7. Reproduction Procedures.

a. Reproduction of TOP SECRET material. Unless restricted by the originating agency, TOP SECRET information, may be reproduced to the extent required by operational needs. For COSMIC Top Secret, copies may only be made in the NATO Subregister. See SM 25-13 for other requirements for NATO document reproduction.

(1) A request for authority to reproduce a COSMIC or TOP SECRET document shall be routed through the directorate Security Manager for approval or disapproval, then to ECJ1-AAC (NATO subregistry), prior to forwarding to the originator.

(2) If the request for reproduction is approved, the directorate TSCO or alternate are the only authorized personnel who may reproduce TOP SECRET (ECJ1-AAC for COSMIC) material.

The single exception to this policy is for TOP SECRET messages, which shall only be reproduced by the SSO Communication Facility.

(3) Reproduction machines must have a notice stating classification limits posted over or on the machine. Machines cleared for classified reproduction shall be situated in an area with controlled access or where another individual has the capability to monitor copying. Authority to grant reproduction of classified material below the TOP SECRET level is limited according to policy established by each Division Chief. This policy must include who may authorize reproduction of classified, where (and on what machine) it can be done, and by whom.

b. The Directorate Security Manager shall clearly post written operating and purge procedures on/near machines authorized to reproduce classified material. Signs must also be posted on those machines **not** authorized for classified reproduction to clearly show this prohibition.

c. FAX machines shall have the same administrative controls as reproduction machines (see para. 6b above). Notices stating the classification level of a particular FAX machine (including UNCLASSIFIED USE ONLY) shall be posted over or on each FAX machine. Classified FAXs shall be situated in an area with controlled access or where another individual has the capability to monitor usage. Classified documents and media shall **NEVER** be sent over unclassified FAX machines.

8. Storage of Classified Material.

a. Every effort shall be made to store classified material in approved GSA security containers. If this is not feasible, the respective Division Security Officer shall submit written justification through the Directorate Security Manager to ECSM requesting approval for "open storage**." *** Every effort shall be made to replace all computers connected to the SECRET LAN with those that incorporate removable hard drives, and personnel shall make every attempt to ensure that classified material is not saved on their hard drives. *****

b. The HQ USEUCOM Chief of Staff is the final approval authority for all requests for open storage of classified material.

c. Under any circumstances, DO NOT store TOP SECRET, COSMIC TOP SECRET, ATOMAL or NATO SECRET documents and media outside a GSA-approved safe.

*****Directorates using approved open storage areas shall ensure that personnel are aware of proper control procedures for the storage areas and that these procedures are reviewed during all phases of division security education. Post the memorandum authorizing an open storage area inside the room near the door. *****

d. Physically separate all ATOMAL documents/media and NATO classified from U.S. classified documents/media during storage in GSA-approved containers (i.e., separate drawers or by file dividers).

9. Working Papers Control Procedures.

a. Working papers shall be dated, marked with the highest classification of information contained in the document and the words "WORKING PAPERS" and destroyed when they have served their purpose.

b. Classified working papers shall be controlled in the same manner as a finished document of comparable classification when:

(1) Released by the originator to any agency outside HQ USEUCOM.

(2) Transmitted electronically (i.e., by computer or other electronic method) or through message center channels within the headquarters.

(3) Held for more than 180 days from the date of the document.

(4) Placed in permanent files.

(5) When TOP SECRET information is contained within “Classified working papers" including information on diskettes and computer hard drives.

10. Area and Container Security.

a. The Directorate Security Manager is responsible for implementing required security measures. During periods of TDY or leave, this responsibility shall pass to the alternate Security Manager.

b. Security Containers.

(1) A Security Container Information Form (SF 700) shall be completed for each combination-locked safe or door, posted, and filed according to USEUCOM SUPPLEMENT 1 TO DOD 5200.1R (the SF 700 shall be attached in a conspicuous location inside the safe on the locking drawer). Directorate Security Manager will maintain all SF 700 (Part 2A)'s for safes storing SECRET and below material. Store all SF 700 (Part 2A)'s for safes storing TOP SECRET material only in containers or areas authorized to that level.

