

Security
DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

History. This memorandum is a revision of the memorandum dated 1 May 1992.

Applicability. This memorandum applies to all Headquarters, Forces Command (HQ FORSCOM) staff agencies and personnel.

Changes. Changes to this memorandum are not official unless they are authenticated by the HQ FORSCOM Deputy Chief of Staff, G-6 (DCS, G-6 or G-6)

Suggested Improvements. The proponent for this memorandum is the Deputy Chief of Staff, G-2. Users are invited to send comments and suggested changes on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, HQ FORSCOM, DCS, G-2 (G-2) (AFIN-SD), 1777 Hardee Avenue SW, Fort McPherson, GA 30330-1062

FOR THE COMMANDER:

OFFICIAL:

DAN K. MCNEILL
Lieutenant General, USA
Deputy Commanding General/
Chief of Staff

SIGNED

WILLIAM T. LASHER
Colonel, SC
Deputy Chief of Staff, G-6

DISTRIBUTION: This publication is available in electronic media only. Special for HQ FORSCOM.

COPIES FURNISHED:

CDR, FORT MCPHERSON (AFZK-IT-AS) (record copy)

TABLE OF CONTENTS

SECTION I	Page
General	
1-1. Purpose	2
1-2. References	2
1-3. Responsibilities	2
 SECTION II	 Page
Implementing Procedures	
2-1. Safeguarding	3
2-2. Non-Disclosure Agreement	4
2-3. Classification and Marking	4
2-4. Reproduction	5
2-5. Destruction	6
2-6. Accountability and Control	7
2-7. Visit Certification	9
2-8. Classified Meetings and Conferences	9

SECTION II	Page
Implementing Procedures (Continued)	
2-9. Storage and Physical Security	10
2-10. Transmission and Transportation	11
2-11. End-of-Day Security Checks	13
2-12. Security Education	14
2-13. Unauthorized Disclosure and Other Security Incidents	14
2-14. Emergency Safeguarding	15
2-15. Inspections	15
Appendix A . Sample Security Manager Appointment Memorandum	16
Appendix B . Sample Alternate TSCO Appointment Memorandum	17
Appendix C . Sample Visit Certification Memorandum	18
Appendix D . Sample Plan for Emergency Safeguarding of Classified Material	19

SECTION I
General

1-1. Purpose.

To provide implementing guidance for the Information Security Program within HQ FORSCOM. This memorandum provides policy and procedural guidance for safeguarding collateral classified information and other controlled unclassified information. It does not apply to Sensitive Compartmented Information (SCI). All security policies and issues regarding SCI should be coordinated through the FORSCOM Special Security Office.

1-2. References.

a. Required publications:

- (1) [Army Regulation \(AR\) 380-5, Department of the Army Information Security Program.](#)
- (2) [FORSCOM Supplement 1 to AR 380-5, Department of the Army Information Security Program.](#)

1-3. Responsibilities.

a. The FORSCOM DCS, G-2, is both the Command Senior Intelligence Officer and the Command Security Manager. The FORSCOM DCS, G-2 delegates the daily execution of the security function to the Chief of the G-2 Security Division (AFIN-SD), who implements and supervises security policy and provides policy guidance regarding all security matters and procedures within the command. The Chief of the G-2 Security Division will appoint a staff representative to serve as the Headquarters Security Manager (HSM), for the execution of security functions and oversight of the information security program within HQ FORSCOM.

b. Headquarters Staff Agency Chiefs will:

(1) Implement security requirements of this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5.

(2) Appoint, in writing, an Agency Security Manager (ASM) to assist the G-2/HSM with the execution and oversight of security functions within the staff agency. Staff agency chiefs will ensure that appointed ASMs are given the necessary authority and administrative support to effectively discharge their assigned duties and responsibilities. The ASMs will be commissioned officers, warrant officers, senior Non-Commissioned Officers (NCOs), or Department of the Army (DA) civilians, with the sufficient grade, authority, training, and available duty time to effectively perform all required ASM duties and functions. Exceptions to grade requirement must be submitted in writing to the G-2/HSM for approval, and will be fully justified and contain assurances that the nominated individual can effectively perform all required ASM duties and functions. Recommend ASMs be

selected based on assigned duty positions which enhance their ability to execute their ASM duties (e.g. Executive Officer or Administrative Officer).

(3) Direct Division Chiefs to appoint Division Security Managers (DSM) to assist the ASM and the G-2/HSM with the execution and oversight of security functions within each division, if deemed necessary. The DSMs will be of sufficient rank or grade to effectively perform all required duties and functions.

(4) Provide to the G-2/HSM a copy of all agency and division security manager appointments. A sample security manager appointment memorandum is provided at [Appendix A](#). There is no requirement to reappoint security managers upon change of Agency or Division Chiefs.

c. Agency Security Managers (ASM) will:

(1) Be fully knowledgeable of all information security requirements, procedures, and responsibilities outlined in this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5, and ensure that they are implemented and enforced within their staff agency.

(2) Perform the security manager duties specified throughout this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5.

(3) Obtain approval from the G-2/HSM regarding any deviation from required policy, procedures, or responsibilities.

(4) Develop written procedural guidance for the agency, which provides detailed instructions and procedures for the various security requirements specified in this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5.

d. Division Security Managers (DSM) will:

(1) Be knowledgeable of all information security requirements, procedures, and responsibilities outlined in this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5.

(2) Perform duties as directed by the ASM, to ensure that all information security requirements, procedures, and responsibilities of this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5, are implemented and enforced within the division.

e. Individuals will:

(1) Properly protect all classified information in their personal custody.

(2) Verify the security clearance level and need-to-know before releasing classified information to other individuals.

