

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131

USEUCOM SUP 1
DOD 5200.1-R

5 May 2003

Information Security Program

1. **Summary.** This supplement provides policy and procedures for the implementation and development of information security programs in USEUCOM.
2. **Applicability.** This supplement is applicable to all units assigned or directly reporting to HQ USEUCOM. This supplement is intended as a guide and baseline policy for use in the development and operation of assigned unit information security programs.
3. **Supplementation.** Commanders may supplement this guidance as necessary in order to ensure program effectiveness.
4. **Suggested Improvements.** The proponent of this supplement is HQ USEUCOM ECJ2 Security Support Office (ECJ2-SSO). Users may send comments and suggested improvements to this supplement to HQ USEUCOM, ATTN: ECJ2-SSO (IP), APO AE 09131.

FOR THE COMMANDER:

OFFICIAL:

JOHN B. SYLVESTER
Lieutenant General, USA
Chief of Staff

DANIEL A. FINLEY
MAJ, USA
Adjutant General

DISTRIBUTION:
P

This supplement supersedes HQ USEUCOM SUP 1, DOD 5200.1-R, dtd 29 Oct 97
GENERAL PROVISIONS

APPENDIX 2 - Definitions. Add the following:

AP2.1.70. Security Deviation: An incident that involves the misuse or improper handling of classified material but does not fall in the categories of compromise, probable compromise or loss.

AP2.1.71. Open Storage: Storage of classified material outside of a GSA approved security container.

APPENDIX 3 - Controlled Unclassified Information. Add the following subparagraphs.Page 143, AP3.2.4.4, Protection of FOUO Information. Add the following:

AP3.2.4.4. FOUO information shall not be posted to a publicly accessible web site. Whenever practical, FOUO information should be transmitted via secure means (i.e. SIPRNET, secure fax). FOUO may be transmitted via NIPRNET to individuals with a need-to-know. Utmost discretion must be used when transmitting FOUO to non-government systems. Specific categories of unclassified information may have more stringent controls (i.e. itineraries on GO/FOs and civilian equivalents, unclassified nuclear information, etc.)

Page 143, AP3.3.5, Protection of Sensitive Information. Please add the following sub-para e.

AP3.3.5. Sensitive information shall not be posted to a publicly accessible web site. Whenever practical, sensitive information should be transmitted via secure means (i.e. SIPRNET, secure fax). Utmost discretion must be used when transmitting sensitive information to non-government systems. Specific categories of unclassified information may have more stringent controls (i.e. itineraries on GO/FOs and civilian equivalents, unclassified nuclear information, etc.)

NOTE: The following NEW Appendices are to be added to the existing DoD 5200.1-R.

Appendix 10	Accountability and Control of Classified Information
Appendix 11	Classified Material Destruction Standards
Appendix 12	Original Secret Classification Authorities
Appendix 13	Sample Preliminary Inquiry Report Memorandum
Appendix 14	Sample Courier Authorization Memorandum and Exception to Policy
Appendix 15	Open Storage Request Procedures
Appendix 16	Declassification and Downgrading Authorities
Appendix 17	Automatic Declassification Review System

Chapter 1
POLICY AND PROGRAM MANAGEMENT

Table of Contents

Paragraph

C1.2.2.1	DOD Components
C1.2.3	Senior Agency Officials
C1.3.2	Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information.
C1.4.1	Military Operations
C1.4.2.2	Waivers to Requirements

CHAPTER 1
POLICY AND PROGRAM MANAGEMENT

Page 9, paragraph C1.2.2.1, DOD Components. Add the following:

The HQ USEUCOM Commander has designated the Director of Intelligence (ECJ2) as the Senior Information Security Authority for HQ USEUCOM and its assigned Elements.

Page 9, paragraph C1.2.3, Senior Agency Officials. Add the following:

Send a copy of appointment letter to ECJ2-SSO(IP). Appointed Security Managers must attend a formal HQ USEUCOM Security Managers Training Course within the first six months of appointment. Security Managers for Offices of Defense Cooperation (ODC) should also provide a copy of appointment letters to Embassy Regional Security Officers (RSOs) and attend appropriate in-house security training.

Page 11, paragraph C1.3.2, Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information. Add the following:

ECJ2-Security Support Office will provide guidance on security, use, and dissemination of Sensitive Compartmented Information (SCI) material in accordance with applicable directives. ECJ6 and 52nd Signal Battalion will provide guidance on security, use, and dissemination of Communications Security Information (COMSEC).

Page 11, paragraph C1.4.1, Military Operations. Add the following:

Operational requirements for classified computer networks and communications in support of EUCOM operations must be coordinated well in advance with ECJ2 and ECJ6. Such requirements shall contain sufficient information to permit a thorough analysis of the impact on national security before approval/accreditation of systems. Issues of connectivity to U.S. classified computer systems or databases, presence of foreign personnel on or in the area of the system, identification of security officials/entity and hardware and software safeguards to protect U.S. classified information must all be included in the identification of the requirement.

Page 11, paragraph C1.4.2.2, Waivers to Requirements. Add the following to paragraph 1-401(b):

Waiver requests from USEUCOM units concerning access to U.S. classified computer systems or databases must be coordinated with the organization(s) with the overall responsibility to protect that information. Other users of the system/database should also be informed of the expanded access to the information they store or transmit on that system.

Chapter 2
CLASSIFICATION

Table of Contents

Paragraph

C2.2.2.2	Delegation of Authority
C2.4	Compilation
C2.5.3	Approval, Distribution and Indexing

Chapter 2
ORIGINAL CLASSIFICATION

Page 15, C2.2.2.2, Delegation of Authority: Add the following:

Within HQ USEUCOM, the Commander, Deputy Commander, and Chief of Staff have Top Secret Original Classification Authority (OCA). HQ USEUCOM elements delegated Secret and Confidential classification authority are listed at Appendix 12.

Page 19, paragraph C2.4.1, Compilation. Add the following:

The consolidation of unclassified U.S. Government operational, logistics and support information in databases or computer networks may increase the sensitivity of information which was previously unclassified due to its dispersion. Special consideration should be given to the classification and protection of this information. EUCOM units designing or using such systems should have a written evaluation of risk to national security and impact on mission of the compromise of such information in consolidated form.

Page 21, paragraph C2.5.3.6, Approval, Distribution and Indexing. Add the following:

f. Copies of each approved classification guide (less SCI) and changes will be forwarded to ECJ2-SSO for distribution to DOD and the Office of Industrial Security as appropriate. Originators also will furnish classification guides (or other classification guidance) to all probable users such as test and evaluation organizations or activities having an official and recurring interest in the subject matter for posting on the ECJ2-SSO web site for distribution (SLAN).

Chapter 4
DECLASSIFICATION AND REGRADING

Table of Contents

Paragraph

C4.1.3.6	Declassification and Downgrading Authority
C4.3	Automatic Declassification at 25 years
C4.9.2.4.5	Classification Challenges

Chapter 4
DECLASSIFICATION AND REGRADING

Page 30, paragraph C4.1.3.6, Declassification and Downgrading Authority. Add the following:

C4.1.3.6. USEUCOM personnel identified in this supplement as having Original Classification Authority (OCA) may delegate declassification and downgrading authority to officials with technical knowledge of classified programs, projects and plans, provided such delegations are in writing to ECJ2-SSO and specify the information categories the official may act upon. (See Appendix 16)

Page 39, paragraph C4.3, Automatic Declassification at 25 years. See Appendix 17 for specific guidance for management of this program.

Page 39, paragraph C4.9.2.4.5, Classification Challenges. Add the following:

C4.9.2.4.5. Send challenges to classification of non-USEUCOM originated information through command channels to ECJ2-SSO. In other cases, send challenges to the security manager of the USEUCOM element or component originating the classified information. Use DA Form 1575 to make a formal challenge. Enter the rationale supporting the challenge in the "Remarks" section of the form. When it is probable that the originator may not be able to determine what document or material is being challenged, the challenger will include a copy of the document or material with DA Form 1575.

Chapter 5
MARKING

Table of Contents

Paragraph

C5.1.1	Marking and Designation Rules
C5.2.1.5	Overall Classification Marking
C5.2.7.1.2	Identification of specific Classified Information
C5.2.9.2	Special Control and Similar Notices
C5.2.9.4	COMSEC Information
C5.2.9.6	Special Access Program Documents (Restrains on Special Access Requirements)
C5.2.9.8	Other Special Notices (Foreign Intelligence Information)
C5.3.3	Classification by Compilation (Travel of Senior Officials; Classification of General/Flag Officer Itineraries)
C5.4.8.3	Removable AIS Storage Media
C5.4.12	Exceptions(1 through 10)
C5.7.6	Posting of Unclassified or Downgraded Classified Materials on the Internet

CHAPTER 5 MARKING

Page 41, paragraph C5.1.1, Marking and Designation Rules. Add the following subparagraphs:

C5.1.1.7. The holder of improperly marked classified documents must contact the document originator to obtain correct marking information.

