

DEPARTMENT OF THE ARMY
 HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
 5001 EISENHOWER AVENUE, ALEXANDRIA VA 22333-0001

AMC Memorandum
 No. 380-5

16 May 2003

Security

HEADQUARTERS AMC INFORMATION SECURITY PROGRAM

This update is necessary to incorporate changes brought about by a new Department of the Army Information Security Regulation (AR 380-5) and to update information on Foreign National visits to HQ AMC, Subversion and Espionage Directed Against the U.S. Army (SAEDA) Activities and the reporting of suspicious activities.

	Paragraph	Page
CHAPTER 1. GENERAL		
Purpose	1-1	1-1
Scope.....	1-2	1-1
Explanation of Terms.....	1-3	1-1
Responsibilities.....	1-4	1-1
CHAPTER 2. CLASSIFICATION		
Classification	2-1	2-1
Classification authority	2-2	2-2
Downgrading & Declassification	2-3	2-2
Marking.....	2-5	2-4
CHAPTER 3. SAFEKEEPING & STORAGE		
Standards for storage equipment	3-1	3-1
Security containers.....	3-2	3-1
Lock combinations.....	3-3	3-2
Safeguarding lock combinations.....	3-4	3-3
Security checks & inspections	3-5	3-3
Security during working hours	3-6	3-3
Typewriter ribbons.....	3-7	3-4
Clean desk policy.....	3-8	3-5
Safeguarding classified in the event of an emergency	3-9	3-5

* This memorandum supersedes AMC-M 380-5, dated 30 July 2001.

	Paragraph	Page
CHAPTER 4. COMPROMISE OF CLASSIFIED INFORMATION		
Conditions requiring reporting	4-1	4-1
Responsibilities.....	4-2	4-1
CHAPTER 5. ACCESS, ACCOUNTABILITY & DISSEMINATION		
Access	5-1	5-1
Accountability.....	5-2	5-1
Dissemination	5-3	5-1
CHAPTER 6. DISPOSAL & DESTRUCTION OF CLASSIFIED INFORMATION		
Disposal	6-1	6-1
Typewriter ribbons.....	6-2	6-1
Computer disks	6-3	6-1
Residue	6-4	6-1
Shredder waste.....	6-5	6-1
Maintenance.....	6-6	6-1
CHAPTER 7. SECURITY OF MEETINGS & CONFERENCES		
Responsibility	7-1	7-1
Foreign National participation.....	7-2	7-1
Meeting or conference notes.....	7-3	7-1
CHAPTER 8. SECURITY AWARENESS		
Responsibility	8-1	8-1
New employees.....	8-2	8-1
Training.....	8-3	8-1
Security Monitor.....	8-4	8-1
Documentation.....	8-5	8-1
Inspections	8-6	8-2
CHAPTER 9. FOREIGN NATIONAL VISITORS TO HQ AMC		
General.....	9-1	9-1
Request Format.....	9-2	9-1
Responsibilities.....	9-3	9-1
General Officer & Senior Executive Service Members	9-4	9-1
CHAPTER 10. SUSPICIOUS ACTIVITIES		
Security is everyone’s business	10-1	10-1
Suspicious Activity	10-2	10-1
Violence.....	10-3	10-1
Reporting	10-4	10-2

	Paragraph	Page
CHAPTER 11. SUBVERSION AND ESPIONAGE DIRECTED AGAINST THE U.S. ARMY (SAEDA) ACTIVITIES		
SAEDA Requirements	11-1	11-1
Reportable Incidents	11-2	11-1
Additional matters of CI interest	11-3	11-3
APPENDIX A. SAMPLE AMC MEMORANDUM FOR BUILDING ACCESS.....		A-1
APPENDIX B. SAMPLE PRELIMINARY INQUIRY REPORT		B-1
APPENDIX C. SAMPLE SECURE INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) EMAILS.....		C-1
APPENDIX D. SAMPLE ACKNOWLEDGEMENT MEMORANDUM.....		D-1

CHAPTER 1

GENERAL

1-1. Purpose. This memorandum prescribes policy and establishes responsibilities for safeguarding and accountability, and for the reporting and investigation of alleged security violations involving classified information and materials within Headquarters, Army Materiel Command (HQ AMC) both at 5001 Eisenhower Avenue, Alexandria, Virginia and Fort Belvoir (Building 1464 and Modular Buildings 1 and 2). It also prescribes procedures to be followed when requesting approval for foreign national visitors to the Headquarters building. Where required information already in AR 380-5 and/or its AMC Supplement 1, will simply be referenced.

1-2. Scope. This memorandum is applicable to all personnel including contractors) assigned to all elements of HQ AMC, collocated AMC subordinate elements, and other AMC elements receiving security support from the HQ AMC Security Manager. Copies of this memorandum will be in each organization, branch or comparable level, where classified material is handled or stored. Deputy Chiefs of Staff, Separate Staff Office Chiefs, Project/Product/Program Managers, and chiefs of elements/activities collocated at HQ AMC will develop procedures to implement the provisions of this memorandum. No part of this memorandum will be cited in any communication dispatched outside HQ AMC except as necessary in support of contracting procedures for work to be done within the Headquarters.

1-3. Explanation of terms.

a. Security Monitor. The individual appointed in each staff activity to perform the functions outlined in paragraph 1-4 below. The security monitor is the focal point for security in each staff activity.

b. Safe Custodians. Individuals whose names, home addresses, and phone numbers appear on Standard Form 700 (Security Container Information). The primary custodian is the first person listed, with all others being alternates.

c. End of Day Security Check. A security inspection conducted at the close of each duty day, to ensure that all classified material has been properly stored and all security containers have been closed, checked and double-checked. The office chief will determine when the end of day inspection is performed and who performs it.

1-4. Responsibilities.

a. HQ AMC Security Manager, located in the DCS G-2, will:

(1) Provide general supervision of all information security programs within the HQ AMC.

(2) Prescribe security standards and procedures for safeguarding classified information.

(3) Supervise, or conduct, security inspections to assure compliance with pertinent security regulations and directives. Each DCS and separate staff activity office will be inspected a minimum of twice annually. One inspection will be announced (see para 8-6 below) and one will be unannounced.

(4) Initiate appropriate action in cases of suspected or alleged security violations.

(5) Provide advice and guidance on safeguarding classified information.

(6) Provide advice and guidance on SAEDA issues.

(7) Retain personnel security program oversight, establishing and implementing policies and ensure compliance with applicable regulations throughout the command.

b. HQ AMC Personnel Security Specialist, located in G-1, Headquarters Commandant will:

(1) Manage and coordinate the personnel security clearance request processing procedure, courier authorizations, visitor authorization process and clearance validations. This includes the issuance of classified material courier cards and security clearance validation for visit authorizations.

(2) Maintain personnel security clearance and access rosters and coordinate with various security officials and Central Clearance Facility.

(3) Serve as the HQ, AMC point of contact for the HQDA Personnel Security Services Division on all personnel security matters.

(4) Receive and review automated requests for security clearances to ensure all required information is included and automated forms have been properly completed and assist in preparation of automation requests, as required. Forward completed requests to HQDA Personnel Security Services Division for further processing and adjudication.

(5) In-process new employees and debrief departing personnel.

(6) Perform special access briefings (i.e., NATO, ATOMAL, COSMIC, and CNWDI).

(7) Coordinate security clearance data with the Special Security Office in support of other special access programs.

(8) Review, analyze, validate, and sign requests for security investigations/clearances for military and civilian personnel.