(3) Ensure that all classified information produced or processed, is correctly marked as specified in AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

SECTION II

Implementing Procedures

2-1. Safeguarding.

a. All HQ FORSCOM personnel are responsible for safeguarding classified information for which they have access. Any holder of classified information is considered to be the custodian of the material. Custodians will provide protection and control of classified information at all times and must follow procedures to ensure that unauthorized persons do not gain access to classified information by sight, sound, or other means.

FORSCOM Memorandum 380-5

b. Classified information will not be discussed with, or in the presence of, unauthorized persons. Prior to permitting access to classified information by other individuals, their security clearance level and need-to-know will be verified. The ASMs will develop procedures to ensure that only properly cleared individuals with a valid need-to-know are authorized access to classified information within the agency. The ASMs will maintain a current security clearance roster of all agency personnel. This roster will minimally contain the name, rank, Social Security Number (SSN), date and level of clearance authorized, and date and type of investigation completed.

c. Classified material removed from storage containers must be kept under the constant surveillance and control of authorized and properly cleared individuals. This requirement also applies to classified computer hard drives and any other type of classified media or material. Classified documents will be covered with appropriate cover sheets when not in use, to prevent the classified information from being viewed by unauthorized or uncleared individuals.

d. Classified material will be properly protected and concealed during transmission and transportation, in accordance with paragraph 2-10 below and Chapter 8, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

2-2. Non-Disclosure Agreement.

a. Prior to granting access to classified information, all DA personnel are required to sign a Classified Information Non-Disclosure Agreement (NDA) (SF 312). The ASMs will ensure that all agency personnel who require access to classified information have executed and signed an NDA before allowing them access to classified information.

b. If an individual has previously executed an NDA, the ASM will maintain a copy of the NDA in the agency security files. If a previously executed NDA cannot be located, the ASM will execute a new NDA, before granting the individual access to classified information. Newly executed NDAs will be properly signed, witnessed, and dated as specified in paragraph 6-3, AR 380-5.

(1) Original NDAs signed by civilian personnel will be forwarded to the supporting local or regional Civilian Personnel Office, to be filed in the individual's Official Personnel File.

(2) Original NDAs signed by military personnel will be forwarded to the appropriate personnel records center, as specified in paragraph 6-3b, AR 380-5.

c. The ASM will maintain copies of executed NDAs for all cleared personnel assigned to the agency, until reassignment, transfer, or separation from federal employment or service. Upon transfer to a new organization, this copy will be forwarded to the gaining organization's security manager.

2-3. Classification and Marking.

a. Agency chiefs will ensure that classified documents prepared and produced within their agency are properly classified and contain the required classification instructions and markings. The ASMs will assist original classification authorities (OCA) and action officers who produce classified products, with the proper classification and marking procedures, as specified in AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

b. Original Classification. Original classification is the initial determination made by an OCA that an item of information could be expected to cause damage to national security if subjected to unauthorized disclosure.

(1) Only officially designated OCAs are authorized to make original classification decisions. The Secretary of the Army has appointed the following individuals within HQ FORSCOM as OCAs:

<u>Position</u>	<u>OCA Level</u>
Commanding General (CG)	TOP SECRET
Deputy Commanding General (DCG)	SECRET
G-2	SECRET
G-3/5/7	SECRET

(2) The OCAs are responsible for ensuring that security classification guides are prepared and issued for classified programs and projects originated under their authority. Security classification guides will be prepared in accordance to Chapter 2, AR 380-5 and FORSCOM Supplement 1 to AR 380-5, to include specificity of elements of information; declassification instructions for each element; and concise reasons for classification.

(3) The OCAs are also responsible for ensuring that interim or supplemental classification guides are prepared and issued, when the proponent command or agency OCA fails to provide adequate classification guidance. In these instances, the OCA should request additional guidance or clarification from originating proponent.

c. Derivative Classification. Derivative classification is the process of classifying an item of information based on official classification guidance provided by another source document or security classification guide.

(1) Action officers who produce derivatively classified information are responsible for making sure that the proper classification instructions and markings are applied, based on the source document or guide. Officials who sign or approve derivatively classified material are ultimately responsible for the accuracy of the derivative classification. The following is an example of a derivative classification marking:

Derived From: Operational Plan (OPLAN) XXXX
Declassify On: Source marked X5
Date of Source: 1 Jan 03

(2) Derivative classification decisions are normally made by action officers and subject matter experts (SME) who are familiar with both the information and the published classification guidance. The FORSCOM G-2 staff cannot provide derivative classification guidance for areas that are not within their area of expertise. The FORSCOM G-2 staff will assist action officers with annotating proper classification instructions and markings on classified information, after the SME has made the appropriate derivative classification decision.

d. All classified information will be properly marked with appropriate classification markings in accordance with Chapter 4, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. This requirement applies to all forms of classified information, to include electronically transmitted messages, electronic mail, photographs, charts, briefing slides, working papers, etc.

2-4. Reproduction.

a. Classified information will be reproduced only when absolutely necessary for mission accomplishment, or when specifically required by other statutes, directives, or regulations. Reproduced copies of classified information will be protected and controlled in the same manner as the original.

b. The ASM will designate reproduction (copying) equipment located within their agency authorized for the reproduction of classified information.

(1) The FORSCOM Form 138-R will be completed and conspicuously placed on or near each item of equipment authorized for reproduction of classified information.

(2) The FORSCOM Poster 93-R will be conspicuously placed on all other reproduction equipment to clearly indicate that reproduction of classified information is prohibited.

c. Reproduction of TOP SECRET information will be strictly controlled and is not authorized without the prior consent of the originator. Reproduction of TOP SECRET information must also be approved by the HQ FORSCOM TOP SECRET Control Officer (TSCO) or other command designated individual. The HQ FORSCOM TSCO will:

(1) Ensure that all reproduced copies are brought under proper control and accountability, as specified in Chapter 6, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

FORSCOM Memorandum 380-5

(2) Designate specific reproduction (copying) equipment authorized for the reproduction of TOP SECRET information.