C5.1.1.8. Particular care must be taken when reproducing classified documents to ensure that classification markings and associated markings are distinct and conspicuous on the reproduced copies.

C5.1.1.9. Documents will be remarked or stamped by hand to ensure legibility when markings are not clearly visible on reproduced copies.

C5.1.1.10. To avoid confusion and improper handling of classified information on EUCOM computer systems, computerized documents, working papers, databases, briefings and any other data files containing classified information must be marked with the highest classification level of the information within the file. Classification markings within the computer file should follow standard policy on paper document markings (headers and footers) and have appropriate paragraph markings. These markings should be visible when the document is printed or e-mailed. Working papers and files should, at a minimum, have a classification level at the beginning of the document or have page markings of the highest classification of information in the document. All diskettes, tapes and other data storage materials used by EUCOM personnel will be labeled with the highest classification level of the information contained. All diskettes used at EUCOM will be labeled. The holder of unmarked data storage devices (diskettes, tapes, etc.) is responsible for protecting that media at the highest level of systems in that area until the contents of the media are determined to be of a lower classification level. Unless EUCOM special handling procedures are used when using unclassified computer media in classified systems, any computer media that is used in classified systems will be marked with the highest classification level of the system and appropriately protected.

Page 42, C5.2.1, Overall Classification Markings. Add:

C5.2.1.5. Documents twenty pages or less shall bear overall page markings commensurate to the highest level of classification assigned to the portion markings contained on that page.

Page 51, paragraph C5.2.7.1.2, Identification of Specific Classified Information. Add the following:

Computer databases or other programs, which do not allow the user to appropriately mark document pages, should be identified as classified using the document summary area or in the filename/title of the document.

Page 53, paragraph C5.2.9.2, Special Controls and Similar Notices. Add the following:

Information bearing the prescribed warning notices shall not be disseminated outside authorized channels without the consent of the originator. Access to and dissemination of Restricted Data by DOD personnel shall be subject to DOD Directive 5210.2.

Page 53, paragraph C5.2.9.4, COMSEC Material: Add the following:

COMSEC information shall be disseminated in accordance with NACSI 4005 and implementing instructions.

Page 53, paragraph C5.2.9.6, Restraints on Special Access Requirements. Add:

Special requirements with respect to access, distribution, and protection of classified information shall require prior approval in accordance with Chapter VIII.

Page 53, paragraph C5.2.9.8, Other Special Controls and Similar Notices, (Foreign Intelligence Information). Add: Dissemination of foreign intelligence information shall be in accordance with the provisions of DOD Instruction 5230.22.

Page 55, paragraph C5.3.3, Classification by Compilation, (Travel of Senior Officials, Classification of General/Flag Officer Itineraries). Add subparagraphs:

C5.3.3.1. Detailed itineraries, which contain the overall schedule with arrival/departure times and places, of all general/flag officers and civilian equivalents, except for "high risk targets", will be marked at least "For Official Use Only" when traveling anywhere within the USEUCOM area of responsibility. When preparing and coordinating itineraries, the office of primary responsibility for the visitor should review the threat and apply more stringent controls to include classification IAW this directive on a case-by-case basis. In instances where this is necessary, classify at the "Confidential" level and mark itineraries in the same manner as those for "high risk targets", as shown below.

C5.3.3.2. Detailed itineraries, which contain the overall schedule with arrival/departure times and places, will be classified at the "Confidential" level when associated with senior leader "high risk targets". High-risk targets include the HQ USEUCOM Commander, Deputy Commander, Chief of Staff, and component command counterparts. Itineraries will be marked as follows:

Derived from: USEUCOM Supplement 1 to DOD 5200.1-R/ the compilation of unclassified information reveals detailed information on the principal's itineraries, and places them in eminent danger.

Declassify On: Completion of visit or trip

C5.3.3.3. In all instances, particular attention should be given to OPSEC. Itineraries should be protected to the maximum extent practicable by means of secure communications, personal contact, and limited distribution. Trips may be announced in advance, but press releases should not contain precise arrival/departure times and places. Only necessary coordination and administrative arrangements to develop and execute the itinerary may be handled as FOUO.

Release of information to Host nation authorities should be limited, but is authorized to facilitate security arrangements and support for principal.

Page 59, paragraph C5.4.8.3, Removable AIS Storage Media. Add the following:

All output shall be labeled and protected at the highest classification level of the information handled by the AIS until manually reviewed by an authorized person to ensure that the output was marked accurately with the classification and caveats. Special consideration should be given to the possibility of information being copied in "slack space" or other hidden areas of a file

when labeling diskettes which have been used in classified systems. When in doubt, assume the information on the diskette or media is classified. All questions in regard to secure copying of information from classified systems in the EUCOM AOR should be addressed to EUCOM J6-I. Consult EUCOM Directive 25-5, Security Requirements for Automated Information Systems, for more information.

Page 60, paragraph C5.4.12, Exceptions. Add the following paragraph and subparagraphs:

Use the following parenthetical symbols for documents, which contain intelligence and NATO information IAW subsections 2 and 3 of Chapter 5.

1. Use "(OC)" for ORCON information.
2. Use "(PR)" for PROPIN information.
3. Use "(CTS)" for Cosmic Top Secret information.
4. Use "(CTSA)" for Cosmic Top Secret Atomal information.
5. Use "(NS)" for NATO Secret information.
6. Use "(NSA)" for NATO Secret Atomal information.
7. Use "(NC)" for NATO Confidential Information
8. Use "(NCA)" for NATO Confidential Atomal information.
9. Use "(NR)" for NATO Restricted information.

Page 65, paragraph C5.7.6, Posting of Unclassified or Downgraded Classified Materials on the Internet. Add the following: Due to the instant and worldwide nature of the Internet, commands in the EUCOM AOR are strongly advised to exercise due diligence before posting previously classified or unclassified information on the Internet. Simply because information is unclassified is not sufficient justification to post the material on the World Wide Web. Unclassified does not necessarily translate into releasable to all countries and individuals on the Internet. Even unclassified data can provide a potential adversary with a wealth of useful information. This

process is vital to protecting sensitive information. Once a document is posted on the Internet, it can be copied thousands of times in seconds and can never be fully retracted.

C5.7.6.1. Commanding Officers are responsible for the content of any command Internet sites. All commands in the EUCOM AOR are required to have a vetting process with inputs from Security, Intelligence and Public Affairs to decide the sensitivity of all documents posted on the Internet. Consideration should be given to limiting the accessibility of such information to certain IP 1-R address groups such as military and U.S. Government only or other restrictions on access.

C5.7.6.2. If the primary consumer of the unclassified information is the HQ USEUCOM staff, another DoD organization, or a small subset of a principle audience, then the preferred means of dissemination may be the HQ USEUCOM Secret Local Area Network (SLAN), the Secret Internet Protocol Network (SIPRNET), unclassified e-mail, or other means separate from posting on the World Wide Web, as practicable and/or appropriate.

Chapter 6 SAFEGUARDING

Table of Contents

Paragraph

C6.1.3 Dissemination of Classified Information

- C6.1.3.1 a. NATO Atomic, NATO Cosmic Top Secret, NATO Secret Information
- C6.1.3.2 b. Policy
- C6.1.3.3 c. Dissemination of Top Secret Information
- C6.1.3.4 d. Dissemination of Secret & Confidential Information
- C6.1.3.5 e. Scientific and Technical Meetings
- C6.1.3.6 f. Limited Dissemination (LIMDIS)

C6.2.1 Policy

C6.2.2.8 Access by Persons Outside the Executive Branch (Information Originating in a NON-DOD Department or Agency)

C6.2.3 Visits

C6.2.4 Access Required by Other Executive Branch Investigative and Law Enforcement Agents

C6.3.2 Care During Working Hours

C6.3.2.7 Cell Phones and Other Similar Communications Devices

C6.3.3 End of Day Security Checks

C6.3.4 Emergency Planning

C6.3.6 Removal of Classified Storage Equipment

C6.3.7 Secure Communications, and Storage of up-to Secret Classified Material in Personal Residences

C6.3.8 Classified Meetings and Conferences

C6.4.1 General Policy

C6.4.3.7 Storage of Classified Information (Open Storage)

C6.4.3.8 Storage of Classified Information (Storage Prohibitions)

C6.4.6.2.1 Equipment Designations & Combinations to Containers

C6.5.3.7 Control Procedures

C6.7.2 Policy

C6.7.2 Methods and Standards

CHAPTER 6 SAFEGUARDING

PAGE 66, Dissemination of Classified Information. Add:

C6.1.3. Dissemination of Classified Information

C6.1.3.1. NATO Atomal, NATO Cosmic Top Secret, NATO Secret. NATO Secret Cosmic and Atomal Information will be controlled on HQ USEUCOM Form 25-13, USEUCOM Classified Materials Register. Removable ADP media (diskettes or cartridges) containing NATO information will also be accounted for on the HQ USEUCOM Form 25-13, commensurate to the level of classified information contained on the media. It is not permitted to process, view or edit NATO classified on systems not specifically cleared for its use. The U.S. SIPRNET connected systems in the EUCOM AOR are not permitted to process NATO classified. See your local system administrator or ISSM for further guidance.