(9) Coordinate all derogatory suitability information issues with HQ DA Safety, Security, Services Division, individual's supervisor, the Command Security Manager, the H3 Operations Center and the individual.

c. HQ AMC Top Secret Control Officer (TSCO), located in the DCS G-2, will perform those functions identified in paragraph 6-21, AR 380-5 and its AMC Supplement 1. The HQ AMC TSCO will also receipt for, control, and make initial distribution of all Joint Chiefs of Staff (JCS), and other special category information classified TOP SECRET.

d. Deputy Chiefs of Staff and separate staff activity chiefs will:

(1) Ensure and monitor compliance with all regulations and instructions, including this memorandum, pertaining to security and the safeguarding of classified information.

(2) Ensure that, prior to granting access to classified information, new employees (including contractors) are briefed by supervisors and/or the security monitor concerning job specific security requirements and **ensure** this briefing is documented. Also ensure employees are briefed on the policies and procedures for generating emails on the Secure Internet Protocol Router Network (SIPRNET), file written confirmation and provide copy to the Command Security Manager.

(3) Ensure that an annual review of classified documents is conducted and documented.

(4) Appoint, in writing:

(a) A staff activity security monitor, and alternates as deemed necessary. Security monitors and alternates must be cleared for the highest level of classified information authorized in that staff activity, be a GS-7 or higher, a Commissioned or Warrant Officer, or a Non-Commissioned Officer holding the rank of Sergeant First Class or higher.

(b) A TSCO and alternates as appropriate, in those offices that hold or review Top Secret material. TSCOs must meet the same grade or rank requirements as security monitors. Changes will be reported promptly to the AMC TSCO.

(5) Report the following to the HQ, AMC Security Manager (AMCMI):

(a) Any security violation or suspected security violation committed by personnel under their supervision.

(b) The loss or possible compromise of any classified information under their control.

(c) Any credible derogatory suitability information (see para 1-304.3, AR 380-67) concerning personnel under their supervision. (Report this to the personnel security specialist in the G-1, HQ Commandant).

(6) Ensure that the name, room number, and telephone number of their security monitor is posted in each office under their jurisdiction.

(7) Provide a list of staff activity points of contact for the following to the HQ,AMC Security Manager, updated as necessary:

(a) Security Monitor (and alternates if any).

(b) Information Systems Security Officers.

(8) Ensure that all visits by non-U.S. personnel are cleared through the DCS for Intelligence prior to the visit. (See Chapter 9).

(9) Establish procedures for a "Clean Desk" policy (see Chapter 8, para 3-8).

e. Staff activity security monitors will:

(1) Provide advice, assistance, and guidance on security matters to their respective deputy chief of staff or office chief and individuals assigned to their staff activity.

(2) Maintain liaison with the HQ AMC security manager on matters relating to security and safeguarding of classified information.

(3) Request appropriate security clearances for assigned personnel, using DAS Form 78 (Request for Security Determination).

(4) Maintain current security regulations and ensure personnel know where they are.

(5) Monitor compliance with the requirements of this memorandum and AMC Supplement 1 to AR 380-5.

(6) Conduct and document (e.g., Memorandum for Record) routine security inspections of the activity at least once each quarter.

(7) Attend scheduled security monitor meetings and disseminate information and material received.

(8) Ensure that safe combinations are changed as prescribed in AR 380-5 and AMC Supplement 1 to AR 380-5. See also paragraph 3-3 below.

(9) Conduct preliminary inquiries of potential security violations within their directorates or staff activities.

(10) Coordinate with G-1, Headquarters Commandant Personnel Security Specialist on all matters pertaining to personnel security.

f. Staff activity TSCOs will:

(1) Maintain register of all Top Secret documents within the staff activity.

(3) Keep an up to date list of all individuals within the staff activity that are authorized to access and/or receipt for Top Secret and special category documents.

(4) Notify the AMC TSCO when individuals are no longer authorized access to Top Secret documents.

CHAPTER 2

CLASSIFICATION

2-1. Classification.

a. There are three levels of classification designations authorized for the protection of information vital to national security: TOP SECRET, SECRET, and CONFIDENTIAL. To be eligible for classification, information must fall within one or more of the following categories of information:

- (1) Military plans, weapons systems, or operations.
- (2) Foreign government information.
- (3) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- (4) Foreign relations or foreign activities of the United States, including confidential sources.
- (5) Scientific, technological, or economic matters relating to the National Security.
- (6) U.S. Government programs for safeguarding nuclear materials or facilities.
- (7) Vulnerabilities or capabilities of systems, resources, installations, projects or plans relating to the National Security.

b. Information may **not** be classified for the purposes of:

- (1) Concealing violations of law, inefficiency, or administrative error.
- (2) Preventing embarrassment to a person, organization or agency.
- (3) Restraining competition.
- (4) Preventing or delaying the release of information that does not require protection in the interest of National Security.

c. Information may **not** be reclassified after it has been declassified and released to the public.

2-2. Classification Authority (see chapter 2, AR 380-5). The authority to classify a document comes from one of two sources: original authority and derivative authority.

a. Original classification authority (OCA) is exercised when a determination needs to be made concerning the classification of new information that requires protection in the interest of National Security but has never been classified. If there is significant doubt about the need to originally classify information, protect it with the highest classification level deemed appropriate and coordinate the original classification action with advice from G-2. HQ, AMC OCA's are:

- (1) Commander, AMC for information up to and including TOP SECRET.
- (2) Chief of Staff, AMC for information up to and including SECRET.

b. When extracting, paraphrasing, restating, or generating in a new form of information that is already classified, derivative classification authority is used. Classification markings for the new document will come from the source documents or a security classification guide.

(1) When extracting classified information from a single source to create a new document, the classification authority for the new document is the source document.

(2) When extracting classified information from two or more sources to create a new document, the classification authority is "MULTIPLE SOURCES." Retain a list of the sources used with a file copy of the new document.

2-3. Downgrading and Declassification (see chapter 3, AR 380-5). Classified information must be declassified or downgraded as soon as national security considerations permit. The decision to declassify or downgrade information is based on the loss of sensitivity due to the passage of time or the occurrence of an event. The declassification of documents is an ongoing process and must be constantly monitored to ensure that it is carried out.

a. Duration of classification. When information is originally classified, the classifier must identify either a date or event that is 10 years or less from the original classification decision, or an exemption category (e.g., X1, X3, etc.). Information may be exempted from the "10-year rule" if, even after 10 years, disclosure would be expected to:

- (1) Reveal an intelligence source, method or activity, or a cryptologic system or activity (X1).
- (2) Reveal information that would assist in the development or use of weapons of mass destruction (X2).
- (3) Reveal information that would impair the development or use of technology within a U.S. weapons system (X3).
- (4) Reveal U.S. military plans or national security emergency preparedness plans (X4).

(5) Reveal foreign government information (X5).

(6) Damage relations between the U.S. and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period longer than 10 years (X6).

(7) Impair the ability of responsible U.S. government officials to protect the President, and other individuals for whom protection services, in the interest of national security, are authorized (X7).

(8) Violate a statute, treaty, or international agreement (X8).

b. Clean out days. A primary vehicle for carrying out the declassification process is the Annual Clean-Out Day. All activities will perform an annual review of classified holdings. Those that are no longer required will be properly destroyed or transferred to the appropriate records holding area. Those that are retained will be inspected to insure that they contain the appropriate classification markings and downgrading instructions. Each DCS and SRA will designate one day during the first quarter of the calendar year as its annual clean-out day. The HQ, AMC Security Manager will be advised of the following in writing NLT 3 working days after clean out:

(1) The date of clean-out day

(2) Percentage of documents destroyed

2-4. Marking (see chapter 4, AR 380-5).

a. All newly created classified documents must be reviewed to ensure they contain proper declassification markings. This must be done prior to dissemination. When extracting information from old documents, review them to ensure compliance. This review must include overall, page and portion markings as well as the “Classified By” or “Derived From” and “Declassify On” lines. All documents dated 14 October 1995 or later, that are marked with the old markings, shall be re-marked as they are removed from files for working purposes or disseminated from the activity. Documents created before 14 October 1995 shall not be re-marked.

b. Marking guidance:

(1) The “**Classified By**” line is used on originally classified documents to show the OCA for the classification of the document. Note that the reason for classification will also be shown on the face of the document. See paragraph (4) below:

(2) The “**Derived From**” line is used when information contained in one or more documents is used as the basis for the classification of a new document. If the information is derived from only one document, that document will be identified on the “Derived From” line.