(3) Maintain a written record of all TOP SECRET reproduction approvals, to include total pages and copies reproduced.

d. Reproduction of SECRET and CONFIDENTIAL information which requires continuous control and accountability, or has special dissemination or reproduction limitations, will not be reproduced without the review and approval of the ASM or other agency designated individual. A written record, as specified above, must also be maintained for these reproduction approvals.

e. The ASM will ensure that all reproduction requests submitted to the Fort McPherson Printing Office are reviewed for proper classification and markings, before forwarding to the printing office. The FORSCOM G-2 staff will provide assistance, as needed.

2-5. Destruction.

a. Classified information should be retained only when necessary for operational purposes, or if required by specific statutes, directives, or regulations. The ASMs will ensure that classified holdings are reviewed annually to identify and destroy any unneeded classified material. Destruction of TOP SECRET information will be accomplished only by the HQ FORSCOM TSCO. SECRET and CONFIDENTIAL information may be destroyed by each agency, as directed by the agency chief or ASM.

b. All destruction methods and devices utilized within HQ FORSCOM must meet the requirements and standards specified in Chapter 3, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Requisitions for new destruction equipment will be coordinated through the G-2/HSM to ensure that the equipment meets prescribed security standards.

(1) When utilizing approved cross-cut shredders for the destruction of classified information, the "secure volume" concept will be employed. This concept requires that no less than 20 pages of material be shredded at one time. Unclassified material may be combined with the classified material to meet the 20-page minimum requirement.

(2) When destroying classified material containing printed data that is smaller than normal printed document text (i.e. microfilm, microfiche, photographs, etc.), a more stringent destruction standard is necessary to prevent the successful reconstruction of the material. If destruction method is by shredding, a smaller sized security screen must be utilized. The ASM will ensure that these destruction standards are met when this type of classified material is destroyed by agency personnel. Destruction of classified information by burning is not authorized in the metro Atlanta area, due to a federal ban by the Environmental Protection Agency.

c. The ASM will establish written procedures for the use of destruction equipment within their agency. These procedures, as a minimum, will cover operating and safety instructions, maintenance, and security. Shredders will be inspected as part of the normal end-of-day security check to ensure all classified material processed through the device has been completely destroyed. Operating and safety instructions will be conspicuously posted on or near each approved destruction device.

d. There are two large disintegrators located in the basement of Marshall Hall, available for use by HQ FORSCOM staff agencies for the destruction of classified material. These disintegrators are capable of destroying classified paper documents, plastic material, typewriter ribbons, floppy diskettes, and compact disks. Use of the disintegrators must be coordinated through the Marshall Hall Building Security Manager.

e. For Official Use Only (FOUO) information, although not classified, must also be protected from access by unauthorized individuals. At a minimum, FOUO material must be destroyed by tearing each copy into several pieces to preclude reconstruction, and placing in normal unclassified trash receptacles.

f. Other Controlled Unclassified Information (CUI), although not classified, may also require the application of additional controls and protective measures for various reasons. This information will be destroyed as directed by the proponent of the information and Chapter 5, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Examples of CUI are Law Enforcement Agency (LEA) Sensitive material; Sensitive but Unclassified (SBU) material; Department of Defense (DoD) Controlled Unclassified Nuclear Information; Sensitive Information, as defined by the Computer Security Act of 1987; and information contained in technical documents.

2-6. Accountability and Control.

a. TOP SECRET Information.

(1) All TOP SECRET information will be provided continuous control and accountability as specified in Chapter 6, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

(2) The FORSCOM G-6 will formally appoint a HQ TSCO. The HQ TSCO is responsible for receiving, dispatching, and maintaining accountability and access records for all TOP SECRET information within HQ FORSCOM, in accordance with AR 380-5, FORSCOM Supplement 1 to AR 380-5, and this memorandum. The HQ TSCO will also maintain the TOP SECRET Accountability Register for HQ FORSCOM.

(3) Agency chiefs will formally appoint Alternate TSCOs to receipt and dispatch TOP SECRET information, through the HQ TSCO, for their individual agency. A sample Alternate TSCO appointment memorandum is provided at [Appendix B](#).

(4) All TOP SECRET material must be processed through the HQ TSCO for proper control and accountability. Only the HQ TSCO is authorized to reproduce, destroy, post changes to, or transfer TOP SECRET material to agencies outside HQ FORSCOM.

(5) When requested, agencies will provide an Alternate TSCO or other properly cleared and knowledgeable individual to assist the HQ FORSCOM TSCO during the destruction or inventory of agency TOP SECRET holdings.

(6) All ASMs will provide the HQ FORSCOM TSCO with a current TOP SECRET Access Roster.

b. SECRET and CONFIDENTIAL Information.

(1) Within FORSCOM, continuous control and accountability of SECRET and CONFIDENTIAL information is prohibited, unless required by other regulations or directives, or specifically requested by the originator. This includes requirements such as document registers, continuous receipting requirements, destruction certifications, and inventories. Certain administrative measures are permitted for the purpose of locating classified material; therefore, custodians may maintain records or listings of classified holdings, which identify the title, date, and location of the classified material. Records or listings will not be used for accountability purposes. The absence of control requirements will not be construed as relief from responsibility for the proper safeguarding of SECRET and CONFIDENTIAL information.