(2) The Directorate Security Manager is responsible for making storage container combination changes. For the combination locked entrance doors, change the combination at

least once per year. Change all other security container combinations and a new SF 700 prepared when:

(a) Departure of an individual who has access to the security container occurs.

(b) A suspected compromise of the security container combinations occurs.

(c) Every six months for security containers that store NATO documents and media.

(d) At least once a year.

(3) During non-duty hours, classified security containers shall be properly secured.

c. Cipher Locked Doors. Change the combinations to the cipher-locked doors using the same guidelines as safes.

d. Office Area Security. Directorates shall institute procedures to ensure classified material within the office is not available to uncleared personnel before, during, or after work hours. Recommended methods are: clean desk policy (no documents are allowed on desks, in work areas, or in-boxes when that desk is unoccupied) and entrance door security (designate an individual within sight of the access door with the responsibility of ensuring uncleared personnel are only allowed access when an escort is present (i.e., if that person does not have visual contact with the door it should be secured))

e. Use a Security Container Check Sheet (SF 702) to certify the opening, closing, and checking of all security containers within each division. Affix a SF 702 on the outside of each security container.

f. Post an Activity Security Checklist (SF 701) outside the entrance of each office and used for office checks. The form shall be modified to include equipment and appliances unique to that office. Each room shall be checked by the last person working in that office. Individuals shall use the SF 701 checklist to ensure that:

(1) In/Out baskets do not contain classified material.

(2) Classified material is not on, under, or in desks.

(3) Classified material has not been placed in waste baskets.

(4) Classified typewriter ribbons and computer disks are properly stored.

(5) Security containers are locked.

(6) Verification of locked security containers has been made by a second individual if available (if only one person remains in an office, that person signs "Checked" block also).

(7) Classified material is not on, between, behind, or under a safe.

(8) Burn bags have been placed in a security container.

(9) STU-III keys are not in the phones and properly secured.

(10) Security containers not opened during a duty day shall be checked and the SF 702 properly annotated.

V. **Automated Information Systems (AIS) Security**

1. General Guidance: This section applies to AISs classified at the TOP SECRET (collateral) level and below. Procedures for Sensitive Compartmental Information (SCI) or Special Access Program (SAP) AISs are available from the ECJ2 SSO.

a. It is DOD policy that "Classified information shall be safeguarded at all times while in AISs. Safeguards shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly…." [DODD 5200.28]

b. The above policy statement says that classified information is classified information and needs to be protected regardless of whether it is in a computer or is written on paper. An individual called an Information Systems Security Officer (ISSO) is appointed for each AIS system in use at HQ USEUCOM and their function is to develop safeguards for their AIS.

c. 'Safeguards' help users protect the classified information contained in the AIS. Safeguards may be built into the system as automatic features or may be procedures users must follow. It is USEUCOM policy that ISSO document AIS security procedures. This document is usually called a Security Features Users Guide (SFUG) or Security Concept of Operations (CONOPS). An excellent summary of AIS user responsibilities can be found on the User Agreement Form a

user signs when getting their password and account information. Users are responsible for knowing and following procedures for the AIS they are using.

d. There is no single set of procedures to follow for every AIS, but there are common elements. This section of the HQ USEUCOM Information Security SOP identifies procedures common to all AISs. If there is a difference between this SOP and an AIS SFUG or CONOPS, the most restrictive guidance will be followed. Security Managers and AIS users are responsible for following the procedures in the SFUG for each AIS on which they have an account. Following is a list of the AISs and ISSOs most commonly encountered at HQ USEUCOM:

SYSTEM NAME	ISSO	Security Procedure Location
C4I SECRET LAN (SLAN)	LTJG Barry Austin (430-7233) TSgt Ron Barmes (430-4184)	SFUG http://www.eucom.smil.mil/ecj6/ecj6-noa/security/slan/SFUG.html {on SIPRNet}
C4I UNCLASSIFIED LAN (ULAN)	LTJG Barry Austin (430-7233) TSgt Ron Barmes (430-4184)	Contact ISSO
Global Command and Control System (GCCS)	LTJG Barry Austin (430-7233) TSgt Ron Barmes (430-4184)	Security CONOPS, contact ISSO