If more than one source is used, the “Derived From” line will show “Multiple Sources,” and a list of the sources will be maintained with the file copy of the document held in the originating office. See paragraph (4) below.

(3) The “**Declassify On**” line indicates the date or events when the material requires declassification. If the classification is derived from a source document, the new document will reflect the same declassification date as the source document. If the classification is derived from “Multiple Sources”, the new document will reflect the date or event which is most remote. Although the marking “Originating Agency’s Determination Required” or “OADR” is no longer authorized for use, if the source document reflects this marking, it will be carried forward to the new document. See examples below.

(4) Examples.

CLASSIFIED BY: LTG Kennedy, Deputy Chief of Staff for Intelligence, HQDA
REASON: Intelligence Sources and Methods
DECLASSIFY ON: 15 Jan 04

DERIVED FROM: HQDA Memo, “Classification Markings”, 12 Oct 95, Office of the Deputy Chief of Staff for Intelligence (DAMI-POC).
DECLASSIFY ON: Source Marked “OADR”
DATE OF SOURCE: 12 Oct 95

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 19 Sep 07

CLASSIFIED BY: LTG Kennedy, Deputy Chief of Staff for Intelligence, HQDA
REASON: Intelligence Sources and Methods
DECLASSIFY ON: XI

c. Placement of markings. Classified by, Derived From and Declassify On lines must appear on the front cover, if any, or on the first page of a classified document. Additionally, this information must appear on each separate appendix, annex, tab, or figure, which might be separated from the document.

2-5. Marking Documents Created on the Secure Internet Protocol Router Network (SIPRNET).

a. To ensure the security of classified information, classification markings WILL be applied to each email and its attachments created on the SIPRNET. As an exception, if the entire message on a secure network is UNCLASSIFIED, it can be marked on its face, top and bottom: “UNCLASSIFIED”, and a statement added: “All portions of this message are UNCLASSIFIED.” (Under no circumstances will a single line classification marking of this nature be applied to an email containing classified information). All other classified emails will be marked according to chapter 4 of AR 380-5 and this memorandum. Additionally, the SUBJECT line of every email will clearly indicate the classification of the most sensitive, highest level of information contained within the email and its attachments.

b. Classified and sensitive documents will be marked to show the highest classification/sensitivity of information contained in the document. For documents containing information classified at more than one level, the overall marking will be the highest level. For example, if a document contains some information marked "SECRET" and some information marked "CONFIDENTIAL", the overall marking would be "SECRET." This marking must be conspicuous enough to alert personnel handling the material that it is classified and must appear in a way that will distinguish it clearly from the text of the document. The overall classification/sensitivity will be conspicuously marked, stamped, or affixed (with a sticker, tape, etc.), top and bottom on the front and back covers (if the document has covers, on the title page (if there is one) and on the first page, in letters larger than those on the rest of the page).

c. Each classified and/or sensitive document must show, as clearly as possible and feasible, which information is classified and/or sensitive and at what level.

d. Each section, part, paragraph and similar portion of a classified and/or sensitive document will be marked to show the highest level of classification/sensitivity of information it contains.

e. Each portion of the text will be marked with the appropriate abbreviation ("TS" for TOP SECRET, "S" for SECRET, "C" for CONFIDENTIAL, or "U" for UNCLASSIFIED) placed in parentheses immediately before the beginning of the portion.

f. EMAIL on the SIPRNET should be treated the same as any other type of classified documents and must be marked as required by AR 380-5.

g. Appropriate classification markings of SIPRNET Email will be applied IAW AR 380-5 and this memorandum just as those created in various word documents, spreadsheets, or PowerPoint software. Until an automated solution has been evaluated and approved for use in classification, the individual creating the email will apply markings manually.

h. All emails transmitted via SIPRNET will include classification markings appropriate to the level and sensitivity contained in the email. This includes unclassified mail. (See Appendix C for examples of email documents which illustrate the following:

Example 1 - UNCLASSIFIED Email

Example 2 - UNCLASSIFIED Email document with UNCLASSIFIED attachments

Example 3 - UNCLASSIFIED Email with a SECRET attachment

Example 4 - SECRET Email document with declassification instructions.

NOTE: Each example is unclassified, and all markings are for training purposes only.

CHAPTER 3

SAFEKEEPING AND STORAGE

3-1. Standards for storage equipment. Classified material will be stored per chapter 7, AR 380-5 and its AMC Supplement 1.

3-2. Security containers.

a. Security containers within each section or comparable organization within a staff activity will bear a distinctive number.

b. Requests for combination changes will be directed to Federal Security Systems (FSS), (703) 339-2912. The Security Monitor will verify the FSS Technician's security clearance before the combination is changed. The Security Monitor or the point of contact for the safe will dial in the new combination; not the FSS Technician. For further assistance contact the Command Security Manager at (703) 617-0081.

c. Security containers used to store classified information will not contain any external markings to indicate the classification or sensitivity of information stored.

d. Security containers that do not contain any classified materials, but require locking during non-duty hours will display the following statement in a conspicuous place on the front of the container:

“THIS CONTAINER DOES NOT CONTAIN ANY CLASSIFIED MATERIAL AND NO SUCH MATERIAL WILL BE PLACED IN IT.”

e. Prior to converting a container from the storage of classified information to the storage of unclassified information, turning a container in as excess, etc., the security monitor will:

(1) Examine the safe carefully, to include behind and under the drawers to insure that it contains no classified information.

(2) Remove the Standard Forms 700 and 702.

(3) Prepare, sign and affix the following statement prominently to the front of the control drawer or door of the container:

“I CERTIFY THAT I HAVE THOROUGHLY EXAMINED THIS CONTAINER AND NO CLASSIFIED MATERIALS REMAIN WITHIN.”

(4) In the case of a safe to be turned in, reset the combination to 50-25-50 and add the following to the statement in paragraph (3) above:

“THE COMBINATION IS SET TO 50-25-50.”

f. When a security container or lock malfunctions, contact AMCEN-R promptly for assistance. If the condition cannot be corrected during normal working hours, or if the discovery occurs at the end of the duty day, the custodian will:

(1) Transfer the classified materials to another security container and place a statement on the malfunctioning container indicating that it contains no classified material. The SF 700 will be removed from the container.

(2) If the material cannot be transferred to another security container, insure that appropriately cleared individuals guard the material until the container is repaired.

(3) Contact the Staff Duty Officer or the Operations Center for assistance if (1) and (2) above cannot be accomplished.

g. The individual unlocking a container will ensure that the SF 702 is properly annotated, and the reversible “OPEN-CLOSED” sign is turned so that the “OPEN” is plainly visible.

h. The individual locking the container will ensure that the SF 702 is properly annotated and the reversible “OPEN-CLOSED” sign is turned so that the “CLOSED” is plainly visible.

i. The individual opening and closing the container can be the same person, however, a different person must check the safe container to ensure it is locked, ensure the SF 702 is properly annotated, and the reversible “OPEN-CLOSED” is turned to “CLOSED.”