(2) The DA Form 3964 will be used to verify the receipt of SECRET material sent by mail to agencies outside the Headquarters. Receipt forms must include, at a minimum, the originator address, recipient address, unclassified or short title of the document, classification level of the document, and number of copies mailed. A copy of the receipt form will be maintained in a suspense file and a tracer action initiated if signed receipt form has not been received by the recipient within 15 working days.

(3) As stated above, certification of destruction is not required for SECRET and CONFIDENTIAL information, unless required by other regulations or directives.

(4) Unless required by other directives, periodic inventory of SECRET and CONFIDENTIAL material is prohibited.

FORSCOM Memorandum 380-5

c. Classified Working Papers.

(1) Classified working papers are documents and material accumulated or created in the preparation of finished documents and material. Classified working papers will be safeguarded and marked in accordance with paragraph 6-24, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

(2) The classified working paper concept will not be used to circumvent normal control, marking, or safeguarding requirements.

(3) All TOP SECRET working papers will be brought under the control by the HQ TSCO as soon as they are created.

d. Foreign Government Information.

(1) Foreign Government Information, especially that which is classified, will be protected, controlled, marked, and destroyed in strict accordance with the respective government's policies and procedures, and Chapter 4, AR 380-5.

(2) The HQ TSCO, who also serves as the COSMIC TOP SECRET ATOMAL (CTSA) Control Officer, will establish procedures for the protection and control of all North Atlantic Treaty Organization (NATO) documents and material received and dispatched by HQ FORSCOM. Access to NATO information will only be authorized to individuals with the appropriate commensurate US security clearance, need-to-know, and who have received the appropriate security briefing. The CTSA Control Officer will establish initial briefing, rebriefing, and debriefing schedules for HQ FORSCOM personnel in accordance with NATO regulations.

e. Controlled Unclassified Information.

(1) As stated in paragraph 2-5e above, CUI, although not classified, may also require additional controls and protective measures for various reasons. This information will be controlled, marked, and destroyed as directed by the proponent of the information and Chapter 5, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

(2) For Official Use Only (FOUO) may only be designated for information which meets one of the nine exemptions to the Freedom of Information Act, as specified in AR 25-55, The DA Freedom of Information Act Program. The FORSCOM G-6 is the HQ FORSCOM proponent for providing guidance regarding the designation and/or release of FOUO information within HQ FORSCOM. As stated in paragraph 2-5e above, FOUO material will be destroyed by tearing each copy into several pieces to preclude reconstruction, and placing in normal unclassified trash receptacles.

(3) The LEA Sensitive information will be controlled, marked, and destroyed in accordance with Chapter 5, FORSCOM Supplement 1 to AR 380-5.

f. Joint Chiefs of Staff (JCS) Papers.

(1) All JCS papers are various forms of documents and information originated by the Joint Staff, which have special restrictions regarding their access, release, and distribution. All JCS papers will be controlled and protected in accordance with JCS policy and Chapter 4, AR 380-5.

(2) The ASMs will ensure that all personnel who have access to JCS papers are briefed on their responsibilities for safeguarding JCS information upon initial assignment, and annually thereafter.

2-7. Visit Certification.

a. Incoming Visits:

(1) All HQ FORSCOM personnel who host visitors to Marshall Hall are individually responsible for verifying the visitor's security clearance and need-to-know, before allowing access to classified information. Verification will normally be in the form of a visit request or certification memorandum from the visitor's employing activity. The visit certification must be signed by an official other than the visitor, and that official must be in a position to verify the individual's security clearance.

(2) Visit certifications must be provided to the Marshall Hall Security Coordinator at least one day in advance of visit. For frequent/recurring visitors, a visitor access roster is required. Access rosters will be authenticated by the ASM of the visited staff agency, and will contain the following information:

- Full Name
- SSN or Identification Number
- Rank/Grade
- Date/Place of Birth
- Employing Activity
- Date and Duration of Visit (not to exceed one year)
- Security Clearance Level
- Date Clearance Granted
- Point of Contact for Visitor

b. Outgoing Visits:

(1) It is the responsibility of each HQ FORSCOM staff agency to provide advance notice and security clearance verification to the visited activity of anticipated visits by staff members who will require access to classified information. Verification will normally be in the form of a visit request or certification memorandum.

(2) The visit certification will contain all required information specified in paragraph 6-16, AR 380-5. The visit certification will be authenticated and signed by the ASM. This responsibility may be delegated to the DSM, as determined by the staff agency chief or ASM. The Installation Security Office security clearance verification memorandum will not be used as a visit certification. A sample visit certification memorandum is provided at [Appendix C](#).

2-8. Classified Meetings and Conferences.

a. Conference rooms located in Marshall Hall are approved for classified discussions; therefore, classified meetings will be conducted within Marshall Hall whenever possible. Sponsors of classified meetings are responsible for ensuring that classified information is limited to persons possessing the appropriate security clearance and the need-to-know for the specific information. This includes providing the proper control of physical, visual, and auditory access to the classified information.

b. TOP SECRET meetings held within Marshall Hall must be coordinated with the HQ TSCO for proper control and accountability of the TOP SECRET information presented.

c. Classified meetings to be conducted in other uncleared facilities located on Fort McPherson and Fort Gillem (i.e., installation theater, training classroom, etc.), require the prior written approval of the G-2/HSM and Installation Security Office, and will only be granted in exceptional circumstances. Requests for approval will be fully justified and will include assurances that all additional security measures specified in paragraph 6-18, AR 380-5 and FORSCOM Supplement 1 to AR 380-5 will be accomplished.

d. Classified meetings will not be held at locations other than US Government installations or cleared contractor facilities, without the approval of the Office of the Secretary of Defense.