2. <u>AIS Marking, File Transfer and Declassifying/Destruction</u> AISs are approved to process up to and including a specific classification of data. For example, SLAN terminals may be used to process UNCLASSIFIED up to and including U.S. SECRET data. Users will not use an AIS to process data at a level other than approved for the AIS. For example, users may NOT use an SLAN terminal to process NATO classified data. AISs will be marked to show users the acceptable processing level.

a. Marking Equipment: AIS equipment is marked with a label (SF 706 (TS), 707 (S), 708 (C), & 710 (UNC)) showing the highest classification level contained in (or is processed by) the equipment. Place these labels on the fronts of monitors, CPU cases, and printers. Labels are not required on keyboards and the mouse.

b. Marking Magnetic Media: External classification markings on magnetic media (hard disks and diskettes) are required:

(1) SF 706 (TS), 707 (S), 708 (C), & 710 (UNC) labels, corresponding to the highest classification of material stored, are required on the visible portion of removable hard disks and the top front edge of diskettes. All diskettes shall have a label affixed to the top side of the diskette. Additionally, TOP SECRET magnetic media must be controlled and handled in the same manner as equivalent level documents through the directorate TSCO.

(2) Non-removable hard disk computers require the highest classification markings of the stored information to be placed on the outside of the case. If a computer has non-removable classified drive, that computer must be located in an area approved for open storage of classified information.

(3) Any disk introduced into a system with a higher classification than listed on the disk must be regraded to the higher classification level unless the disk's write protection tab is "on".

c. Marking EMAIL: The most commonly encountered AIS security violation at HQ USEUCOM is improperly marked EMAIL.

(1) CLASSIFIED EMAIL. The subject line begins with a security marking indicating the overall classification of the EMAIL's content and ends with a security marking indicating the classification of the subject line itself. The EMAIL body will begin with a classification banner indicating the OVERALL security classification. The standard is to put one banner at the beginning of the message and one at the end. All paragraphs and subparagraphs are labeled with the standard security markings (U), (C), or (S). The last line of text is the declassification instruction. USE OF "OADR" IS PROHIBITED. See DOD 5200.1-R, Chapter 5, Marking.

(2) UNCLASSIFIED EMAIL (with no classified attachments). A totally unclassified EMAIL(body of EMAIL and any attachments are unclas) does not need classification markings.

(3) UNCLASSIFIED EMAIL (with classified attachments). Handled like papercopy Transmittal Documents. Even though the body of your EMAIL might be unclassified (remember, there are classified attachments) the subject line has to reflect the highest classification level of everything including the attachments. The body of the unclassified EMAIL must also be marked (top and bottom) with the highest classification found in any of the attachments. Example: An unclassified transmittal document has one Secret and two Confidential attachments - mark the EMAIL as 'SECRET'. Individual paragraph markings are not required. The bottom of the EMAIL will be marked to show its status when separated from the classified material. Examples include: "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES," "UNCLASSIFIED WHEN filename IS REMOVED,"

"CONFIDENTIAL UPON REMOVAL OF ENCLOSURES," or a similar statement.

d. Transferring files between AISs of differing classification levels:

(1) Low to High. Data files can be transferred from a system of lower classification to one of higher classification as long as the transferring disk's write protection tab is in the "on" position. If the tab isn't "on", the disk must be remarked as the higher classification level.

(2) High to Low. AIS specific procedures must be used to avoid inadvertently copying classified information onto the transfer disk and later injecting it into the AIS of lower classification. Just deleting information is not enough to guarantee it is removed from a file. Word processing documents typically store the text you delete in the back of the file in case you want to 'undo' your edits later. This information can be recovered from a file and cause a security compromise. Refer to the AIS SFUG or Security CONOPS and follow the stated procedures. If there are no stated procedures, then this type of transfer is not allowed.

e. Declassifying/Destruction: Equipment, printer toner cartridges/ribbons, hardcopy output, and media must be properly sanitized prior to disposal or turning it into DRMO for reissue.