3.3 Lock combinations.

a. Combinations will be selected at random.

b. Combinations will be recorded on Standard Form (SF) 700. Part 1 of the SF 700 will be posted on either side or directly behind the back panel on the inside of the control drawer of security containers. In the case of a vault or other type of door, Part 1 will be placed on the back of the door.

c. The SF 700 will contain the names of those persons who have the combination. It will be stamped with the highest classification of the information authorized to be stored in the safe.

d. Deputy Chiefs of Staff or separate reporting activities will establish one master safe within their staff activity, or they may authorize individual master safes within each division. In either case, all combinations within that staff organization will be maintained in that master safe. The combination to the master safe at division level will be stored in a master safe within the

DCS. The combination to the DCS master safe will be stored in the master safe maintained by the HQ AMC Security Manager.

(1) If any of the safes in a DCS contain NATO material, the combination to those safes (or to the DCS master safe) will be stored in the NATO Subregistry, the Point of Contact at the NATO Subregistry is located in Room G2W09, 617-9441.

(2) The combinations for ALL safes authorized to store Top Secret information will be maintained by the AMC TSCO, located in Room G2C63, 617-8987.

e. In case of an emergency, combinations for master safes may be obtained from the HQ, AMC Security Manager, AMC TSCO, or NATO Subregistry as appropriate.

3-4. Safeguarding lock combinations. Individuals WILL NOT carry lock combinations on their person in any manner (e.g., in wallets or purses, written on calendar pages, walls, desk blotters, note pads, etc.) nor will they be stored in any computer files.

a. So-called “convenience lists” of Secret and Confidential combinations will be kept to an absolute minimum. Convenience lists of Top Secret combinations are **PROHIBITED**.

b. When convenience lists are deemed necessary, they will be marked, protected, and stored according to the highest classification of any of the combinations listed.

3-5. Security Checks and Inspections

a. Security containers will be checked and the SF 702 completed whenever the container is closed and everyone is leaving the area (e.g., for lunch, office meetings, end of day, etc.)

b. The end-of-duty day security inspection will include a complete check of the office areas including, but not limited to:

(1) Ensuring that security containers are locked and checked.

(2) Checking to see that no classified material has been left on desks, work areas, credenzas, wastebaskets, etc.

(3) Checking to see that keys have been removed from all Secure Telephone Units (STU-III) and the Fortezza card removed from all Secure Telephone Equipment (STE).

(4) Completing Standard Form 701 (Activity Security Checklist).

3-6. Security. All personnel who handle classified material are responsible for adhering to the following:

- a. All classified material will have the appropriate cover sheet attached to the front of the document whenever it is outside an approved security container.
- b. Classified material and open security containers WILL NOT be left unattended.
- c. Classified conversations will be conducted in a low tone of voice, bearing in mind that rooms are not soundproof.
- d. Persons using unsecured telephones will ensure that no classified conversation is ongoing near-by, since telephones contain microphones capable of picking up and amplifying sound from several feet away.
- e. Computers will not be left with classified information visible on the screen.
- f. Classified material may be carried in corridors and elevators within HQ AMC provided it is covered by the appropriate cover sheet.
- g. Classified information will NOT be discussed over unsecured telephones, in corridors, elevators, cafeteria or snack bars, rest rooms, on the DOD buses, or in other public or common-user places.
- h. Classified material will be hand-carried directly from one office to another. Intermediate stops at washrooms, cafeteria, snack bar, etc., are prohibited.
- i. Classified material will only be processed on computers and other automated information systems that are properly accredited for that level of classification.
- j. All classified waste will be either shredded in an approved shredder, or placed in an appropriate "burn bag" and secured at the end of each day. See the Command Security Manager for authorized shredders approved for use in the destruction of classified information. As a security and OPSEC enhancement the destruction of all classified, controlled unclassified information, and uncontrolled paper is highly recommended by an approved method (i.e. burning or shredding).
- k. Visitors (contractors, maintenance personnel, commercial representatives, etc.) will be escorted and supervised as appropriate while in areas where classified information is present.
- l. Building passes (DD Form 1466, or AMC Visitor Badge) will be worn in plain view at all times while in the HQ AMC building.

3-7. Typewriter ribbons and computer disks.

- a. Typewriter ribbons used in producing classified information will be removed from typewriters, marked with the highest classification of material typed, and properly stored when not in use. These ribbons will be destroyed as classified waste. Destruction will be

accomplished by breaking the plastic apart, removing the ribbon and placing it in a burn bag, or shredding it.

b. Computer disks used to store classified information will be marked with the highest classification of information on them. They will be destroyed as classified waste. Destruction will be accomplished by breaking the plastic case open, removing the disk, cutting it in half, and placing it in a burn bag. To destroy hard drives, see G6 (Chief Information Office) for further instructions.

3-8. Clean-desk policy. A clean desk enhances security. Anything left on a desk in an unlocked office is subject to review by cleaning teams, maintenance personnel, etc., who are in the building during non-duty hours. At the end of each duty day, desks, chairs, credenzas, bookcases, etc., should be cleared of all working materials to the degree necessary to ensure the security of classified information. Because of the many different office environments that exist within HQ, AMC, individual DCS or office chiefs will determine the exact extent the desks and surrounding areas must be kept clear.

3-9. Safeguarding classified material in the event of an emergency. The volume of classified material within HQ, AMC makes emergency evacuation or removal impractical. Therefore, in the event of an emergency (e.g., civil disturbance, disaster, fire, etc.) requiring evacuation of personnel from the building, the following measures will be taken:

- a. All classified material will be secured in authorized containers.
- b. Personnel will ensure that all security containers have been locked prior to departing an office area.
- c. If time permits, the SF 702 will be annotated.
- d. Personnel in route between offices with classified material will use their own discretion as to whether they can return it to its normal security container without undue threat to their safety. The individual may report to the nearest DCS administrative office, or other office with available security containers and secure the material. If this is not feasible, the individual in possession of the material will protect it until it can be properly secured. Under no circumstances will the material be turned over to a fireman, warden, police officer, or guard for safekeeping.
- e. **The safety of personnel is paramount.** Under **NO** circumstances will individuals place themselves in unnecessary danger to secure classified information.

CHAPTER 4

POSSIBLE COMPROMISE OF CLASSIFIED INFORMATION

4-1. Conditions requiring reporting. The following, as well as any other suspected security violations, must be reported immediately to the staff activity security monitor.

- a. Security containers found unlocked and unattended after normal duty hours.
- b. Classified documents left unsecured and unattended.
- c. Top secret or special-access documents lost to accountability.
- d. Disclosure of classified information to an unauthorized person.
- e. Classified information appearing in public media.
- f. Classified information discussed over unsecured means of communications.
- g. Classified information processed on an automated information system not accredited to that classification level.
- h. Loss of a STU-III key or STE Fortezza card.

4-2. Responsibilities.

- a. The individual discovering classified material left unsecured and unattended will:
 - (1) Immediately notify the security monitor. In the case of an open security container, the discoverer will also notify the custodian or alternate from the listing on the SF 700 for that container.
 - (2) Take possession of the material or guard it until the security monitor is notified and the material can be properly stored.
- b. The security monitor will:
 - (1) Take immediate action to ensure that the material is properly protected until it can be secured in an approved security container.
 - (2) In the case of an open security container, ensure that the custodian or alternate has been notified.
 - (3) Make a complete inventory of the classified material found unsecured.

(4) Notify the DCS or staff activity chief.

(5) Contact the HQ, AMC Security Manager to receive a PI report number.

The DCS will:

(Notify the DCS G2 that a violation has occurred.