FORSCOM Memorandum 380-5

e. Any classified meeting involving non-US government associations or foreign participation, require the approval of HQDA (DAMI-CD). Requests will be submitted through the G-2/HSM and will include all information and assurances specified in paragraph 6-18, AR 380-5.

2-9. Storage and Physical Security.

a. TOP SECRET Material. TOP SECRET material will only be stored in areas and containers specifically designated and approved by the HQ TSCO.

b. Security Containers.

(1) Classified material will only be stored in General Services Administration (GSA) approved security containers. Security containers will be inspected and approved by the ASM before being authorized for storage of classified material, to ensure that they meet GSA standards. The ASM will assign identification numbers to all approved security containers within their agency. Identification numbers will be affixed to the outside of each container, and will also be recorded on the respective Standard Form (SF) 700 (Classified Container Information) for that container.

(2) The tops of security containers will be free of extraneous material, to prevent classified material from being inadvertently left unsecured or intermingled with other unclassified material.

(3) Security containers that are not approved for storage of classified material will be clearly marked with the following notice: NOT AUTHORIZED FOR STORAGE OF CLASSIFIED INFORMATION.

(4) Open storage of classified information will only be authorized when necessary for mission accomplishment or when the volume or size of the classified information prohibits storage in GSA approved security containers. Open storage vaults or secure rooms must meet physical and procedural requirements of Chapter 7, AR 380-5 and FORSCOM Supplement, and require the written approval of the G-2/HSM.

c. Locks/Combinations.

(1) Each security container must be equipped with a GSA approved lock meeting current GSA and federal standards.

(2) Combinations will be changed annually and as required by paragraph 7-8, AR 380-5. The ASMs are responsible for ensuring that all lock combinations are changed as required within their agency. Only properly cleared and technically competent individuals are authorized to change combinations. Professional locksmiths assigned to the installation are available, upon request, to provide training and assistance in changing combinations. Requests for training or assistance should be submitted to the Marshall Hall Building Security Manager.

(3) New combinations will be tested at least three times before locking the container. If the new combination does not successfully open the security container, the installation locksmith should be contacted to assist in changing, repairing, or replacing the lock.

(4) No two security containers within the same agency will have the same combination. Memory or convenience numbers, such as birthdays, telephone numbers, street addresses, or social security numbers, will not be used as combinations.

(5) Combinations to security containers will be classified at the highest level of the classified material authorized for storage within the container. The combination will be recorded on SF 700 (Part 2A) and placed inside the envelope portion of the form (Part 2). Both part 2A and Part 2 will be marked with the appropriate classification of the combination. Combinations will not be personally retained in wallets, purses, briefcases, desk drawers; on calendars, organizers, or note pads; or in other unapproved locations. Any medium containing a combination to a classified storage container will be properly marked and protected as classified information.

(6) Combinations to TOP SECRET storage containers or facilities will be provided to the HQ FORSCOM TSCO for proper control and safeguarding. Combinations to SECRET and CONFIDENTIAL storage containers or facilities will be stored in a designated master container within each agency. Combinations to agency master containers will be provided to the FORSCOM Operations Center (FOC) for proper control and safeguarding. The FOC will designate a security container for this purpose.

(7) Part 1 of SF 700 will contain the required information for the primary individual responsible for each security container, as well as other individuals who have access to the combination of the container, and will be placed on the inside of the locking drawer of the security container.

(8) In the event a combination lock fails to open a security container (lock out), the ASM will be notified, who will contact the DoD Lock Program Proponent for assistance in attempting to open the container. If this method fails, the ASM will coordinate with an installation locksmith to have the security container drilled to access the container. Once a security container is drilled, the classified material contained within must be removed and stored in another approved security container until the drilled container has been properly repaired in accordance with GSA approved standards.

2-10. Transmission and Transportation.

a. Approved Methods of Transmitting and Transporting Classified Material:

(1) TOP SECRET material may be transmitted and transported only by approved encrypted electronic methods or by authorized couriers, as specified in paragraph 8-2, AR 380-5. Hand carrying of TOP SECRET material outside this headquarters requires the advance approval of the G-2/HSM, and must be coordinated and processed through the HQ TSCO.

(2) SECRET and CONFIDENTIAL material may be transmitted and transported only by approved encrypted electronic methods, authorized couriers, or mailed through the US Postal Service or other authorized mail delivery systems, as specified in paragraphs 8-3 and 8-4, AR 380-5. Mailing of SECRET and CONFIDENTIAL material must be coordinated with and processed through the HQ FORSCOM Classified Material Control Office (CMCO).

(3) The increased use of Secret Internet Protocol Router Network (SIPRNET) computers within HQ FORSCOM has resulted in an increase in users inadvertently transferring and transmitting classified information from SIPRNET computers to unclassified computers and networks. All ASMs will ensure that agency personnel are trained and educated on the proper procedures for processing, transmitting, marking, and safeguarding classified information on SIPRNET computers and other accredited automated information systems.

b. Authority to Approve Hand carrying of Classified Information.

(1) Hand carrying of classified information will only be authorized when absolutely necessary and when no other acceptable methods are available (i.e., secure fax, electronic message/e-mail, mail).

(2) As stated above, hand carrying of TOP SECRET material requires the approval of the G-2/HSM.

(3) Hand carrying of SECRET or CONFIDENTIAL material may be approved by the ASM in accordance with the provisions specified in this memorandum, Chapter 8, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. The ASM may delegate approval authority to DSMs; however, the ASM is responsible for ensuring that DSMs comply with all provisions specified in this memorandum and above regulations.

c. Hand carrying Classified Material within the Local Area.