C6.1.3.2. Policy. The originating official or activity may prescribe specific restrictions on dissemination of classified information when necessary. Particular emphasis shall be placed on traditional need-to-know measures to aid in the strict control of classified information.

C6.1.3.3. Dissemination of Top Secret Information.

C6.1.3.3.1. Top Secret information, originated within the Department of Defense, may not be disseminated outside the Department of Defense without the consent of the originating DOD Component or higher authority.

C6.1.3.3.2. Top Secret Information, whenever degradable from classified portions bearing lower classifications, shall be distributed separately.

C6.1.3.3.3. Standing distribution requirements for Top Secret information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

C6.1.3.4. Dissemination of Secret and Confidential Information.

C6.1.3.4.1. Secret and Confidential information, originating within the Department of Defense, may be disseminated within the Executive Branch, unless prohibited by the originator.

C6.1.3.4.2. Standing distribution requirements for Secret and Confidential information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

C6.1.3.5. Scientific and Technical Meetings

Use of classified information in scientific and technical meetings is subject to the provisions of DOD Directive 5200.12.

C6.1.3.6. Limited Dissemination (LIMDIS)

This subsection establishes limits on measures for the protection of information beyond those involving access to classified information per se, but not so stringent as to require the establishment of a Special Access Program. It prohibits use of terminology indicating enhancements to need-to-know, such as Special Need to Know (SNTK), MUST KNOW, Controlled Need to know (CNTK), or other similar security upgrade designations and associated unique security requirements such as specialized nondisclosure statements. Limited dissemination controls are the only security enhancement short of a Special Access Program, which may be employed for control over specific information for specified periods of time. In this context, these procedures may be initiated and continued, showing that additional access controls are required in order to assure the security of the designed information. The decision to apply these procedures shall be made at the original classification authority level of command or supervision in accordance with the DOD Component. Except by agreement, such requirements shall not be imposed outside of the approving DOD Component. LIMDIS protective measures are restricted to one or more of the following:

C6.1.3.6.1. Decentralized maintenance of disclosure listings, briefings concerning access limitations and physical security restrictions limited to requirements such as placing the material in sealed envelopes within approved storage containers to avoid inadvertent disclosure and the commingling with other files;

C6.1.3.6.2. Using unclassified nicknames (no code words may be assigned to LIMDIS information);

C6.1.3.6.3. Marking the material as LIMDIS along with the assigned nickname;

C6.1.3.6.4. Marking inner envelopes containing designated LIMDIS information with the notation: "To be Opened Only by Personnel Authorized Access";

C6.1.3.6.5. Requiring electronically transmitted messages containing designated information to be marked with the uniform caveat LIMDIS; and

C6.1.3.6.6. Prescribing unique oversight procedures to be accomplished by Component professional security personnel (industrial security inspections will be conducted in the normal manner by the Defense Security Service).

PAGE 67, paragraph C6.2.1, Policy. Add the following:

Due to the volume of information and worldwide connectivity of today's U.S. military classified networks, extreme diligence should be exercised when giving anyone access to these systems.

PAGE 69, paragraph C6.2.2.8, Information Originating in a NON-DOD Department or Agency. Add the following:

C6.2.2.8. Except under rules established by the Secretary of Defense, or as provided by Section 102 of the National Security Act, classified information originating in a department or agency other than Department of Defense shall not be disseminated outside the Department of Defense without the consent of the originating department or agency.

PAGE 69, paragraph C6.2.3, Visits. Add the following paragraph and subparagraphs:

Procedures shall be established to control access to classified information by visitors. (DoD Instruction 5230.20 provides further guidance regarding foreign visitors.)

C6.2.3.1. Except when a continuing, frequent working relationship is established, through which current security clearance and a need-to-know are determined, its contractors, and other agencies shall provide advance notification of the pending visit that establishes the visitor's security clearance and the purpose of the visit. Visit requests shall be signed by an official other than the visitor who is in a position to verify the visitor's security clearance.

C6.2.3.2. Visit requests will normally be on official letterhead stationary and include the following:

C6.2.3.2.1. Full name, date and place of birth, social security number, and rank or grade of visitor;

C6.2.3.2.2. Security clearance of the visitor;

C6.2.3.2.3. Employing activity of the visitor;

C6.2.3.2.4. Name and address of the activity to be visited;

C6.2.3.2.5. Date and duration of proposed visit;

C6.2.3.2.6. Purpose of visit in sufficient detail to establish need-to-know; and

C6.2.3.2.7. Names and phone numbers of persons to be contacted for confirmation.

C6.2.3.3. Visit requests may remain valid for not more than 1 year

Page 69, Add paragraph C6.2.4, Access Required by Other Executive Branch Investigative and Law Enforcement Agents

Normally, investigative agents of other departments or agencies may obtain access to DOD information through established liaison or investigative channels. When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA, or Secret Service agents may obtain access to DoD information as required by its classification. Before any public release of the information so obtained the approval of the head of the activity or higher authority shall be obtained.

Page 70, paragraph C6.3.2, Care During Working Hours. Add the following subparagraphs:

C6.3.2.3. Distinctively marked burn bags will be used for the collection of classified waste. Burn bags containing classified waste must be protected IAW established procedures for the level of classified material contained within.

C6.3.2.4. Custodial, maintenance, and construction personnel and all other uncleared personnel will be escorted at all times while in offices and controlled areas to prevent unauthorized access to classified material. Escorts will remain with custodial and uncleared personnel unless another responsible person accepts escort responsibilities. Elements are responsible for providing escorts in their own areas.

C6.3.2.5. Classified material will not be carried loose when being hand carried between buildings. Such material will be carried in a briefcase or other suitable container not bearing classification markings.

C6.3.2.6. Reversible "OPEN-CLOSED" or "OPEN-LOCKED" signs will be used on each security container and secure area in which classified information is stored.

C6.3.2.7. Cell phones and other similar communications devices (i.e. radios), which provide non-secure communications, are prohibited from being operated in any areas where classified or sensitive information is discussed or processed. If they are carried into such areas they must be turned off and batteries removed.

Page 70, paragraph C6.3.3, End of Day Security Checks. Add the following paragraph and subparagraphs:

C6.3.3.1. Persons discovering a security container or secure facility open and unattended will:

C6.3.3.1.1. Keep the container or storage area under guard or surveillance.

C6.3.3.1.2. Notify the element security manager and one of the persons listed on Part 1, SF 700, affixed to the inside of the container or storage area. If one of these people cannot be contacted, the duty officer or element chief will be notified.

C6.3.3.1.3 The Security Manager or the individual contacted will:

C6.3.3.1.3.1 Report personally to the location; check the contents of the container or area for visible indications of tampering, theft, or compromise. If any evidence of tampering, theft, or compromise is noted, installation or activity security personnel will be immediately notified so that an investigation can be initiated. The custodian will conduct an inventory of the container contents and report any discrepancies immediately.

C6.3.3.1.3.1 When tampering is evident, the custodian will contact their Security Manager and ECJ2-SSO immediately. Do not touch until investigators have cleared the scene. Change the combination and lock the container as soon as possible, once the investigative offices have completed their assessment. If the combination cannot be changed immediately, the security container will be secured and placed under guard until the combination can be changed, or the classified contents will be transferred to another security container or secure area.

C6.3.3.1.3.2 Report the incident to ECJ2-SSO within 24 hours or the next duty day.

Page 71, paragraph C6.3.4, Emergency Planning. Add the following subparagraphs:

C6.3.4.4. Emergency plans will be labeled "For Official Use Only." The plan will be filed as the first document in the locking drawer of each security container or in an area deemed appropriate by the security manager.

C6.3.4.5. Elements will conduct, at a minimum, semiannual drills to determine the adequacy of emergency plans. A record of these drills will be maintained by the element security manager.

Page 71, paragraph C6.3.6, Removal of Classified Storage Equipment. Add:

C6.3.6.1 Procedures for TURN IN of Security Containers:

C6.3.6.1. Security container drawers **must** be removed and the container physically examined to ensure NO classified material has been lodged behind the drawers. Removing the container drawers is the **only way** you can guarantee that all classified material has been recovered.