(2) Ensure that a Preliminary Inquiry (PI) is conducted Under the provisions of paragraph 10-3 of AR 380-5 and AMC Suppl 1 within fifteen working days of the incident. See Annex B for a recommended format for preliminary inquiries.

(3) Ensure that the PI report is coordinated with the Office of Command Counsel (AMCCC) before sending it to the Deputy Chief of Staff G-2 (AMXMI).

(4) After signature by the DCS G-2, ensure that the approved recommendations are implemented.

(5) Initiate action through HQ Commandant to appoint an Investigating Officer if appropriate.

(6) If the PI indicates possible compromise of information, ensure that the classification authority for each document involved is notified and request a re-evaluation of the classification because of possible compromise (DA Form 1575 may be used).

(7) Implement/execute recommendation as appropriate. Monitor implementation/execution of recommendations and report to AMCCS (Copy Furnished AMXMI) every thirty days until complete.

c. The safe custodian will:

(1) Immediately inspect the contents of the safe in an effort to determine if anything is missing.

(2) Inspect the safe for any obvious signs of tampering. If signs of tampering are evident, transfer the classified material to another container.

(3) Ensure the combination to the container is changed.

(4) Lock the container and annotate the SF 702.

d. The Deputy Chief of Staff, G2 will:

(1) Review all preliminary inquiries for accuracy.

(2) Responsible for reporting incidents to the Chief of Staff.

e. The HQ AMC Security Manager will:

(1) Review the PI report to ensure adequacy of the evidence, findings and recommendations.

(2) Initiate action to appoint an Investigating Officer if appropriate.

(3) Monitor action of the staff activity as appropriate and assist/provide guidance to the DCS to ensure the PI is completed and approved recommendations are implemented.

(4) Advise DCS with notification request for reevaluation of classified compromised information.

(5) Monitor implementation/execution of recommendations; provide advice and assistance as appropriate.

CHAPTER 5

ACCESS, ACCOUNTABILITY AND DISSEMINATION

5-1. Access

a. Clearance. Prior to granting access to any classified information, the custodian of that information will ensure that the individual to whom the information is to be given has the appropriate security clearance. Clearance information is obtained from the G-1 Headquarters Commandant (AMCPE-P).

b. Need-to-Know. In addition to verifying an individual's security clearance, the holder of classified information will also validate the individual's need to know. Neither rank nor security clearance entitles one to unlimited access to classified information.

c. Prior to forwarding any classified materials to a contractor, verification of the contractor's facility clearance and storage capability will be obtained from the Contracting Officer. Classified materials may be transmitted to the security officer of the contractor facility.

d. Custodians of classified material must use extreme caution whenever visitors are present in the work area to ensure no classified information is inadvertently disclosed.

e. When a HQ AMC employee receives visitors for classified discussions, that employee will ensure a visit request with the necessary clearance information is on hand. The visit request should be coordinated with DCS G-3, the Office of Security, Force Protection and Law Enforcement to arrange for the appropriate visitor's pass.

5-2. Accountability

a. All Top Secret documents brought into HQ AMC, including those hand carried by personnel from any source and those received electronically, must be brought under AMC accountability control by the AMC TSCO.

b. All SCI documents will be brought directly to the SSO (G2C63).

5-3. Dissemination. Classified documents will not be removed from HQ AMC for the purpose of working on such materials at home or for other purposes involving personal convenience. Classified material will only be removed from HQ AMC when it is absolutely necessary.

a. CONUS:

(1) SECRET classified material required by personnel on temporary duty (TDY) within CONUS will be forwarded to the TDY station via registered mail or authorized courier, to be held for the person concerned. For exceptions, see section 4, Chapter 8, AR 380-5 and AMC

Supplement 1. Also see AR 380-5, Chapter 8 for entire guidance on transporting classified material.

(2) Personnel who hand-carry classified material between locations within the Military District of Washington will ensure that they have a current DD Form 2501, COURIER AUTHORIZATION, in their possession at all times. The provisions of section 4, chapter 8, AR 380-5 with its AMC Supplement 1 will be adhered to.

b. OCONUS. Only under extreme emergencies will personnel on travel outside the Continental United States be authorized to carry classified materials with them. For COMSEC material see AR 380-40. The Commander, AMC, and the DCS G-2 are authorized to approve the hand-carry of classified material OCONUS. Requests will be submitted in writing, a minimum of five working days before actual travel. The memo will be marked "FOR OFFICIAL USE ONLY – PROTECTIVE MARKING CANCELLED UPON COMPLETION OF OCONUS TRAVEL" and will include the following information:

(1) Name of courier.

(2) Type of material (e.g., slides, documents, computer disks, etc.) and classification level of information to be hand-carried.

(3) Justification, including why the information could not be sent ahead and how the mission would be adversely affected if the request is denied. If the material must be hand-carried on the return trip, explain why.

(4) Itinerary (provide a copy of the complete itinerary from the travel office), to include justification for non-U.S. flag carriers if required.

(5) In-transit and TDY location storage arrangements.

c. Classified information will NOT be sent via email unless that system has been specifically approved for and accredited to process classified information classified at that level (i.e., Secure Internet Protocol Router Network (SIPRNET)).

d. Classified information will not be discussed over any unsecured telephone system (including facsimiles).

e. Reproduction.

(1) Reproduction of TOP SECRET and special category documents requires prior approval from the HQ AMC TSCO, IAW AR 380-5, para 6-25b.

(2) Reproduction of classified material will be kept to a minimum.

(3) Only those copiers specifically approved by the DCS or staff activity chief (or the security monitor) on HQ AMC LABEL 202 will be used to reproduce classified material.

(4) Individuals making copies of classified documents will insure that the classification markings are sharp and easily readable on the reproduced copies. After reproduction of classified documents individuals will print at least two to five blank pages (depending on the number of pages reproduced) through the copier to ensure no classified information exists in the copier.

f. Transmission.

(1) Classified material to be transmitted outside of HQ, AMC will be hand carried, unsealed, to the classified mail room along with two copies of AMC Form 200 (Address Label) with the appropriate address for dispatch. If the material is classified SECRET, include an original and three copies of a properly completed DA Form 3964. Multiple documents may be transmitted on a single DA 3964.

(2) Classified material may be hand-carried between HQ, AMC (5001 Eisenhower Avenue, Alexandria, Virginia and Fort Belvoir (Building 1464, and Modular Buildings 1 and 2). It will be handled on a "person-to-person" basis and will NOT be deposited in "IN" boxes, left on desks or tables, etc. Classified material will have the appropriate cover-sheet attached when it is hand-carried. Personnel hand-carrying classified material between offices WILL NOT stop in the snack bar, cafeteria, credit union, travel office, etc., or any other places not directly associated with official duties while in possession of the classified material.

CHAPTER 6

HQ ARMY MATERIEL COMMAND PROCEDURES FOR THE DESTRUCTION AND DISPOSAL OF CLASSIFIED INFORMATION

6-1. Classified information no longer needed shall be shredded in a shredder that has been approved for destruction of classified information (IAW AR 380-5). Crosscut shredders are the only authorized shredders approved for use in the destruction of classified information. The crosscut-shredding machine must reduce the material to shreds no greater than 1/32nd of an inch (plus 1/64th inch tolerance) by ½ inch crosscut. **(Before purchasing see the HQ AMC Security Manager, Room 1E14, 617-0081) to ensure the potential shredder meets the standards of AR 380-5.**

All shredders designated to destroy classified information shall be marked “GSA APPROVED TO DESTROY CLASSIFIED INFORMATION.”

All shredders not approved to destroy classified information shall be marked “THIS SHREDDER IS NOT APPROVED TO DESTROY CLASSIFIED INFORMATION.”