(1) Written courier authorization is required for individuals who hand carry classified material between buildings on Fort McPherson and to locations within the local surrounding area. A Courier Authorization Letter will be used for one time courier authorizations and a Department of Defense (DD) Form 2501 (Courier Authorization Card) will be used when there is a recurrent need to locally hand carry classified material. A DD Form 2501 will not be used for courier authorization to locations outside the local surrounding area. All ASMs will maintain a

FORSCOM Memorandum 380-5

record of all courier authorizations issued within their agency. A sample Courier Authorization Letter is provided at Appendix M, FORSCOM Supplement 1 to AR 380-5.

(2) Individuals approved to locally hand carry classified material will be briefed on their individual security responsibilities. Individuals will certify in writing that they have received this briefing and that they fully understand their responsibilities and the provisions of this memorandum and Chapter 8, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Individuals who frequently hand carry classified material may be briefed at annual intervals. All ASMs will maintain a record of all courier briefings issued within their agency. The HQ FORSCOM CMCO is available to assist ASMs with briefing and certifying individuals authorized to hand carry classified material. A sample briefing/certification is provided at Appendix L, FORSCOM Supplement 1 to AR 380-5

(3) Classified material hand carried between buildings on Fort McPherson will be concealed by placing in an unmarked container, such as an envelope or briefcase. Classified material hand carried within the local surrounding area of Fort McPherson will be placed in a wrapped, sealed, and marked inner container, as specified in paragraph 8-9, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. A brief case may be used as the outer wrapper, when hand carrying classified material within the local surrounding area only. For the purpose of this memorandum, the local surrounding area is defined as any location within a 25-mile radius of Fort McPherson. Classified material hand carried outside the local surrounding area will be double-wrapped in accordance with paragraph 8-9, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. The HQ FORSCOM CMCO is available to assist individuals with preparing and wrapping classified material to be hand carried.

(4) The DD Form 2501 (Courier Authorization Card):

(a) As stated above, DD Forms 2501 will only be issued to individuals with a demonstrated need to frequently hand carry classified information on the installation or within the local surrounding area, and will not be issued as blanket authority to hand carry classified information.

(b) The G-2/HSM is the central controlling authority for all DD Forms 2501 issued within the headquarters. The G-2/HSM will issue forms by serial number to each ASM utilizing DA Form 410 (Receipt for Accountable Form). The ASM may further disseminate forms to subordinate DSMs for issuance to division personnel; however, ASMs will remain responsible for the overall control and accountability of the forms.

(c) Issuance of DD Forms 2501 to individuals will be documented using a sign-out roster format, which will include at a minimum the individual's full name; rank; SSN; security clearance; authorized level; date of issue; date of expiration; and name and signature of the security manager issuing the DD Form 2501.

(d) The ASM will maintain full accountability of all DD Forms 2501 issued to the agency, to include the total number issued to the agency; individual records (by serial number) of active forms issued to individuals; and inactive forms that have been turned-in or destroyed. Unissued forms and accountability records of forms will be secured under lock and key.

(e) The ASM will ensure that all blocks of DD Forms 2501 are completed, fully and accurately. Expiration date (Block 2) will not exceed two years from the date of issuance. Geographical limits (Block 7) will be annotated with "25-mile radius of Fort McPherson, GA." Duty phone number (Block 10a) will be that of the issuing security manager. After hours phone number (Block 10b) will be that of the FORSCOM FOC (404) 464-5222, who will contact the respective ASM at home, if necessary. All DD Forms 2501 will be signed by both the individual and the issuing security manager.

(f) Issued DD Forms 2501 may be retained by individuals for the duration of the authorization period. Lost or stolen forms will be immediately reported through the ASM to the G-2/HSM.

d. Hand carrying Classified Material Aboard Commercial Aircraft.

(1) A Courier Authorization Letter is required for individuals who hand carry classified material aboard commercial aircraft, both in the Continental United States (CONUS) and Outside CONUS (OCONUS). Courier Authorization Letters will be issued for each specific courier requirement, and will not be issued as recurrent blanket

authorizations to hand carry classified material. The ASM will maintain a record of all courier authorizations issued within their agency.

(2) Individuals approved to hand carry classified material aboard commercial aircraft will be briefed on their individual security responsibilities. Individuals will certify in writing that they have received this briefing and fully understand their responsibilities, and the provisions of this memorandum, Chapter 8, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Individuals who frequently hand carry classified material may be briefed at annual intervals. The ASM will maintain a record of all courier briefings issued within their agency. The HQ FORSCOM CMCO is available to assist agency security managers with briefing and certifying individuals authorized to hand carry classified material. A sample briefing/certification is provided at Appendix L, FORSCOM Supplement 1 to AR 380-5.

(3) Classified material hand carried aboard commercial aircraft will be double-wrapped in accordance with paragraph 8-9, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. The HQ FORSCOM CMCO is available to assist individuals with preparing and wrapping classified material to be hand carried.

(4) The Courier Authorization Letter will contain all required information as specified in paragraph 8-15, AR 380-5 and will be signed by the issuing security manager. The courier will keep the original copy of the authorization letter in his possession. A sample Courier Authorization Letter is provided at Appendix M, FORSCOM Supplement 1 to AR 380-5.

(5) The issuing security manager will maintain an inventory which identifies all classified information being hand carried for each individual courier authorization.

(6) As stated above, hand carrying of classified information should only be authorized when absolutely necessary, and when no other acceptable methods are available. Hand carrying classified information aboard commercial aircraft, especially to overseas locations, subjects the information to increased risks. Therefore, ASMs should carefully consider all risks and alternative measures available before authorizing the hand carry of classified information aboard commercial aircraft.

(7) A Courier Authorization Letter is not required for hand carrying classified information aboard military aircraft or military chartered aircraft; however, all other security procedures apply.