C6.3.6.2. Next, set the combination to the factory setting, 50-25-50 and post combination along with name phone number of individual responsible for clearing the container and the date cleared.

C6.3.6.3. Contact DOL for instructions on transportation and turn-in procedures.

Paragraph C6.3.7, Communications & Storage of up-to Secret Classified Material in Personal Residences. Add the following:

C6.3.7.1 Secure communications, and storage of up-to Secret classified material in personal residences must be approved by the USEUCOM Chief of Staff prior to installation. Approval will only be given when residences are located on US controlled installations, and will not be authorized for personal convenience. Requests must be processed through ECJ2-SSO for recommendation, prior to forwarding to the Chief of Staff.

C6.3.7.2 Requests should be from the Director of the requesting organization and forwarded through ECJ2-SSO to the Chief of Staff for consideration and recommendation. On receipt of requests for secure storage/communications in residents, ECJ2-SSO will contact the Directorate

XO to arrange for a security survey of the residence, prior to submission of the request to the Chief of Staff.

C6.3.7.3 Where such communications units and storage are permitted, care must be exercised to ensure that unauthorized personnel, to include family members, are not within hearing/seeing distance when classified discussions or communications take place, and that the control key for the communications unit is either personally retained or stored in the GSA security container. In some cases, it may be necessary for the custodian/user of the unit to make notes regarding the classified discussion that occurs over the secure telephone. When this occurs, such classified notes (and accompanying notepads, which may have impressions or carbons of notes) can be retained in the personal residence only until the next duty day. If the next duty day falls during a period of more than one day, leave, temporary duty (TDY), or other absence, the material will be delivered to a U.S. Government or cleared contractor facility for storage prior to such absence. While in a personal residence, such classified notes will be safeguarded in a GSA approved safe, or under the personal, physical control of the authorized, cleared holder of the notes, at all times.

Page 73, paragraph C6.3.8, Classified Meetings and Conferences. Add subparagraph C6.3.8.1.11:

(11) In order to ensure compliance with the appropriate regulations, ECJ2-SSO will be notified immediately of plans to conduct classified meetings and conferences.

Page 75, paragraph C6.4.1, General Policy. Add:

C6.4.1.1. US Missions will store and safeguard classified and administratively controlled materials in accordance with applicable regulations and policies of both the Department of State and the Department of Defense. At facilities approved for storage of classified information, the Regional Security Officer will designate controlled access areas and establish supervisory controls over the distribution and storage of classified and administratively controlled materials. All USEUCOM field element offices are subject to accreditation of classified storage areas by the Department of State. See DOD Instruction 5210.84 for additional information on requirements for organizations falling under Embassy Chiefs of Mission.

C6.4.1.2. DOD has agreed to comply with DOS minimum security standards. In those cases where DOD standards exceed DOS requirements, the DOD component office coordinates required upgrades with the DOS Regional Security Officer. If the Regional Security Officer and the Field Element Chief cannot agree on the level of upgrade, they will refer the disagreement through the Chief of Mission to the Department of State, and through Headquarters United States European Command (ECJ4/ECJ2-SSO-IP) to the Defense Intelligence Agency in Washington, DC and request resolution of the matter.

Page 78, paragraph C6.4.3, Storage of Classified Information. Add:

C6.4.3.7. Open Storage. Open storage will only be approved for material too large for containers; for bulk material that must be reviewed on a daily basis making storage in containers impractical; or for instances when classified containers are not available. Secure storage

facilities for open storage of classified material will be established in accordance with the following:

C6.4.3.7.1. Field elements located in facilities that fall under the jurisdiction of the Department of State will obtain DOS approval for open storage. Requests will be submitted IAW DOS procedures. All other HQ USEUCOM field elements will obtain HQ USEUCOM ECJ2 approval for open storage.

C6.4.3.7.2. A memorandum designating the area as an open storage facility will be posted on or near the inside of the locking door to the facility. Facilities not possessing a memorandum of designation will contact ECJ2-SSO to determine what actions are necessary.

C6.4.3.7.3. Open storage facilities will be reevaluated annually by ECJ2-SSO during security staff assistance visits and recertified each time a structural change occurs to the open storage facility. Anytime there are structural changes to an approved area, requests for recertification will have to be processed through ECJ2-SSO for ECJ2 approval.

C6.4.3.7.4. HQ USEUCOM Directorates desiring storage of classified information in an open configuration will submit written requests through ECJ2-SSO for final approval. Include as a minimum justification, description of the type and quantity of material to be stored, and a statement identifying existing physical security measures present in the storage facility. Prior to submission of the written request for open storage ECJ2-SSO must conduct a physical security survey of the space to ensure the area meets the construction criteria for Class B vault, vault-type room, strong room, or secure storage room including an approved alarm system.

C6.4.3.8. Storage Prohibitions.

C6.4.3.8.1. Do not store funds, weapons, medical security items, controlled drugs, precious metals, or other items susceptible to theft, in any security type equipment, including vaults and vault-type rooms, which store classified material. Chief of Staff may waive this requirement in emergencies, or temporarily when acceptable storage containers are not available.

C6.4.3.8.2. Security equipment purchased for the use of storing classified material will not be used for routine storage of supplies and other non-administrative unclassified material.

C6.4.3.8.3. Security containers will not be used to solely store wholly unclassified material.

C6.4.3.8.4. Interiors of each security container drawer, vault or storage room will be marked with numeric 1, 2, and 3 stickers to indicate the priority of its contents for destruction. Within SCIF facilities, these stickers may be placed on the outside of security containers.

Page 79, paragraph C6.4.6.2.1, Combinations to Containers. Add the following subparagraphs:

C6.4.6.2.1.5. Every 12 months when NATO information is stored in the security container.

C6.4.6.2.1.6. Persons having knowledge of combinations to containers containing NATO material will be briefed and sign the NATO briefing statement.

Page 82, paragraph C6.5.3 Control procedures. Add:

C6.5.3.7. Individuals reproducing classified material will, upon completion, run an additional 2 sheets through equipment to determine presence of latent images. Destroy these sheets as classified waste. Printers and fax machines used for processing classified will contact the unit's security managers for instructions for turn-in of toner cartridges.

Page 84, paragraph C6.7.1.2, Policy. Add the following subparagraphs:

C6.7.1.2.1. The first Wednesday in February is the HQ USEUCOM annual clean-out day.

C6.7.1.2.2. A quarterly purge of classified holdings will be conducted.

Page 84, paragraph C6.7.2, Methods and Standards. Add paragraphs:

C6.7.2.3 An aggressive downgrading and destruction program contributes to effective emergency planning. USEUCOM elements will review at least 25 percent (or 3 linear feet, whichever is more) of classified holdings each quarter to determine whether or not the material may be destroyed, declassified, or downgraded.

C6.7.2.4 Procedures for TURN IN of classified computers and storage media.

All computer systems and media used to process classified materials at HQ USEUCOM will be re-utilized and disposed of in accordance with guidance from the supporting information assurance office (i.e. ISSO, ISSM). Security Managers will ensure all media (diskettes, CD-ROMs, etc.) are removed prior to turn-in. Computers will not be turned in to DRMO unless hard-drives are removed.

Chapter 7
Transmission and Transportation

Table of Contents

Paragraph

C7.1.2.4 Top Secret Information

C7.1.3.11 Secret Information

C7..2.1.3 Envelopes or Containers

C7.3.3 Hand-carrying or Escorting Classified Material Aboard Commercial
Passenger Aircraft

CHAPTER 7
TRANSMISSION AND TRANSPORTATION

Page 88, paragraph C7.1.2.4, Top Secret Information. Add the following to subparagraph:

Within HQ USEUCOM, the EUCOM Courier will provide this service.

Page 90, paragraph C7.1.3, Secret Information. Add:

C7.1.3.11 Use a receipt when entering Secret material into a mail distribution system, secondary distribution systems, or the US Postal Service.

Page 92 paragraph C7.2.1, Envelopes or Containers. Add:

C7.2.1.3 Top Secret Register Pages (EUCOM Form 23-15) may be used as a receipt when transferring Top Secret material from one TSCA to another on the same installation. This applies to releasing Top Secret messages and computer input data products to telecommunications facilities, data processing installations, and data processing centers for secondary transmission or data processing.

Page 97, paragraph C7.3.3, Hand-Carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. Add:

C7.3.3.3. HQ USEUCOM Directors/Office Chiefs are authorized to approve memos requesting to hand-carry classified aboard commercial aircraft.