(1) Equipment. Hard disks must be removed from AIS equipment and transferred to the C4I Helpdesk even if marked UNCLASSIFIED. Printer toner cartridges/ribbons will be removed after declassifying as noted in (2) below. Labels denoting the classification level of the equipment will be removed. Equipment can then be handled as UNCLASSIFIED.

(2) Printers. Laser printer cartridges must be sanitized prior to being recycled at SSSC by printing 5 pages of random characters entirely filling each page. Printer ribbons must be physically destroyed. This can be accomplished by putting them in with your 'burn bags' and shredding in the Patch Barracks Destruction Facility (bldg. 2323) or equivalent facility.

(3) Hardcopy output. Handle and control all output from AIS as the classification level of the AIS until it is reviewed and regraded.

(4) Media.

(a) Hard disks and magnetic tape are extremely difficult to declassify and reuse. Security Managers will not attempt to declassify these items: turn them into the C4I Helpdesk for declassification or destruction.

(b) All UNCLASSIFIED floppy disks can be expected to have at least some FOUO material and will be reformatted prior to disposal or being sent outside the organization. If the floppy is physically damaged and reformatting is not an option, carefully disassemble the floppy disk case and remove the disk inside. Shred the disk between two pieces of paper in any shredder approved for at least SECRET hardcopy.

(c) CLASSIFIED floppy disks are not worth the effort to declassify and reuse. Carefully disassemble the floppy disk case and remove the disk inside. Put the disk in your 'burn bags' for destruction in the Patch Barracks Destruction Facility (bldg. 2323) or equivalent facility. These disks will not be shredded in an office style shredder since the remaining pieces would still hold considerable information.

(d) UNCLASSIFIED Compact Disks can be thrown away.

(e) FOUO Compact Disks can be destroyed by breaking them into two pieces and throwing them UNCLASSIFIED trash. Be extremely careful when breaking a CD; tiny plastic shards can fly everywhere!

(f) CLASSIFIED Compact Disks can be destroyed by using a sander (like one used for sanding wood). Sand the label side of the CD down into the plastic, making sure to remove all of the label. It is important to sand down into the plastic to remove the recording tracks. It is not necessary to turn the entire disk into dust. The disk will then be placed in a 'burn bag' for shredding in the Patch Barracks Destruction Facility (bldg. 2323) or equivalent facility.

3. AIS Configuration and Location Two considerations used in determining if an AIS's 'safeguards' are adequate to protect they data they process are AIS configuration and location. Users should be aware that modifying either of these features can change how well data is protected.

a. Privately owned computers will be used only in the stand-alone configuration and only AFTER WRITTEN AUTHORIZATION IS RECEIVED FROM THE HQ USEUCOM ISSM (ECJ6-I 430-5341/7300). Privately owned computers will not be used to process classified and sensitive unclassified information.

b. Use of privately owned software on government computers is not allowed without specific written permission of the AIS ISSO. Especially avoid any executables received via email since many of the little games and screen savers received from 'friends' via email have viruses.

c. Users must coordinate AIS equipment moves with the ISSO if equipment is being moved from one room to another or needs to be plugged into a new network drop. Simply moving equipment around on your desk or within the existing room does not require ISSO approval.

d. Under no circumstances are additional network connections (including modems and Palm Pilot™-like computers) allowed without ISSO approval.

e. If a computer has non-removable classified drive, that computer must be located in an area approved for open storage of classified information.

4. AIS Access Control The most effective attacks against AISs begin with unauthorized individuals gaining access via existing user accounts. It is essential for users to follow good security practices when using their accounts to prevent unauthorized users from gaining access.

a. User Accounts. A user account is assigned to an individual for performance of their jobs in much the same way any other piece of government equipment might be (e.g. a rifle). The account is uniquely assigned to a user, but remains the property of the government and its use can be audited by the government as stated in the log on banner which is shown to the user each time they log on.

(1) AIS specific training (initial and yearly refresher) is required to have an account on a USEUCOM AIS. This training is documented in the User Agreement Form and must be read, signed, and forwarded to the AIS ISSO yearly or the user's account will be deactivated.