As a security and OPSEC enhancement, the shredding of all classified, controlled unclassified, and sensitive uncontrolled information is highly recommended.

6-2. Typewriter ribbons used in producing classified information will be destroyed as classified waste. Destruction will be accomplished by breaking the plastic apart, removing the ribbon, and shredding the ribbon. The plastic may be thrown away.

6-3. Computer disks used to store classified information will be destroyed as classified waste. Destruction will be accomplished by breaking the plastic case open, removing the disk, cutting the disk in half and shredding it. The plastic case may be thrown away.

6-4. Residue shall be inspected during each destruction to ensure the classified information cannot be reconstructed.

6-5. Shredder Waste. When shredder plastic bags are full to capacity, check the bag to ensure all particles have been shredded properly and empty the contents of the shredder bag into a dumpster or similar large sized waste container. **DO NOT PLACE** the sealed plastic bag in a dumpster (The purchase of a High Security Cross-Cut shredder will eliminate the requirement to empty the contents of the shredder bag).

6-6. Maintenance. Each Security Monitor or designated personnel is responsible for ensuring the maintenance of the shredder is conducted periodically, e.g., there is a sufficient supply of

AMC-M380-5

shredder plastic bags and the shredder is oiled/lubricated properly and calls are placed for maintenance.

CHAPTER 7

POLICY AND PROCEDURES FOR SECURITY OF MEETINGS AND CONFERENCES

7-1. Responsibility. The security of classified information used in meetings and conferences is the responsibility of the staff office hosting the meeting or conference. Prior to granting access to any classified information the custodian of that information or the host of the conference will ensure that the individual to whom the information is to be given has the appropriate security clearance. Clearance information is obtained from the HQ AMC Commandant's Office from the Personnel Security Specialist for HQ AMC personnel. Visitors outside of HQ AMC will ensure their security clearances are passed to the host of the conference prior to the conference or meeting.

Office Chiefs and Security Monitors will:

- a. Validate security clearances and need-to-know of all attendees (including HQ AMC personnel – please do not assume that all HQ AMC personnel have security clearances) prior to admitting them to the meeting.
- b. Validate the requirement to release classified information to any non-Executive branch persons attending the meeting.
- c. If foreign nationals are to attend the meeting, ensure that proper approval has been received through the AMC G-2 from Department of the Army. (See para 7-2 below).
- d. Station personnel outside the room entrance to prevent unauthorized access or disclosure of information. Ensure that access control personnel have a list of approved attendees whose clearances have been validated.
- e. Ensure that access control is maintained at all times (e.g., initial entrance, re-entrance after breaks, lunch, etc.).
- f. Ensure the speakers announce the security classification of the material being discussed at the beginning and at the conclusion of each presentation.
- g. Ensure appropriate security classification signs are displayed during classified briefings.
- h. Advise all attendees whether or not classified note taking is authorized. If authorized, explain how the notes will be secured and how they will be transmitted to the attendees' home stations.

- i. Ensure appropriate classified material cover sheets are used on ALL classified material.
- j. Ensure all classified material is properly safeguarded during all breaks in the meeting.
- k. At the conclusion of the meeting, ensure the area is thoroughly checked, and double-checked by a different person, to be sure all classified material has been removed.
- l. If electronic briefing presentation (e.g., PowerPoint slides) is used, ensure automated information system is approved to process level of classified information used.

7-2. Foreign national participation. If foreign nationals are to be invited to the meeting, coordinate with the AMC G-2. Consideration of guidance in AR 380-10 (Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives) is required to minimize the chance for a problem in the planning process. This should occur as far in advance as possible, but not less than 30 days before the event, and will address the issues of invitations (formal vs. informal), visit authorizations, and the disclosure of information. See paragraph 6-18 of AR 380-5 for specifics guidance. Also see Chapter 9 and Annex A of this memorandum for further guidance.

7-3. Meeting or conference notes. If classified and unclassified materials will be mailed to the attendees in separate packages, each unclassified package will be checked by two different people before mailing. This will ensure no classified material is inadvertently included in the unclassified package.

CHAPTER 8

SECURITY AWARENESS

8-1. Responsibility. The best defense against the compromise of classified information is an educated and aware employee. Security awareness is everyone's responsibility.

8-2. New Employees. All newly assigned military and civilian personnel are required to attend the AMC New Employee Orientation.

8-3. Training. The AMC Security Manager will conduct annual security awareness refresher training for all assigned and attached personnel. This includes the biennial Subversion and Espionage Directed Against the Army (SAEDA) training.

8-4. Security monitor. The security monitor will provide:

a. Initial security awareness training to all newly assigned or attached personnel. To satisfy this requirement simply go to the HQAMC website (www.hqamc.army.mil), scroll down to the HQ AMC Security Guide. Go to the List of Contents, all of the listed topics can be accessed under the following categories:

- (1) Procedures For Protecting Information
- (2) Protecting Sensitive Unclassified Information
- (3) Personal Conduct and Reporting Requirements

Upon completion of training, personnel will acknowledge by signing acknowledgement memorandum (See Appendix D) 1) they attended training; 2) they will comply with applicable regulations and guidance and 3) they have read and understand their obligations. The memorandum will be signed by the DCS, individual's supervisor, or DCS Security Monitor and the individual who received the training.

b. Periodic (at least semi-annual) refresher training to all personnel.

c. Security briefings to all personnel authorized to hand-carry classified material while on TDY.

8-5. Documentation. Security training will be documented.

a. Security monitors will maintain attendance lists for all training (see paragraph 8-3 and 8-4 above) for two years or until employee leaves HQ AMC. Include names, date and topic of training.

b. For annual security awareness training, SAEDA briefings, etc., the security monitor will provide AMXMI-SCM attendance figures (number assigned and number attending training) not later than 3 working days after the last training session, or as directed by AMXMI-SCM.

8-6. Inspection. The HQ AMC Security Manager will conduct announced and unannounced inspections of offices within the Headquarters. The announced inspections are:

February	G-1
March	G-2
April	G-3
May	G-3
June	Command History Office
July	G-5
August	G-6
September	G-8
October	Command Group
November	Separate Reporting Activities

CHAPTER 9

FOREIGN NATIONAL VISITORS TO THE HQ AMC

9-1. General. In order to expedite entry of foreign visitors to the AMC building and maintain security of all personnel and facilities, the Commander, AMC must be aware of all foreign nationals who visit the AMC building, to include those who visit Separate Reporting Activities or tenant organizations. If foreign nationals are to visit AMC, coordinate with AMXMI-SCM and consideration of guidance in AR 380-10 (Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives is required, to minimize the chance for a problem in the planning process. This should occur as far in advance as possible, but not less than 30 days before the event, and will address the issues of invitations (formal and informal), visit authorizations, and the disclosure of information. This chapter prescribes actions to be taken whenever a foreign national visits Headquarters, AMC. These actions are necessary to ensure compliance with AR 380-10 and AR 525-13, Antiterrorism Force Protection (AT/FP) Security of Personnel Information and Critical Resources.

9-2. Request Formats. Annex A contains a sample format for a memorandum SUBJECT: Foreign National Request for Admittance to HQ AMC.

9-3. Responsibilities.

a. The **G-2** (AMXMI-SCM) will staff requests for AMC activities, provide the AMC position with regard to approval/denial of all foreign national visits to HQ, AMC activities and HQ, Department of the Army, and maintain a master record of all official foreign national visit approvals to visit HQ, AMC and other tenant activities.

b. The **G-3 Office of Security, Law Enforcement and Force Protection** (AMCOPS-S) will, upon receipt of the memorandum from AMXMI-SCM, facilitate entry of approved foreign nationals into the AMC building by notifying guards located in the lobby.