C7.3.3.4. All USEUCOM personnel escorting or hand-carrying classified outside their normal work area require authorization for such action. A verbal approval from the individual's supervisor is sufficient when hand-carrying between buildings or areas where the travel does not pass through a known or probable site of a DOD inspection point (gate entrances to installations, entries to facilities controlled by guards and so forth). Within the Greater Stuttgart area, individuals issued the EUCOM badge are authorized to act as a courier. The DD Form 2501, Courier Authorization Card will be used for travel outside the Greater Stuttgart area but within Germany. Written authorization is required for all other cases not covered in Chapter 7, section 3 of DOD 5200.1-R). In addition, all personnel will use a briefcase, or other closed container to prevent loss or observation of classified material being hand-carried outside work areas.

C7.3.3.5. Personnel hand-carrying classified information aboard Government or Commercial Aircraft will comply with the provisions listed in paragraph C7.3.3.

C7.3.3.6. The Security Manager (or other responsible office) will maintain a log for each hand-carry authorization, as well as, a list of material being carried (should a compromise occur).

Chapter 8
Special Access Programs

Table of Contents

Paragraph

C8.1.3.3	Control and Administration
C8.1.4.4.9.	Establishment of DoD Special Access Programs, (Contract Security Classification Specification)
C8.1.4.5.3.5	"Carve Out" Contracts
C8.1.4.7.1	Establishment of DoD Special Access Programs
C8.1.5.1	Review of Special Access Programs
C8.1.9.3	Termination and Transitioning of SAPs

CHAPTER 8
SPECIAL ACCESS PROGRAMS

Page 100, paragraph C8.1.3.3, Control and Administration. Add:

HQ USEUCOM/ECJ2-SSO (IP) is the central point of contact for all HQ USEUCOM Special Access Programs. They will maintain a listing of all HQ USEUCOM Special Access Program Focal Point Officers and program nicknames. Special Access Program (SAP) list will be updated annually.

Page 103, paragraph C8.1.4, Establishment of DoD SAPs, (Contract Security Classification Specifications). Add the following:

C8.1.4.4.9.1 If classification considerations are simple (or brief), a properly completed DD Form 254 will suffice.

C8.1.4.4.9.2 Reviews will be made at the same time as reviews of associated security classification guides. Reviews of DD Form 254 will consider any difficulties or problems that have surfaced during use of the guidance and should ensure that:

C8.1.4.4.9.1. All classification guidance required by the contractor is provided.

C8.1.4.4.9.1.2. The classification decisions involved have been personally approved by an individual with the requisite classification authority.

C8.1.4.4.9.1.3. The guidance is current and conforms with that found in other sources.

C8.1.4.4.9.1.4. The guidance is specific and unambiguous. Any problems encountered with interpretation of the guidance must be carefully considered and resolved.

Page 105, paragraph C8.1.4.5.3.5, "Carve Out" Contracts. Add.

USEUCOM elements sponsoring a Special Access Program affecting a contractor will use DD Form 254 as the legally binding instrument. ECJ2-SSO (IP) will be provided one copy of the completed DD Form 254 for submission to the Director, DSS.

Page 106, paragraph C8.1.4.7, Establishment of DOD Special Access Programs. Add:

C8.1.4.7.1. HQ USEUCOM activities planning to establish a Special Access Program, or to participate in a program directed by another DOD Component must send a recommendation for establishment or participation through command channels to ECJ2-SSO (IP). The request must contain the information identified in DOD 5200.1R, Chapter 8.1.4.5.3.4. ECJ2-SSO (IP) reviews the recommendation and takes the following action:

C8.1.4.7.1.1. Forwards the request to the Chief of Staff for concurrence and ensures the request is submitted to The Deputy Under Secretary of Defense for Policy (DUSD(P)) for approval.

C8.1.4.7.1.2. Returns all Chief of Staff non-concurrences to the recommending activity.

Page 106, paragraph C8.1.5.1, Review of Special Access Programs. Add:

The Special Access Program Manager of each approved USEUCOM program will ensure the conduct of annual reviews and document these reviews each December.

Page 109, paragraph C8.1.9.3, Termination and Transitioning of SAPs. Add:

The Special Access Program Manager responsible for the approved Special Access Program sends SAP termination reports to ECJ2-SSO as required. ECJ2-SSO will forward report to DUSD(P).

Chapter 9
Security Education

Table of Contents

Paragraph

C9.1.1.5	General Policy
C9.2.1	Cleared Personnel
C9.3.2.9	Original Classifiers
C9.3.4.11	Derivative Classifiers, Security Personnel and Others
C9.3.5.7	Other (Additional Briefing Requirements)

CHAPTER 9
SECURITY EDUCATION

Page 110, paragraph 9-C9.1.1.5, General Policy. Add subparagraph (e):

C9.1.1.5. ECJ2-SSO conducts oversight of the USEUCOM Information Security Program. ECJ2-SSO will:

C9.1.1.5.1. Provide technical guidance and assistance to element security managers.

C9.1.1.5.2. Ensure that security education requirements outlined within this chapter are complied with.

C9.1.1.5.3. Conduct Staff Assistance Oversight Reviews (SAR) of component, HQ USEUCOM staff and field element information security programs.

C9.1.1.5.4. Assist in the training of Information Security Managers.

Page 110, paragraph C9.2.1, Cleared Personnel. Add the following:

C9.2.1.3. Security Education training is done in two phases: Indoctrination and recurring training.

C9.2.1.4 Information security indoctrination and recurring training, as a minimum, will include all subject areas listed in chapter nine of the DOD 5200.1-R. USEUCOM element chiefs will ensure indoctrination and recurring training programs are established and conducted properly.

C9.2.1.5. Indoctrination training will be conducted within 30 days of an individual's arrival at USEUCOM elements. For those members arriving on temporary duty (TDY) assignments, the host element chief provides indoctrination training as required by the specific mission of the TDY. Recurring training will be conducted annually at a minimum.

C9.2.1.6. Records of all security education training will be maintained by the element security manager. Records will include: target audience, date training was conducted, and subjects presented.

Page 113, paragraph C9.3.2, Original Classifiers. Add:

C9.3.2.9. A videocassette production titled, "Classification Management: A Decision Making Process" satisfies the indoctrination discussed in paragraph 9-301. ECJ2-SSO also has briefing slides available for conduct of this training.

Page 114, C9.3.4, Derivative Classifiers, Security Personnel and others. Add the following:

C9.3.4.11. Appointed Security Managers will:

C9.3.4.11.1. Conduct semiannual self-inspections of their elements. Results will be maintained on file for one year.

C9.3.4.11.2. Conduct and document indoctrination and recurring briefings.

C9.3.4.11.3. Develop a Standard Operating Procedure pertaining to the security operations of their particular element. Organizations assigned to HQ USEUCOM at Patch Barracks will use the "HQ USEUCOM Information Security Operating Instruction". Directorate/Staff Office specific instructions should be developed to supplement this instruction.

C9.3.4.11.4. Maintain a continuity notebook, which includes but is not limited to the following:

C9.3.4.11.4.1. Security Manager and Top Secret Control Officer Letters of Appointment.

C9.3.4.11.4.2. Area and/or Office Standard Operating Procedures or Memorandums referring to Security Procedures and Policies.

C9.3.4.11.4.3. Documentation of Training and Briefings.

C9.3.4.11.4.4. DOD 5200.1-R, Information Security Program Regulation as supplemented.

Page 114, Other - Additional Briefing Requirements. Add:

C9.3.5.7. The following Special Briefings are required to be conducted:

C9.3.5.7.1. When an employee is authorized to carry or escort classified material

C9.3.5.7.2. When an employee is granted access to Sensitive Compartmented Information or information subject to special access program controls (if the program so requires).

C9.3.5.7.3. When an employee is granted access to NATO classified information.

C9.3.5.7.4. Each year requirements for counterintelligence briefings will be coordinated by the directorate security manager with the local Military Intelligence (MI) units. Security Managers will be responsible for coordinating with MI to obtain this brief and Field elements located at DOS locations should coordinate these briefings with the Regional Security Officer.

Chapter 10
ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

Table of Contents

Paragraph

C10.1.1.4	Policy
C10.1.2.2	Reporting (Responsibility of Discoverer)
C10.1.3.1	Inquiry/Investigation (Preliminary inquiry) Add subparagraphs (c,d, and e)

CHAPTER 10
ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

Page 117, paragraph C10.1.1, Policy. Add:

C10.1.1.4. Field element offices located at Department of State facilities will, in addition to this supplement, follow the security violations reporting procedures established in Department of State regulations and policies.

Page 117, paragraph C10.1.2.2, Responsibility of Discoverer. Add:

Additionally, report this information to HQ USEUCOM (ECJ2-SSO) within 24 hours or the next duty day.