2-11. End of Day Security Checks.

a. All ASMs are responsible for ensuring that end-of-day security checks are performed at the end of each working day within each division and office, to ensure that all classified material has been properly secured. End of day security checks will be performed in accordance with the provisions of this memorandum, paragraphs 6-10 and 6-11, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Standard Form (SF) 701 (Activity Security Checklist) or similar local form will be used to record daily end of day security checks. The ASMs or DSMs will prepare written appointments or rosters designating specific individuals, by name, responsible for conducting end of day security checks. End of day security checks do not relieve individuals of their responsibility to protect and secure classified material in their custody.

b. End-of-day security checks will minimally include:

(1) Check of all security containers to ensure they are properly locked and checked, and that SF 702 (Security Container Check Sheet) has been annotated and initialed. If a security container is still in use at the time the end-of-day security check is performed, it is the responsibility of the individual assigned the security container to ensure that the security container is locked and checked by a separate individual, before departing the office. Individuals may contact the Marshall Hall Security Guard Office for assistance in checking and initialing security containers.

(2) Checking desktops and other surfaces to ensure they are free of classified material.

(3) Checking wastebaskets to ensure they do not contain any classified material.

FORSCOM Memorandum 380-5

(4) Checking all magnetic media and electronic processing devices (i.e., computer hard drives, electronic memory typewriters, facsimile machines, printers, copiers) which process classified information, to ensure that classified information has been cleared, removed, destroyed, or properly secured in an approved security container.

2-12. Security Education.

a. The ASM will ensure that all assigned personnel within their agency receive initial security orientations, annual security refresher briefings, security termination briefings, and other security related training and education, as required by Chapter 9, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Security training and education requirements will be coordinated with the Installation Security Office, who has the overall responsibility for establishing security awareness, education, and training programs for all units and activities on the installation. The FORSCOM G-2 staff is also available to provide security related training and education assistance, when needed.

b. The ASM will ensure that all assigned personnel traveling outside the US and its territories receive an area of responsibility (AOR) threat update for the country visited, within two months of travel. Threat updates will be coordinated with FORSCOM G-2 (AFIN-SD), who has the overall responsibility for providing threat updates and briefings for all assigned personnel within HQ FORSCOM.

2-13. Unauthorized Disclosure and Other Security Incidents.

a. The unauthorized disclosure (or compromise) of classified information can result in damage to national security and sensitive military operations, and can endanger the lives of military personnel. Unauthorized disclosure normally occurs as a result of violations of security procedures or security weaknesses. Not all security violations or security weaknesses result in a compromise. Therefore, it is imperative that each violation, weakness, or security related incident be immediately investigated to determine if a compromise has occurred, and if so, to minimize the damage and prevent further compromise.

b. Reporting Procedures.

(1) Any individual who becomes aware of a security violation, weakness, or incident involving the possible loss or compromise of classified information, will immediately notify their supervisor, who will report the information through channels to the agency chief and ASM.

(2) Any individual who discovers unattended classified information, to include an open security container, will safeguard the classified information and immediately report the information through channels to their agency chief and ASM. If an open security container is found, the individual(s) listed on the SF 700 (Security Container Information) will also be contacted and directed to inventory the contents, secure any classified material involved, and report the circumstances to the agency chief and ASM. The SF 700 should be attached to the inside of the locking drawer of the security container.

(3) If unattended classified information, to include an open security container, is discovered after duty hours, and the ASM and/or individual(s) listed on the SF 700 cannot be located, the Marshall Hall Security Guard Office, (404) 464-7353, will be notified. The Security Guard Office will contact the respective ASM at home, who will take the appropriate actions to ensure the classified information is properly secured.

c. Preliminary Inquiry.

(1) Agency chiefs will ensure that a preliminary inquiry is conducted for any security incident occurring within their agency that involves the possible loss or compromise of classified information, and will concurrently notify the G-2/HSM. If another agency or organization appears responsible, the agency chief will also notify the agency or organization concerned of the incident and circumstances.

(2) Preliminary inquiries will be conducted in accordance with Chapter 10, AR 380-5 and FORSCOM Supplement 1 to AR 380-5. Preliminary inquiry reports will be prepared in the format provided in Figure 10-1, AR 380-5, and provided to the G-2/HSM within twenty working days from the date of discovery of the incident.

(3) The ASM is responsible for ensuring that preliminary inquiries are promptly and properly completed, and that corrective actions are implemented.

(4) The G-2/HSM will review the results of preliminary inquiry reports to determine if the findings, recommendations, and corrective actions are sufficient to resolve and close the issue, or if further action or investigation is warranted.

d. Common Security Violations: Security violations and weaknesses normally can be prevented through effective security education and oversight programs. All ASMs will develop procedures within their agency to ensure that security policies and procedures are fully understood and enforced. The following are some of the most common security violations that occur within HQ FORSCOM, and warrant additional attention:

- (1) Processing or transmitting classified information on unclassified computer and networks.
- (2) Failing to properly annotate classified material with the appropriate classification/declassification markings.
- (3) Leaving classified computer hard drives in unattended computers.
- (4) Failing to properly label classified magnetic media (i.e., diskettes, compact disks).
- (5) Failing to double check security containers during end-of-day security checks.

2-14. Emergency Safeguarding.

a. All ASMs will develop an emergency plan for the protection, removal, and destruction of classified material within their agency, in the event of an emergency, such as enemy action, terrorist activity, civil disturbance, or natural disaster. A sample emergency plan template is provided at [Appendix D](#).

b. All ASMs will establish procedures to ensure that excess or unneeded classified material is destroyed, to reduce the amount of classified material on hand.