9-4. General Officers or Senior Executive Service members. If the visit involves foreign General Officers or SES equivalent visits, the effected staff element must coordinate with the Protocol Office (AMCPR), room 10S32.

CHAPTER 10

SUSPICIOUS ACTIVITY

10-1. Security is everyone's business. The cooperation of all personnel is needed to ensure both the internal security against foreign agents working under cover and the physical security of AMC personnel and facilities.

10-2. Suspicious activity. In areas where classified information is in use, suspicious activity will be reported immediately to the **DCS**, Security Monitor, or the office supervisor. If they are not available, notify the HQ AMC Security Manager. During non-duty hours, report suspicious activity to the Guard Station at 617-1894. Examples of reportable incidents can be found in Chapter 11 of this memorandum.

10-3. Violence. Violence is used to send a message. Violent acts are usually preceded by nonviolent or less than violent messages, i.e., written, spoken, or physical action. These early messages of protest, of changes in attitude leading to violence, as well as the observable preparations for a violent attack all can provide warnings of a coming attack, if we are alert, observe, and report. AMC employees must constantly watch for and report suspicious activity. The following are examples of suspicious activity that should be reported to the G-3 Office of Security, Law Enforcement and Force Protection (617-9367) during duty hours and the Staff Duty Office (617-9223) after duty hours:

- a. Signs, speeches, or conversations that suggest violence towards established authority, leaders, ethnic, or political groups.
- b. Information that members of organized groups are quitting or being expelled as "not fitting in."
- c. Persons emotionally expressing threats of violence toward individuals, groups or institutions.
- d. Persons emotionally expressing feelings of being under attack, harassed, or targeted by some other group or person.
- e. Persons emotionally or repeatedly blaming "others" for some problem and advocating violence as a solution to the problem.
- f. Multiple off-post thefts of funds, firearms, or explosives.
- g. A stranger loitering and suspiciously observing government buildings, people, or activities.

h. A stranger asking unusual, personal, or detailed questions regarding AMC personnel, the AMC HQ building, and/or activities.

i. A person taking pictures or making sketches of personnel and/or the building.

j. An unusual, oversized, or inappropriately parked vehicle (particularly in the vicinity of large numbers of people or special events).

k. Abandoned parcel or suitcase.

l. Suspicious, oversized, or unusual mail.

10-4. Reporting. When you make a report, include as much of the following as you can.

a. Report the activity.

b. Describe any person(s) observed, i.e., name, sex, age, appearance, clothes, distinguishing features (physical, speech, etc.).

c. Provide the time of day the activity was observed.

d. Describe the location of the activity.

e. Describe the vehicle involved (e.g., make, model, year, color, license plate, distinguishing marks, etc.).

f. Describe the package, suitcase, or mail (e.g., color, size, type, brand name, distinguishing marks, etc.).

g. Describe the nature or details of any conversations or messages.

h. Provide copies of any flyers, pamphlets, or messages that can be obtained without personal risk or exposure.

CHAPTER 11

SUBVERSION AND ESPIONAGE DIRECTED AGAINST THE U.S. ARMY INCIDENTS

11-1. SAEDA requirements. Subversion and espionage directed against the U.S. Army (SAEDA) activities (see chapter 3, AR 381-12) should be reported immediately to the National Capital Region office of the 902d MI Group at commercial (703) 805-3008, **and** the HQ, AMC Security Manager at (703) 617-0081. Do NOT discuss this with anyone other than those identified above.

11-2. Reportable incidents. The following incidents and situations will be reported as indicated in paragraph 10-3 (above).

a. Attempts by unauthorized persons to obtain classified or unclassified information concerning U.S. Army facilities, activities, personnel, technology, or material through questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence, or computer hacking.

b. Known, suspected, or contemplated acts of espionage.

c. Contacts by DA personnel or their family members with persons whom they know or suspect to be members of or associated with foreign intelligence, security, or terrorist organizations. These do not include contacts which DA personnel have as a part of their official duties.

d. Contacts by DA personnel with any official or other citizen of a foreign country when that person:

(1) Exhibits excessive knowledge or undue interest about the DA member or his duties.

(2) Exhibits undue interest in U.S. technology; research, development, testing, and evaluation efforts; weapons systems; or scientific information.

(3) Attempts to obtain classified or unclassified sensitive information, concerning U.S. Army facilities, activities, personnel, or technology.

(4) Attempts to place DA personnel under obligation through special treatment, favors, gifts, money or other means.

(5) Attempts to establish any type of business relationship that is outside the range of normal official duties.

e. All incidents in which DA personnel or their family members traveling to or through foreign countries are:

(1) Subjected to questions regarding their duties.

(2) Requested to provide military information.

(3) Threatened, coerced, or pressured in any way to cooperate with a foreign intelligence service or foreign government official.

(4) Offered assistance in gaining access to personnel or locations not routinely afforded Americans.

(5) Contacted by foreign government law enforcement, security, or intelligence officials.

f. Any known, suspected, or possible unauthorized disclosure of deliberate compromise of classified information, regardless of the circumstances.

g. Information concerning any international or domestic terrorist activity or sabotage that poses an actual or potential threat to Army or other U.S. facilities, activities, personnel, or resources.

h. Any known or suspected illegal diversion or attempted illegal diversion of U.S. technology to a foreign country.

i. Active attempts to encourage military or civilian employees to violate laws, disobey lawful orders or regulations, or disrupt military activities (subversion).

j. Known or suspected acts of treason by Army personnel.

k. Participation by Army personnel in activities advocating or teaching the overthrow of the United States by force or violence or seeking to alter the form of Government by unconstitutional means (sedition).

l. Known, suspected, or attempted intrusions into classified or unclassified automated information systems by unauthorized users or by authorized users attempting to gain unauthorized access.

m. Any situation involving coercion, influence, or pressure brought to bear on DA personnel through family members residing in foreign countries.

11-3. Additional matters of Counterintelligence Interest. The following are additional matters which are of CI concern and which should be reported as SAEDA incidents.

- a. Discovery of a suspected listening device or a device which could be used for technical surveillance in a sensitive area, secure area, or conference room. DA personnel discovering such a device will not disturb it or discuss the discovery in the area where the device is located. Before taking any action, consult AR 381-14 for handling and reporting procedures.
- b. Unauthorized or unexplained absence of DA military or civilian personnel who have had TOP SECRET, Sensitive Compartmented Information (SCI), special access program, or TOP SECRET cryptographic access or an assignment to a special mission unit within the year preceding the absence.
- c. Any report of attempted or actual suicide by a DA member who has had access to classified material within one year preceding the incident.
- d. Assassination or attempted or planned assassination of anyone by terrorists or agents of a foreign power.
- e. Defection, attempted defection, threats of defection, or the return to military control of U.S. military defectors.
- f. Detention of DA personnel by a foreign government or entity with interests hostile to those of the United States.
- g. Impersonation of Army Intelligence personnel or the unlawful possession or use of U.S. Army Intelligence identification, such as badges and credentials.
- h. Willful compromise of the identity of U.S. Intelligence personnel engaged in clandestine intelligence and counterintelligence activities.
- i. Incidents in which foreign countries offer employment to U.S. personnel in the design, manufacture, maintenance, or employment of nuclear weapons.