Page 119, paragraph C10.1.3.1, Preliminary Inquiry. Add:

C10.1.3.1.7. The preliminary inquiry must follow the format in Appendix N and be initialed by the staff element director or chief to indicate concurrence with the recommendations and corrective actions as stated in the preliminary inquiry. Additionally, this report must be submitted to HQ USEUCOM (ECJ2-SSO) within ten working days after the initial 24 hour notification to HQ USEUCOM. If during the conduct of an inquiry it is discovered that the possibility of espionage, subversion or deliberate acts of compromise were involved in the violation, immediate notification will be made to the Security Support Office, ECJ2-SSO.

C10.1.3.1.8. Actual or potential compromises at HQ USEUCOM and at commands in the EUCOM AOR dealing with computer networks, computer media, e-mail, or any other computerized systems will also be reported to ECJ6-I within 5 working days of the incident. Actual or potential compromises dealing with computer intrusions must be reported to ECJ6-I immediately due to the need for evaluation of counterintelligence, criminal or technical options and ramifications. Incident reports are classified FOUO and must be protected appropriately.

C10.1.3.9. Individuals appointed as investigating officer by ECJ1 on official orders will be briefed by an attorney from the HQ USEUCOM Legal office, (ECJA).

Page Inserts. Insert pages AP10-1 through AP 17-3 (Appendixes 10 - 17).

APPENDIX 10
ACCOUNTABILITY AND CONTROL OF CLASSIFIED INFORMATION

a. Top Secret information.

1. Control Officers. Top Secret Control officers (TSCOs) and alternates shall be designated within offices to be responsible for receiving, dispatching, and maintaining accountability registers of Top Secret documents. Such individuals shall be selected on the basis of experience and reliability, and shall have Top Secret security clearances. TSCOs need not be appointed in those instances where there is no likelihood of processing Top Secret documentation.

2. TSCO will at a minimum:

(a) Maintain a Top Secret Register.

(b) Receive, sign for, and dispatch all Top Secret material transmitted to or from the elements they serve; and maintain receipt for Top Secret material dispatched or transferred.

(c) Conduct periodic checks within the element to ensure the proper handling and safeguarding of Top Secret information.

(d) Monitor the reproduction of Top Secret material.

(e) Ensure persons having custody of Top Secret material are properly relieved of accountability before they depart on leave or temporary duty for more than 45 days, or when they are transferred, reassigned, separated, retired, or otherwise change status with regard to custody or possession of Top Secret material.

(f) Report any action or omission by personnel, which violates rules for safeguarding and controlling Top Secret information to the element chief or element security manager and ECJ2-SSO.

b. Accountability.

1. Top Secret Registers. Top Secret materials maintained in an approved Sensitive Compartmented Information Facility (SCIF) may be managed in the same manner as SCI information. However, materials not maintained in a SCIF, and Top Secret materials removed from a SCIF on a permanent basis shall be entered into the following system of control and accountability:

(a) Top Secret accountability registers shall be maintained by each office originating or receiving Top Secret information. Active register pages will be maintained until placed inactive, and shall, as a minimum, reflect the following:

(1) Sufficient information to identify adequately the Top Secret document or material to include the title or appropriate short title, date of the document, and identification of the originator;

(2) The date of the document or material was received;

(3) The number of copies received or later reproduced; the disposition of the Top Secret document or material and all copies of such documents or materials.

(4) Assign a consecutive number to each register by including the calendar year and TSCA functional address symbol; for example: 02-ECJ1-0043. Use the alphabetical letter A, B, C and so on to prepare continuation pages to the basic form.

(5) Each register will remain active until it is made inactive; for example: transferring material to another TSCO; destroying the material; posting entries to; or incorporating with another recorded document; or downgrading and/or declassifying based on proper authority.

(6) Inactive registers will be maintained on file for two calendar (2) years.

(7) Receipts of Top Secret documents and material will be accounted for by a continuous chain of receipts. Receipts shall be maintained for two calendar (2) years.

(8) Retention of Top Secret information shall be retained only to the extent necessary to satisfy current requirements. Custodians shall destroy non-record copies of Top Secret documents when no longer needed. Record copies of documents that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

2. Top Secret material, including removable ADP Media (diskettes and cartridges), will be accounted for on USEUCOM Form 25-13, Top Secret Register.

c. Disclosure Records.

1. Each Top Secret document or item of material shall have appended to it a Top Secret disclosure record, (AF Form 144). The name and title of all individual(s), including stenographic and clerical personnel to whom information in such documents and materials has been disclosed, and the date of such disclosures, shall be recorded thereon. Disclosures to individuals who may have had access to containers in which Top Secret information is stored, or who regularly handle a large volume of such information need not be so recorded. Such individuals, when identified on a roster, are deemed to have had access to such information. Disclosure records shall be retained for two (2) calendar years after the document or materials are transferred, downgraded, or destroyed.

2. Attach AF Form 144, Top Secret Access Record and Cover Sheet, to each Top Secret document or material including removable ADP Media (diskettes or cartridges) to identify all persons given access to the information. AF Form 144 will be kept with the document at all times until the document is destroyed, transferred to another TSCO, downgraded, or declassified. Once action has been taken as mentioned above, attach AF Form 144 to the inactive USEUCOM Form 25-13 and maintain on file for two (2) calendar years.

d. Inventories

1. All Top Secret documents and material shall be inventoried at least once annually. The inventory shall reconcile the top Secret accountability register with the documents or material on hand. At such time, each document or material shall be examined for completeness. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, a request for waiver of the annual inventory requirement accompanied by full justification may be submitted to the DUSD(P).

2. Additionally, inventories will be conducted on change of the TSCO or whenever directed by the TSCO appointing authority. The TSCO will not perform the inventory.

e. Secret Information.

1. The control system for Secret information must be determined by a practical balance of security and operating efficiency. Baseline requirement includes use of the Joint Staff Records Keeping System, which replaces the Modern Army Records Keeping System (MARKS), and the following minimum requirements:

2. It must provide a means to ensure that Secret material sent outside a major subordinate element (the activity) of the DOD Component concerned has been delivered to the intended recipient. Such delivery may be presumed where the material is sent electronically over secure voice or data circuits. Ensuring physical delivery may be accomplished by use of a receipt as provided in chapter 7, section 7-102 or through hand-to-hand transfer when the receiving party acknowledges responsibility for the Secret material.

3. It must provide a record of receipt and dispatch of Secret material by each major subordinate element. The dispatch record requirement may be satisfied when the distribution of Secret material is evident from addresses or distribution lists for classified documentation. Records of receipt and dispatch are required regardless of the means used to ensure delivery of material (see paragraph a., above).

4. When Secret material is being transmitted outside of the Command a DA Form 3964, Classified Document Accountability Record will be used to record its receipt and dispatch.

5. Records of receipt and dispatch for Secret material shall be retained for a minimum of calendar two (2) years.

f. Confidential Information.

Administrative controls shall be established to protect Confidential information received, originated, transmitted, or stored by an activity.

g. NATO Information.

1. NATO Atomal documents will be controlled on HQ USEUCOM Form 25-13, USEUCOM Classified Material Register.

2. NATO Cosmic Top Secret documents will be controlled on HQ USEUCOM Form 25-13, USEUCOM Classified Material Register.

3. NATO Secret documents will be controlled on HQ USEUCOM Form 25-13, USEUCOM Classified Material Register.

4. NATO Secret, Cosmic and Atomal information will be accounted for and inventoried in the same manner as U.S. Top Secret, Appendix J, para 4 (1) and in accordance with USSAN 1-69.

5. Removable ADP media (diskettes or cartridges) containing NATO information will be accounted for on the appropriate HQ USEUCOM Form 25-13, commensurate to the level of classified information contained on the media.

APPENDIX 11
CLASSIFIED MATERIAL DESTRUCTION STANDARDS

1. General. This appendix contains basic concepts and guidelines that assist in determining the sufficiency of various destruction techniques. It also provides residue dimension standards that will assist in achieving secure destruction. No single destruction method has been found to be as effective, versatile, and secure as burning.

2. The methods for routine destruction of classified material shown below are approved for use by USEUCOM elements.

a. Pyrolysis (high temperature multistage).

b. Shredding.

c. Pulping (wet process).

d. Pulverizing (dry process).

3. Approved routine security destruction equipment.

a. Design specifications of equipment used for each of the destruction methods in paragraph K-3 will, as a minimum, conform to the following applicable standards:

(1) Pyrolytic furnaces - Federal Clean Air Act, as amended.

(2) Shredders - Interim Federal Specifications FF-S- 001169 with amendment 3.

(3) Pulping Machines - Interim Federal Specifications FF-P-00800A with amendment 2.

(4) Pulverizing Machine - Interim Federal Specifications FF-P-00810A with amendment 3

(5) All others - to be approved by Intelligence Materiel Development and Support Office (IMDSO) per paragraph 9-101 prior to procurement.

b. Residue Standards.