(2) No account may be 'shared'. There must be only one person with the password for each account. Passwords must be changed at least every 180 days and not be easily guessable. ISSOs periodically run tools to guess passwords and may lock a user out if their password is easily guessed. Passwords, even for UNCLASSIFIED AISs, are handled as SECRET. If a password needs to be written down, do so on an SF 700 and treat it like a safe combination. If a possible compromise of the password has occurred, change the password immediately and report the incident through the C4I Helpdesk.

(3) If a user notices 'suspicious' activity on their account, they will contact the C4I Helpdesk as noted in the Incidents section below. Examples of 'suspicious' activity can include: having a logon failure where the AIS displays a notice that they are already logged on or having files mysteriously appear or disappear.

(4) Never leave AIS equipment unattended while logged on. It is permissible to activate a screen-saver with a password feature if a user leaves the area for periods up to 30 minutes. If

gone longer than 30 minutes, the user will log off the account and secure the hard drives/floppy disks in a manner commensurate with the classification of this media.

b. Controlling the area.

(1) Ensure all personnel in the general vicinity have the appropriate clearance for the data being processed or are screened from viewing any classified information.

(2) Ensure the monitor is turned away from uncontrolled areas to avoid inadvertent disclosure of classified information.

(3) Foreign nationals are NOT allowed access to USEUCOM AISs except in a very few cases. If there is a foreign national who is permanently assigned to a work area with AIS equipment, their presence in this work area must be documented to the ISSO. Do this quarterly even if you think the ISSO knows the foreign national is in your work area.

(4) Printers must be turned off at night to clear their buffers of potentially classified information. If a printer is directly connected to the network, the network buffer must be cleared by the last person using the printer before shutting it off for the night.

5. Incidents AIS security officials continually assess adequacy of safeguards and need user feedback to accomplish this. It is important for users to properly report AIS security incidents to assure good assessments.

a. Viruses.

(1) It is a DOD requirement that all government AISs have virus detection software installed. This software is freely available from DISA and may be loaded on your home computer if you use if to do work while at home. The distribution site is http://199.211.123.12/ Virus/avirus.html on the Internet. Check with the AIS ISSO to see what product and version is in use with that particular AIS.

(2) Both executable and data documents can be infected with viruses. Both will be scanned prior to beings introduced into an AIS.

(a) Since loading software other than what comes loaded on the AIS equipment is UNAUTHORIZED, there should be no problems with infected executables. To ensure, however,

this is the case, scan all floppies anyway and have the virus detection software scan your hard drive at least weekly.

(b) Data documents like Microsoft WORD™ can also pickup viruses called macro viruses. Limited protection from these viruses for WORD ™ is available from the following site on classified USEUCOM terminals connected to the SIPRNET http://www.clf.navy.smil.mil/clf/n6/n63/scanprot.htm. This software automatically scans documents when they are opened. An UNCLASSIFIED site for this software is not currently available.

(3) Report all virus detections to the C4I Helpdesk. The Helpdesk will assist in cleaning the virus off the equipment if the user requests assistance.

b. Data spills. A data spill is placing or finding the data classified higher than the AIS on which it is found (e.g. SECRET on an UNCLASSIFIED AIS).

(1) Do not delete the EMAIL, message, or file containing the information. The source of the data spill has to be traced and may be destroyed if the information is deleted.

(2) Contact the C4I Helpdesk and report the incident. If you are the source of the incident, the Helpdesk will require your assistance in notifying all other recipients of the information of the incident.

(3) If the source of the data spill is a SIPRNET web page, send an email (classified SECRET) to icsrosewc@ismc.sgov.gov and ismc@ismc.sgov.gov with the URL of the page and how the page was found (i.e. what search engine). Alternately, call DSN312-644-1800 on a STU III telephone.

(4) If the source of the data spill is an INTERNET web page, contact ECSM (430-8172) or ECJ6-I (430-5341/7300) immediately via secure means.

c. Unauthorized access.

(1) If a user notices ‘suspicious’ activity on their account, they will contact the C4I Helpdesk immediately. Examples of ‘suspicious’ activity can include: having a log on failure where the AIS displays a notice that they are already logged on or having files mysteriously appear or disappear.

(2) If notices someone logging onto other than that person’s account, they will contact the C4I Helpdesk and report the incident.