The proponent of this memorandum is the Deputy Chief of Staff, G-2, U.S. Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommend Changes to Publications and Blank Forms), to the Commander, HQ AMC, ATTN: (AMXMI-SCM), 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

AMC-M380-5

FOR THE COMMANDER:

OFFICIAL:

RICHARD A. HACK
Lieutenant General, USA
Deputy Commanding General

MICHAEL D. COLTON
Chief, IT Programs & Support Division

DISTRIBUTION:

H
samergedess@hqamc.army.mil

APPENDIX A

SAMPLE AMC MEMORANDUM FOR BUILDING ACCESS

Office Symbol

MEMORANDUM THRU

Office of the Deputy Chief of Staff, G-2, ATTN: AMXMI-SCM
(Security Countermeasures), Room 1E14

Office of the Deputy Chief of Staff, G-3, ATTN: AMCOPS-CS
(Office of Security, Law Enforcement and Force Protection), Room 1E10

FOR HQ AMC Security Guard Force

SUBJECT: Foreign National Request for Admittance to HQ, AMC.

1. On (date) the following named individual(s) will be in the Headquarters building for briefings.

RVA Case #:

NAME(S):

RANK:

DATE OF VISIT:

2. Request they be allowed access to the building to conduct official business.

3. POC is _____.

SIGNATURE BLOCK

APPENDIX B

SAMPLE PRELIMINARY INQUIRY REPORT

Appropriate Office Symbol

MEMORANDUM FOR Headquarters, U.S. Army Materiel Command, ATTN: DCS G-2
5001 Eisenhower Avenue, Alexandria, VA 22333-5001

SUBJECT: Preliminary Inquiry No. ????? (Include the PI number assigned)

1. References.

a. AR 380-5, Department of the Army Information Security Program,
29 September 2000 and AMC Supplement 1 thereto, 19 April 2001.

b. AMC Memo 380-5, Headquarters AMC Information Security Program,
July 2002.

2. In compliance with above references, the following is my Report of Preliminary Inquiry.

3. Facts and Circumstances. (The individual conducting the inquiry will be completely objective and consider all facts and circumstances to answer the following questions. When the facts are lengthy or complicated, a separate paragraph containing a narrative summary of events, in chronological order, may also be necessary).

a. Who? (Complete identity of everyone involved and how they are involved.)

b. What? (Exact description of what happened, the information/material involved, what happened to it, and, if lost, what steps were taken to locate the missing information.)

c. When? (Date and time the incident occurred (if known) and the date and time the situation was discovered and reported.)

d. Where? (Complete identification of unit, section, activity, building, room number, etc. of where the incident took place.)

e. How? (Circumstances of the incident, chronologically, relating how the information/material was lost or compromised. Summarize the evidence supporting your conclusion and attach supporting enclosure(s) when appropriate.)

f. Why? (What are the applicable policies, regulations, etc. for controlling the information/material involved? Were they followed? Was anyone negligent or derelict in their duties? Was the unit/activity SOP adequate to ensure compliance with applicable regulations/directives for ensuring the proper protection of the information/material concerned under the circumstances?)

4. Findings. When all of the above questions have been answered, the individual conducting the inquiry will review the facts to reach findings on the following matters:

a. Did a loss of classified information/material occur?

b. Did a compromise occur, or under the circumstances, what is the probability of compromise? (Or state that a compromise did not occur, or that there is minimal risk of damage to national security.)

c. Is there any indication of significant security weaknesses in the unit/activity? If so, state them. (Were there any deficiencies in procedures for safeguarding classified information?)

d. Is disciplinary action appropriate?

5. Recommendations. (The individual conducting the inquiry will make specific recommendations based upon their findings. The recommendations will include any relevant corrective actions or administrative sanctions consistent with the findings.)

6. Comments. (Use this area for any additional comments not covered by the preceding paragraphs. If there are none, do not include this paragraph.)

7. Point of Contact. (Give full identification of the individual conducting the inquiry to include full name, rank, SSN, full unit/activity designation/location, and phone number.)

(Signature and Signature Block
of the Head of the Activity)

APPENDIX C

EXAMPLE 1

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

To: gsmart@hqtradoc.smil.mil
Cc: gijoe@hqamc.smil.mil
Subject: (U) Proper Marking of UNCLASSIFIED SIPRNET E-mail

UNCLASSIFIED

THE CLASSIFICATION OF THIS EMAIL IS UNCLASSIFIED. (The font size of "UNCLASSIFIED" classification should be at least 14 PITCH)

1. The purpose of this e-mail message is to illustrate how to mark an e-mail created on SIPRNET that is entirely UNCLASSIFIED.
2. No portion markings for this document are necessary because the entire email is UNCLASSIFIED.

UNCLASSIFIED

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 2

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

To: gsmart@hqtradoc.smil.mil
Cc: gijoe@hqamc.smil.mil
Subject: (U) Proper Marking of SIPRNET E-mail (UNCLASSIFIED with UNCLASSIFIED ATTACHMENTS)

UNCLASSIFIED

ALL PORTIONS OF THIS E-MAIL ARE UNCLASSIFIED AND ITS ATTACHMENTS ARE UNCLASSIFIED. (The font size of the "UNCLASSIFIED" classification should be at least 14 PITCH)

The purpose of this e-mail is to illustrate how to mark an e-mail message created on SIPRNET that is UNCLASSIFIED with UNCLASSIFIED attachments.



AGENDA.doc

UNCLASSIFIED

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 3

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

To: gsmart@hqtradoc.smil.mil
Cc: gijoe@hqamc.smil.mil
Subject: (S) Proper Marking of SIPRNET E-mail (UNCLASSIFIED with CLASSIFIED ATTACHMENTS)

SECRET

THE CLASSIFICATION OF THIS E-MAIL IS SECRET, REGRADE UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ATTACHMENTS. (The font size of the "SECRET" classification should be at least 14 PITCH)

1. (U) The attached MS Word file is classified SECRET//NOFORN and is the most recent edition of the HQ AMC Terrorism INTSUM.
2. (U) MSC Operations Center, ensure a copy is provided to your command's Senior Intelligence Officer (SIO).
3. (U) All personnel are required to respond back if you receive duplicate e-mails.



AGENDA.doc

REGRADE UNCLASSIFIED WHEN SEPARATED
FROM CLASSIFIED ATTACHMENTS

SECRET

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

EXAMPLE 4

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

Doe, John CIV AMC G2

To: gsmart@hqtradoc.smil.mil
Cc: gjoe@hqamc.smil.mil
Subject: (S) Proper Marking of SIPRNET E-mail (CLASSIFIED with
DECLASSIFICATION INSTRUCTIONS)

SECRET

THE CLASSIFICATION OF THIS E-MAIL IS SECRET. (The font size of the "SECRET" classification should be at least 14 PITCH)

1. (U) The purpose of this e-mail message is to illustrate how to mark an e-mail created on SIPRNET with declassification instructions. This is paragraph 1 and contains UNCLASSIFIED information. Therefore, this portion will be marked with the designation "U" in parentheses after the paragraph number.
2. (S) This is paragraph 2 and contains the highest classification for this SIPRNET e-mail, which is SECRET information. Therefore, this portion will be marked with the designation "S" in parentheses after the paragraph number.
3. (C) This is paragraph 3 and contains CONFIDENTIAL information. Therefore, this portion will be marked with the designation "C" in parentheses after the paragraph number.

DERIVED FROM: XYZ Memo, 14 March 1995
DECLASSIFY ON: Source marked X2
DATE OF SOURCE: 14 March 1995

SECRET

(CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY)

APPENDIX D

SAMPLE ACKNOWLEDGEMENT MEMORANDUM

(INITIAL SECURITY BRIEFING)

Appropriate Office Symbol

Date

MEMORANDUM FOR G2, (ATTN: Command Security Manager)

SUBJECT: Initial Security Briefing

1. I certify that the following individual has been given an initial security briefing and understands their responsibilities to protect classified information IAW AR 380-5, paragraph 9-4 and the HQ AMC Security Guide.

(Signature of Individual)

2. POC for this action is the undersigned.

(DCS Signature Block)