(1) Pyrolysis. Pyrolytic furnace ash residue must not contain unburned product. If unburned product is found, it will be treated as classified waste and maintenance personnel will be instructed to correct this fault in the furnace's burn cycle. Ash residue is to be examined and reduced by physical disturbance and will be considered destroyed when capable of passing through a 1/2 inch (13mm) square wire sieve. Furnace operators should be permanently assigned and trained to perform necessary adjustments and maintenance and be cleared for access to the highest level of material being routinely destroyed.

(2) Shredders. Shredders must have maximum particle dimensions as follows: Ninety percent (90%) of the shredded particles shall not exceed five square millimeters (5 mm²) and none of the remaining particles shall exceed ten square millimeters (10 mm²). Seventy five percent (75%) of the shredded particles shall have no edge dimension exceeding five millimeters (5 mm) in length. The remaining particles (a maximum of twenty five percent (25%)) may exhibit edge dimensions between five and twelve and one half millimeters (5 - 12.5 mm) in length. No particle shall have an edge dimension greater than twelve and one half millimeters (12.5 mm) in length. Any crosscut shredder whose residue particle size (total area) is equal to or smaller than that of the above Class I shredder is similarly approved for Top Secret destruction, when used in accordance with the "secure volume" concept of operation. Classified microfilm, microfiche, or similar high data density material will not be destroyed by shredding.

(3) Pulping. The Interim Federal Specifications FF-P-00800A with amendment 2 specifies the perforated screen or ring used in the masticating unit (through which all pulp must pass) will have 1/4 inch (6.350mm) or smaller diameter perforations. Since the pulping process entails wetting and dissolving action, plastic-based or other water-repellent-type papers normally should not be put through this system. However, if wetting additives are used and the ratio of soluble to non-soluble paper kept high (16 to 1 or greater), the masticating unit normally will tolerate that material. This toleration is totally dependent upon the sharpness of the pulper's cutters. Foreign matter, such as metal and glass, must be excluded from charge loads by visual inspections. Standard systems employing 1/4 inch diameter perforated security screen are approved for the destruction of classified paper-based documents through Top Secret. Top Secret material will not be destroyed on equipment where security screens with larger perforations are in use. Random samples of residue from such units should be collected by the security manager for periodic examination. Samples may be sent to IMDSO for evaluation and comment.

(4) Pulverizers. The Interim Federal Specifications FF-P-00810A with amendment 3 covers pulverizing as a dry destruction process. It does not, however, specify a specific dry destruction method; consequently, within this category are hammer mills, choppers, hoppers, and hybridized disintegrating equipment.

4. Toner/Printer Cartridges: Toner/printer cartridges, prior to turn-in must be cleared of possible classified residual information. This can be accomplished by using the print random program or other unclassified data sheet on the equipment being replaced

APPENDIX 12
ORIGINAL SECRET CLASSIFICATION AUTHORITIES

The USEUCOM officials identified below are authorized to make original classification authority determinations for information up to and including SECRET.

Director, Manpower, Personnel and Security Directorate (ECJ1)

Director, Intelligence Directorate (ECJ2)

Director, Operations Directorate (ECJ3)

Director, Logistics & Security Assistance Directorate (ECJ4)

Director, Plans and Policy Directorate (ECJ5)

Director, Command, Control, and Communications Systems Directorate (ECJ6)

Special Assistant for Security Matters (ECSM)

Director, Office of Operations, Research, and Analysis (ECCS-OR)

Director, Comptroller (ECCM)

Director, Inspector General (ECIG)

Director, Mobilization and Reserve Component Affairs (ECRA)

Director, Public Affairs (ECPA)

Director, Special Operations Directorate (ECSO)

Legal Advisor (ECJA)

Command Chaplain (ECCH)

Chief, Joint Analysis Center (JAC)

Chief, USNMR, SHAPE

Director, George C. Marshall Center

Political Advisor

Chiefs of Field Elements to include Task Force and Forward Headquarters' Commanders

Chiefs of Offices of Defense Cooperation (ODCs)

Chief of the Joint Interagency Coordination/Planning Group

APPENDIX 13
SAMPLE PRELIMINARY INQUIRY REPORT MEMORANDUM

(ORGANIZATION)

MEMORANDUM THRU DIRECTOR (Of element submitting the inquiry)

FOR ECJ2-SSO

SUBJECT: Preliminary Inquiry - Control No. EC-02-01

1. Reference. DOD 5200.1-R, Information Security Program Regulation, and the HQ USEUCOM Supplement.
2. Authority. A preliminary inquiry was conducted from 21 through 23 Mar 02 under the authority of the above reference.
3. Description of Incident: The basis for this inquiry was that a Secret message was found unsecured in Room 248 of Building 3322 at approximately 1240 hours, 20 Mar 02.
4. Personnel Interviewed:
 - a. MSgt John P. Smith, ECJ2-XX.
 - b. Capt. Bill Jones, Joint Staff J1.
 - c. SSgt Larry Williams, ECJ2-XX.
 - d. Maj Roger Moore, ECJ2-XX.
5. Facts. Testimony provided to and observations of the inquiring official revealed:
 - a. A Secret message, reference 1.c., was transmitted from the Joint Staff J1 to ECJ2-XX on 19 Mar 02. According to Capt. Jones, the message was transmitted as priority precedence in the support of the Stilwell Commission.
 - b. At approximately 1130, 20 Mar 02, SSgt Williams received a telephone call from the Vaihingen Telecommunications Center (VTCC) about the reference Secret message. Notification of classified message pickups is a routine action between the VTCC and ECJ2-XX. SSgt Williams proceeded to the VTCC and took possession of the referenced Secret message.
 - c. Upon SSgt Williams' return to his work place at approximately 1150, 20 Mar 02, he processed the message and noted that the message was for immediate action by the ECJ2-XX office. SSgt Williams hand carried the message to the ECJ2-XX branch. The message was left in the "in basket" and SSgt Williams left the building for a racquetball appointment.
 - d. The message was found unsecured at approximately 1249, 20 Mar 02 by MSgt Smith upon his return from his scheduled lunch. The message was under a stack of paper in the "in basket." MSgt Smith did not recall receiving the message prior to going to lunch.
 - e. The ECJ2-XX office area is not a secured area. There are three individuals, all with Secret security clearances, that work in the area. Very little public traffic occurs in the area of the ECJ2-XX office. Although the

facility receives contract janitorial services, the cleaning crew normally cleans the room around 1400 each duty day. Maj Moore, who occupies the adjacent office, did not recall seeing any personnel in the ECJ2-XX office during the time period the message was left unsecured.

6. Conclusion. As a result of the testimony and of personal observations, it is concluded that:

- a. The incident occurred by unit personnel failing to follow established safeguarding procedures. Operating instructions direct the "hand-to-hand" release/transfer of classified material and prohibit use of in baskets.
- b. SSgt Williams' haste to meet a scheduled racquetball appointment caused a variance in protection procedures.
- c. The message was left unsecured for approximately 40 minutes. There is no evidence that unauthorized personnel had access to the message.
- d. A compromise of classified information did not occur.

7. Recommendations. Recommend that:

- a. Additional emphasis on unit procedures be addressed at regular intervals to enhance unit security education.
- b. That this incident should be closed as a security deviation.

Encl
Interview Statements

THEODORE W. MATTESON
MSgt, Inquiry Official

Instructions for Completing a Preliminary Inquiry Report

Report Content. Up to this point, you have made a determination of facts by checking records, reviewing directives, examining evidence, and interviewing people. It is now time to sit down and write the report. To assist you in preparing the written report, it is important to understand the general content for each of the seven sections of the written report. The following explanation of each of the sections is provided.

- a. **Section I - References.** This paragraph is used to reference any applicable directives, the authority for the inquiry, and any other documents which are referenced in the inquiry report.
- b. **Section II - Authority.** This paragraph of the report cites the authority for conducting the inquiry and states when, where, and by whom the inquiry was conducted.
- c. **Section III - Matters Investigated.** This paragraph contains a brief statement of the matter inquired into, the location of the security incident, and how the security incident was initially discovered or reported. When names of personnel are included, furnish their full name, rank, and duty title.
- d. **Section IV - Personnel Interviewed.** List all personnel who were interviewed by showing their rank, full name, duty title or functional address.
- e. **Section V - Facts.** This section is the heart of the entire inquiry report. It presents, in an orderly fashion, all established facts which have a bearing on the security incident. Facts are presented in chronological order with opinions and evaluation being omitted.
- f. **Section VI - Conclusion.** This section will contain a brief summary of conclusions reached after a review of all pertinent information by the inquiry official. Conclusions must be supported by the evidence obtained during the inquiry process. One of the following must be established: (1) compromise occurred; (2) possible compromise occurred; (3) inadvertent access occurred; or (4) the incident is a security deviation. One of the most important tasks of an inquiry official is to ascertain who or what is responsible for the security incident. The job is not finished unless this is accomplished and documented. Occasionally, there is a systemic or procedural breakdown where an activity fails to properly safeguard classified material due to misunderstanding of a requirement or, even more rarely, disregarding or ignoring requirements and lack of an effective security education and training program. Whatever the situation, the person or procedure that caused the incident is identified so corrective and preventive action can be taken by the appointing official.
- g. **Section VII - Recommendations.** This last section contains the inquiry official's recommendations for further action. Based on the conclusion (section V of the report, you can recommend the incident be deemed a security deviation and the incident closed. A recommendation on the need for an investigation is necessary when it has been concluded that an investigation would clarify the causative factors, responsibility, or compromise aspects of the violation.