6. Official Use HQ USEUCOM Staff Memorandum 100-3 (5 May 97) provides guidelines governing personal use of HQ USEUCOM AISs. Users are responsible for complying with these guidelines.

7. Publishing Information This sections refers to publishing information either via Internet/SIPRNET sites or by EMAIL.

a. HQ USEUCOM Staff Memorandum 15-1 (24 Nov 97) provides policy on posting information on USEUCOM's Internet WWW pages.

(1) Directorates will designate (in writing) those personnel who shall be given access to upload or modify files on the web server in accordance with SM 15-1.

(2) Directorates will ensure that information within their purview, which is posted to the public access WWW information service, is accurate, timely and appropriate for public release. This includes a method for regular review to ensure posted information continues to be appropriate, applicable and accurate.

(3) Directorates will submit for ECPA review any new pages and significant changes to style or content of previously posted pages.

b. Directorates must also consider OPSEC value of the information prior to posting it. Questions on OPSEC should be referred to ECJ33 and ECSM.

c. The only restriction on publishing information on SIPRNET accessible sites and via classified EMAIL is verification of "need-to-know". Executive Order 12958 states "A person may have access to classified information provided that the person has a need-to-know the information." Need-to-know means an authorized holder of classified information makes a determination that a recipient requires access to specific classified information.

(1) Publication of classified or sensitive but unclassified information via EMAIL will only be accomplished if each person on the EMAIL address needs-to-know the information in the EMAIL.

(2) Publication of classified or sensitive but unclassified information on USEUCOM's SIPRNET accessible pages will be accomplished in accordance with need-to-know policies. Access to information posted to SIPRNET accessible pages will be restricted by the page owner to only personnel with a need-to-know the classified or sensitive but unclassified information.

VI. STU-III Security

1. General Information.

a. References:

(1) NTISSI No. 3013
(2) Operating guide for the GE/RCA STU-III Terminal
(3) User's Manual for the Motorola STU III/A Sectel Term
(4) User's Manual for the AT&T STU III Terminal

b. Terms and Definitions:

(1) STU-III System: Consists of the STU-III Terminal with a crypto fill and the associated STU-III keys (one Master and up to 8 Cryptographic Ignition Keys (CIKs)).

(2) STU-III Terminal: Refers to the actual phone with secure voice/data capabilities; terminals are accountable as CCI (Controlled Cryptographic Item) equipment and a keyed terminal is classified to the level of it's key.

(3) STU-III Keys/KSD64A's: Refers to the key-shaped computer chip used to key a STU-III terminal for secure communications; there are two types of key: Master Keys and CIKs.

(4) Master Key: A STU-III key capable of making or reinitializing zeroed CIKs. Masters should not be used on a daily basis due to the possibility of accidentally zeroing it. If zeroed, the ability to make new CIKs is lost and the entire system must eventually be re-keyed by CMDSA. One Master is issued with each terminal at the time of it's Initial or CMDSA re-key.

(5) CIKs: A STU-III "operational" key used to key the terminal on a daily basis. One CIK is issued with each terminal at the time of it's initial keying or re-keying. Up to 8 CIKs can be made from the Master and a CIK that is accidentally zeroed can be locally re-keyed from the

Master. CIKs must be kept under personal control and/or security container at all times (secured in a locked desk or safe); otherwise, a security violation may occur if a CIK is left unprotected in the proximity of its associated terminal (i.e., left in a desk next to the telephone where anyone could find and use the STU-III at a classified level).

(6) Controlled Cryptographic Item (CCI): Equipment that is accountable by serial number to the Property Book Officer/NCO. CCI equipment must be inventoried at intervals directed by the Property Book NCO.

(7) Fill: CRYPTO keying material loaded into the STU-III phone terminal (by CMDSA). Each fill has a corresponding and unique (Master) key; "loss of fill" will render a STU-III system incapable of "going secure" and requires a CMDSA rekey (i.e., an entirely new fill and Master).