2-15. Inspections.

a. Staff representatives of the FORSCOM G-2 will conduct announced security inspections of each HQ FORSCOM staff agency on an annual basis, when adequate resources are available; otherwise, inspections will be conducted at least every two years.

(1) The purpose of security inspections will be to verify compliance with information security requirements and procedures specified in this memorandum, AR 380-5, and FORSCOM Supplement 1 to AR 380-5, and to evaluate the effectiveness of the HQ FORSCOM information security program.

(2) Each agency to be inspected will be notified at least 30 days prior to the date of scheduled inspection.

b. Staff representatives of the FORSCOM G-2 will also conduct periodic unannounced after-duty-hour inspections of selected staff agencies, to ensure compliance with security policies and procedures.

c. All ASMs will conduct periodic announced/unannounced inspections and spot checks within their agency, as necessary, to evaluate the effectiveness of the agency's information security program. Follow-up inspections will also be conducted to monitor the completion of required corrective actions.

d. All inspections and follow-up inspections will be formally documented and retained on file by the inspecting agency. Copies of inspection reports will also be provided to the G-2/HSM.

e. Additional guidance for conducting and documenting security inspections is provided in paragraph 1-24, AR 380-5 and FORSCOM Supplement 1 to AR 380-5.

APPENDIX A
Sample Security Manager Appointment Memorandum

(OFFICIAL LETTERHEAD)

(OFFICE SYMBOL)

(DATE)

MEMORANDUM FOR _____

SUBJECT: Appointment of [Agency/Division] Security Manager

1. References:

a. AR 380-5, Department of the Army (DA) Information Security Program, 29 September 2000.

b. FORSCOM Supplement 1 to AR 380-5, DA Information Security Program, 27 May 2003.

c. FORSCOM Memorandum 380-5, Information Security Program, (date).

2. In accordance with the above references, you are hereby appointed as the [Agency/Division] Security Manager for [Agency/Division], effective _____.

3. You are required to thoroughly familiarize yourself and comply with all provisions outlined in the above references, and to perform the duties and responsibilities specified in reference c above.

SIGNATURE BLOCK OF AGENCY CHIEF

CF:
DCS, G-2 (AFIN-SD)

APPENDIX B

Sample Alternate Top Secret Control Officer Appointment Memorandum

(OFFICIAL LETTERHEAD)

(OFFICE SYMBOL)

(DATE)

MEMORANDUM FOR _____

SUBJECT: Appointment of HQ FORSCOM Alternate Top Secret Control Officer (TSCO)

1. References:

a. AR 380-5, Department of the Army (DA) Information Security Program, 29 September 2000.

b. FORSCOM Supplement 1 to AR 380-5, DA Information Security Program, 27 May 2003.

c. FORSCOM Memorandum 380-5, Information Security Program, (date).

2. In accordance with the above references, you are hereby appointed as the HQ FORSCOM Alternate TSCO for [Agency/Division], effective _____.

3. You are required to thoroughly familiarize yourself and comply with all provisions outlined in the above references, and to perform the duties and responsibilities specified in reference c above.

SIGNATURE BLOCK OF AGENCY CHIEF

CF:

DCS, G-2 (AFIN-SD)

DCS, G-6 (TSCO)

APPENDIX C
Sample Visit Certification Memorandum

(OFFICIAL LETTERHEAD)

(OFFICE SYMBOL)

(DATE)

MEMORANDUM FOR (VISITED ACTIVITY)

SUBJECT: Verification of Collateral Security Clearance

1. The following security clearance information is provided to support a visit by the individual listed below to your organization from _____ to _____. This memorandum serves as official verification of his/her security clearance.

a. Name: _____

b. SSN: _____

c. Rank/Grade: _____

d. Date/Place of Birth: _____

e. Security Clearance Level: _____

f. Visiting Activity POC/Phone No:

g. Purpose of Visit:

2. If additional information is required, please contact the undersigned at (xxx) xxx-xxxx, DSN: xxx.

SIGNATURE BLOCK OF AGENCY/
DIVISION SECURITY MANAGER

APPENDIX D

Sample Plan for Emergency Safeguarding of Classified Material

1. Classified material must be safeguarded from the threat of loss or compromise in the event of an emergency, such as enemy action, terrorist activity, civil disturbance, fire or natural disaster. This plan addresses actions to be taken by individuals assigned to _____ (agency) for safeguarding classified material in the event one of the above situations occurs.

a. When circumstances permit securing of classified material:

(1) Collect all classified material in your work area and store in the nearest security container; lock the container; and immediately vacate the building or seek shelter.

(2) The senior representative present will ensure all security containers in their AOR are locked prior to vacating the building.

b. When circumstances do not permit securing of classified material:

(1) Collect all classified material in your work area and maintain in your possession as you vacate the building or seek shelter.

(2) Upon reaching the assembly point, individuals hand carrying classified material must report that fact to the ASM/DSM or senior representative present. The ASM/DSM or senior representative present will either take possession of the classified material or provide the individual further instructions for storing and safeguarding the material.

c. In the event of such an acute emergency that evacuation of the building is urgent, it may be necessary to leave classified material unsecured in the building. In this event, the person leaving the classified material unsecured will advise the ASM/DSM or senior representative present as soon as possible after exiting the building and reaching safety. The ASM/DSM or senior representative present will also advise the G-2/HSM that classified material was left unsecured in the building.

2. If the threat is caused by:

a. Fire and Natural Disaster. Proceed to _____ and await further instructions.

b. Enemy Action, Terrorist Attack, or Civil Disturbance. Remain in the building and await further instructions.

3. Individuals will acquaint themselves with and periodically review this plan and upon implementation will, as conditions warrant, execute the actions indicated.

**SIGNATURE BLOCK OF AGENCY/
DIVISION SECURITY MANAGER**