APPENDIX 14
SAMPLE COURIER AUTHORIZATION MEMORANDUM
AND EXEMPTION NOTICE

ECJ1

MEMORANDUM FOR Whom It May Concern

SUBJECT: Designation of Official Courier

1. Major John Smith, SSAN 123-45-6789, Manpower, Personnel, and Security Directorate (ECJ1), HQ US European Command, AE 09131, is designated an official courier for the United States Government. Upon request, he will present his official identification card bearing the number A-1111222.
2. Major Smith is hand-carrying three sealed packages, size 9" x 8" x 24" addressed from "HQ USEUCOM, ATTN: ECJ1-H, APO, AE 09128-4209," and addressed to "DoD Historian, the Pentagon, Room 3C333, Washington, DC 20330-4000." Each package is identified on the outside of the package by the marking "OFFICIAL BUSINESS - MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.
3. Major Smith is departing Stuttgart International Airport, Germany with a final destination to Washington National Airport, District of Columbia. Known transfer points are Frankfurt International Airport, Germany and John F. Kennedy International Airport, New York.
4. This courier designation can be confirmed by contacting the undersigned at HQ USEUCOM ECJ1, 49-711-680-9988 (US to overseas); 0711-680-9988 (overseas to overseas); or DSN 430-9988.

Director's Signature
Block

APPENDIX 15
OPEN STORAGE REQUEST PROCEDURES

(Prepare memorandum for ECJ2 through ECJ2-SSO)

SUBJECT: Open Storage of Classified Material

1. Request open storage of classified material be approved for (Division office symbol)
 - a. Location: Building number, room number
 - b. Classification: Up to U.S. Secret
 - c. Description: Construction standards of the area
 - d. Physical Security Inspection: Contact ECJ2-SSO and request a Physical Security Survey and obtain letter stating area meets physical security requirements.
 - e. Justification: Whichever of the following is applicable:
 1. Material is too large for conventional containers.
 2. Bulk material that must be reviewed on a daily basis.
 3. Security containers are unavailable.
 - f. Procedures: Existing security standards for the area.
 - g. Reduction Efforts: Date/details of last review of classified holdings.
2. POC.....

Signature Block

Encls:

1. Copy of ECJ2-SSO memorandum of results of the survey
2. Copy of DEH memorandum on facility construction standards (if necessary)

APPENDIX 16
DECLASSIFICATION AND DOWNGRADING AUTHORITIES

The USEUCOM officials identified below are delegated authority to make declassification and downgrading determinations for information in their function areas of interest up to and including TOP SECRET as indicated.

Organization	Classification Level
ECJ1	
Director, Manpower and Personnel	Top Secret
Deputy Director	Secret
Chief, Operations, Policy, Plans, and Manpower	Secret
Chief, Adjutant General	Secret
ECJ2	
Director, Intelligence	Top Secret
Deputy Director	Secret
ECJ3	
Director, Operations	Top Secret
Deputy Director, Operations	Secret
Chief, Operations Systems	Secret
Chief, Exercise Division	Secret
Chief, Current Operations	Secret
Chief, Operation Plans	Secret
Chief, Command and Control	Secret
Chief, Joint Operations Center (JOC)	Secret
Chief, Short Range Plans Group (SRPG)	Secret
Chief, Long Range Plans Group (LRPG)	Secret
ECJ4	
Director Logistics and Security Assistance	Top Secret
Deputy, Director	Secret
Chief, Military Secretariat	Secret
Chief, Logistics Operations Division	Secret
Chief, Logistics Plans Division	Secret
Chief, Joint Movement Division	Secret
Chief, Engineering Division	Secret
Chief, Multinational Agreements Division	Secret
Chief, International Division	Secret
Organization	Classification Level
Chief, Program and Policy Division	Secret
ECJ4 (Con't)	
Chief, Medical Readiness	Secret
ECJ5	
Director, Plans and Policy	Top Secret
Deputy Director	Secret
ECJ6	
Director, Command, Control and Communications	Top Secret

Systems		
Deputy Director	Secret	
Special Operations (ECSO)		
Director, ECSO	Top Secret	
Deputy Director,	Secret	
Chief of Staff, ECSO	Secret	
Chief, Personnel and administration		Secret
Chief, Intelligence	Secret	
Chief, Operations	Secret	
Chief, Logistics	Secret	
Chief, Plans and Policy	Secret	
Chief, Comm-Electronics	Secret	
Operations, Research, and Analysis (ECCS-OR)	Top Secret	
Chief, Information Management Branch	Secret	
Chief, Analysis Branch	Secret	
Chief, Simulation Branch	Secret	
Comptroller, ECCM	Top Secret	
Legal Advisor, ECJA	Top Secret	
Inspector General, ECIG	Top Secret	
Organization	Classification Level	
Command Chaplain, ECCH	Top Secret	
Security Matters, ECSM	Top Secret	
Political Advisor, ECPLAD	Top Secret	
Historian, ECCS-H	Secret	
Chief, USNMR, SHAPE	Top Secret	
Public Affairs, ECPA		
Director	Top Secret	
Deputy Director	Secret	
EUCOM Joint Analysis Center, (JAC)		
Commander	Top Secret	
Deputy Commander	Secret	
Chief, JAC Operations Division	Secret	
Chief, JAC Imagery Division	Secret	
Chief, JAC Analysis Division	Secret	
Chief, JAC Targets Division	Secret	
Chief, JAC Order of Battle Division	Secret	

APPENDIX 17

Management and Administration of the Automatic
Declassification System for 25-Year Old and Older Materials

1. PURPOSE. This appendix formalizes the policy and procedures required to manage and administer the USEUCOM automatic declassification system for 25-year old and older materials, which is mandated by Executive Order 12958. It accordingly sets forth the general relationship and responsibilities of the ECJ1 Records Management Office, ECJ2 Special Security Office, and USEUCOM Historian for conduct of these automatic reviews of USEUCOM classified materials over 25-years old.

2. AUTHORITY. Authority for administration of the automatic declassification program is Executive Order 12958, Classified National Defense Information, and DOD 5200.1-R, Information Security Program Regulation.

3. GENERAL POLICIES. ECJ1 will be responsible for and provide overall management of the USEUCOM Automatic Declassification Program for national defense classified materials that are 25-years old or older. The USEUCOM Historian and ECJ2-SSO will provide support to this effort as prescribed by specific duties outlined below.

4. SPECIFIC RESPONSIBILITIES:

a. The ECJ1 Records Management Office will be responsible for:

- (1) Serving as overall manager for the declassification program.
- (2) Coordinating training efforts for staff personnel conducting management oversight reviews.
- (3) Programming for funding, to include processing of invoices for contractors and providing fund cites to other staff personnel conducting oversight reviews.
- (4) Coordinating visits/oversight reviews by staff personnel.
- (5) Working closely with other identified team members to conduct and/or program necessary training for staff reviewers.
- (6) Provide personnel (senior NCOs, Officers, and civilian equivalents) to conduct management oversight reviews of contract personnel assigned to perform initial reviews of materials.

AP17-1

USEUCOM SUP 1
DOD 5200.1-R

a. ECJ2-SSO will:

- (1) Provide technical advice and assistance to the ECJ1 Records Management Office on security issues, to include subject category expertise, guidance, and oversight for classified materials containing intelligence information.
- (2) Develop and continually update USEUCOM declassification guidance for use in administering this program.
- (3) Assist USEUCOM declassification team in reviewing/validating declassification and exemption decisions made by initial reviewers.

(4) Assist ECJ1 with preparation of necessary security documents, such as passing of security clearances and acquiring necessary badges or passes.

(5) Assist ECJ1 with training of USEUCOM Staff Oversight team members.

(6) Provide personnel (senior NCOs, Officers, and civilian equivalents) to conduct management oversight reviews of contract personnel assigned to perform initial reviews of materials.

d. ECCS-H will:

(1) Provide technical guidance to the USEUCOM declassification team on matters pertaining to declassification and exemption decisions made by initial reviewers.

(2) Assist ECJ1 with training of USEUCOM Staff Oversight team members.

AP17-2