(8) Key Management Center (KMC): The central authority responsible for controlling key material and issuing/updating Compromised Key Lists (CKL). All STU-III keys must be updated through KMC when the terminal receives an initial or CMDSA rekey, and at least annually thereafter. Quarterly KMC calls are HIGHLY recommended. The numbers to call are Comm 1-800-635-6301; DSN 312-936 1810; local 99-0130-81-0752.

(9) COMSEC Material Direct Support Activity (CMDSA): The 587th Signal Company is the local authority responsible for controlling key material and providing assistance to local users on STU-III terminals to include CMDSA Re-keys. (DSN 430-5561/8449).

2. Physical Security Considerations:

a. STU-III terminals are considered CCI (inventoried) items.

b. STU-III terminals, when unkeyed, must be:

(1) Protected as a "high-value item".

(2) Accounted for by serial number.

(3) Installed/stored in U.S. controlled facilities only.

(4) Reported to security personnel if lost or stolen.

c. STU-III terminals, when keyed, must be considered classified to the level of their keying material when CIKs are installed. Keyed terminals with CIKs installed must be:

(1) Protected at the level of their keying material.

(2) Used by authorized U.S. persons only, or under direct U.S. supervision if used by foreign nationals during official business.

(3) Installed only in areas that are approved for the appropriate level of classified conversations/data transmission.

3. Responsibilities.

a. Property Book Custodian: STU-III terminals are CCI items and are accountable by serial number by Property Book Officers, who may sub-hand receipt terminals to sub-hand receipt holders.

b. Directorate STU-III Representative: The directorate STU-III Representative shall provide training and guidance to STU-III users and shall assist with all security audits pertaining to this portion of this memorandum.

c. Security Managers: Security Managers shall maintain accountability of CIKs. Specific duties include:

(1) Maintain updated STU-III Key Control Logs on all STU-III keys within the directorate.

(2) Maintain proper storage of Masters and 1 to 2 extra zeroed CIKs; inventory semi-annually.

(3) Inventory issued CIKs quarterly; ensure all CIKs are accounted for.

(4) Spot check use and control of issued CIKs; ensure keyed terminals and keys are not left unattended.

(5) Coordinate all initial and CMDSA re-keys within the Directorate.

d. Designated STU-III Hand receipt Holders: Each hand receipt holder shall maintain accountability of STU-III terminals.

e. Users: STU-III terminal users shall sign for one CIK from the Division Security Officer (STU-III Key Control Officer). They shall maintain the key either on their person or in a secure storage container when not in use.

f. Turn-In/Storage/Transportation Considerations: Personnel holding STU-III terminals that require repairs, turn-in as excess, or storing for future use, shall make arrangements with the

Property Book NCO to zero the terminal before it leaves their control (do NOT attempt to zero the terminal prior to contacting the Property Book NCO).

(1) NEVER turn-in, ship or store STU-III terminals with Keying Material, CIKs, Fill Devices or KSD64A's (blank keys). Excess/unused keys must be turned-in to CMDSA.

(2) A zeroed/un-keyed STU-III Terminal is an UNCLASSIFIED, Controlled Cryptographic Item (CCI), and be accounted for as a "high-value item."

(3) Limit access of the terminal during transportation to U.S. citizens only (this includes proper escort during movement).

(4) Store terminals in U.S. controlled facilities only.

(5) Report loss/theft of terminal to your security personnel.

4. STU-III Guidelines and Reference. Additional guidelines and procedures for STU-III management can be obtained by contacting 587TH signal Company at DSN 430-5561/8449/7196.

VII. Conclusion:

1. While security regulations do not guarantee protection and cannot be written to cover all conceivable situations, use of basic security principles, common sense, and a logical interpretation of directives will enhance security for the directorate.

2. This SOP, along with any directorate specific supplementation and/or guidance, shall remain a part of each security manager's continuity book, and made available to directorate personnel. Ensure personnel review this SOP annually as part of the HQ USEUCOM and directorate's continuing security education program.

3. Disclaimer. Nothing in this document shall relieve an individual of the responsibility to ensure proper security measures are implemented. Additionally, when conflicts arise between this operating instruction and governing regulations, follow the guidance contained in governing regulations.

FOR THE COMMANDER IN CHIEF

DAVID L. BENTON
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

DISTRIBUTION:
P