Department of the Army
Headquarters, United States Army Forces Command
1777 Hardee Avenue, SW
Fort McPherson, Georgia 30330-1062
27 May 2003

Security
DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

Supplementation. Further supplementation is not permitted without prior approval of the FORSCOM Deputy Chief of Staff (DCS), G-2.
Suggested improvements. The proponent agency for this supplement is the FORSCOM DCS, G-2. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Headquarters, US Army Forces Command, DCS, G-2 (AFIN-SD), 1777 Hardee Avenue, SW, Fort McPherson, GA 30330-1062.

FOR THE COMMANDER:

OFFICIAL:

JULIAN H. BURNS
Major General, USA
Chief of Staff

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

Distribution: This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for HQ FORSCOM, LO at HQ FORSCOM; CONUSAs, USAR, ARNG.

Copies Furnished: HQDA (DAMI-CD); USARC; NGB; HQ FORSCOM (AFCI-A) (Record Copy)

AR 380-5, dated 29 September 2000, is supplemented as follows:

Add the following appendices to the table of contents:

J. Sample Report of Security Inspection
K. Sample Unannounced Security Check (After Duty Hours)
L. Sample Courier Briefing and Certification
M. Sample Courier Authorization
N. Suggested Topics for Security Education Briefings
O. Sample Preliminary Inquiry Appointment Memorandum
P. Sample Appointing Authority Review Memorandum
Q. FORSCOM Major Subordinate Commands, Senior Mission Commands, and Direct Reporting Units

Chapter 1, Paragraph 1-6e. Add the following subparagraphs:

(1) The FORSCOM Deputy Chief of Staff, G-2 is both the Command Senior Intelligence Officer and the Command Security Manager. The FORSCOM 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.

*** This supplement supersedes FORSCOM Supplement 1 to AR 380-5, dated 15 December 1988.**

(2) In a similar manner, FORSCOM Major Subordinate Commands, Senior Mission Commands, and Direct Reporting Units (as designated in APPENDIX Q) will appoint a Designated Unit Security Manager (DUSM). The DUSMs will be responsible for implementation and oversight of the Information Security Program for their respective command/unit. The DUSMs will be appointed in writing, and will serve as the primary proponent for all information security matters, and security advisor to the commander.

(3) The principal duties and responsibilities of the DUSM are as follows:

(a) Perform those duties specified in Paragraph 1-7, AR 380-5, as the designated unit level equivalent to a Command Security Manager.

(b) Serve as the designated unit's principal point of contact for coordinating information security requirements and issues with the FORSCOM G-2. Designated Senior Mission Commands which are subordinate to a Major Subordinate Command (MACOM) will inform their higher headquarters of all information security related issues and transactions coordinated with the FORSCOM G-2.

(c) Serve as the designated unit's delegation authority for all information security program delegations authorized by the FORSCOM G-2 to the unit, as specified in this supplement. Designated Senior Mission Commands which are subordinate to a major subordinate command (MSC) will inform their higher headquarters of all decisions and authorizations made as a FORSCOM delegated authority.

(4) The DUSMs will be commissioned officers; warrant officers; Senior NCOs; or DA civilians, with the sufficient grade, authority, training, and available duty time to effectively develop and implement the Information Security Program for their respective units. Contractors will not be appointed as DUSMs, due to several critical functions of these positions that are prohibited from being performed by contractor personnel. Requests for waivers to this requirement will be reviewed on a case-by-case basis, with strong justification and explanation of how prohibited functions can be effectively delegated to other personnel. Requests for waivers will be submitted to the FORSCOM G-2 for review and approval.

(5) Additional security managers may be appointed for subordinate units and activities, as determined by the commander.

(6) A copy of DUSM appointments will be provided to the FORSCOM G-2.

Chapter 1, Paragraph 1-10. Add the following paragraphs:

a. This supplement applies to all military and civilian personnel employed by, and assigned or attached to FORSCOM commands, units, and activities. It applies to members of the Army National Guard only when on Federal Active Duty.

b. In the event that procedures specified in this supplement directly conflict with information security requirements of the host installation, the DUSM will immediately notify the FORSCOM G-2. The FORSCOM G-2 will coordinate with the Installation Management Agency (IMA) for resolution. In the interim, this supplement will take precedence over local installation policy, pending final resolution and guidance by this headquarters.

c. Liaison officers assigned to FORSCOM from other commands and agencies will conform to security requirements of this command insofar as operational requirements permit. Requests for deviation from FORSCOM policies may be authorized by the DUSM, when in conflict with security procedures of their parent organization.

d. Contractor visitors to FORSCOM commands, units, and activities who are performing classified contract activities will also conform to security requirements of this command. Requests for deviation from FORSCOM policies may be authorized by the DUSM, when in conflict with security procedures of their cognizant security office.

e. Any person subject to this regulation who inadvertently comes into possession of classified material, for which he/she is not authorized access, will safeguard the material and take action as specified in Paragraph 10-2, AR 380-5. The DUSM will take other appropriate actions as specified in Chapter 10, AR 380-5, and this supplement.

Chapter 1, Paragraph 1-18b. Add the following subparagraphs:

(1) FORSCOM recommends the use of mock or "notional" classified information only in rare instances designed to meet specific training objectives.

(2) When using mock or "notional" classified information during military exercises, it will be clearly identified as such. The words "CLASSIFIED FOR TRAINING ONLY" shall be annotated directly below the overall classification markings, as specified in Paragraph 4-4, AR 380-5, and this supplement. The following is an example of the proper classification marking to be placed on mock or "notional" classified exercise documents:

SECRET
"CLASSIFIED FOR TRAINING ONLY"

(3) Exercise information classified "CLASSIFIED FOR TRAINING ONLY" will be protected in the same manner as real-world classified information at that level, and will be destroyed as classified waste at the end of the exercise, in accordance with AR 380-5 and this supplement.

(4) If real-world classified information is introduced or used in military exercises, it will not be intermingled or stored with other mock classified exercise documents.

Chapter 1, Paragraph 1-19. Add the following paragraphs:

e. Requests for waivers to requirements contained in this regulation and requests for delegation of approval authority will be forwarded through command channels to the FORSCOM G-2. Requests will be fully justified and contain all required information specified in Paragraph 1-19c, AR 380-5.

f. Waiver and delegation approvals will not be considered official unless documented in writing and signed by the appropriate approval authority. Copies of approvals will be maintained by the FORSCOM G-2 and the requesting command, unit, or activity, and will be reviewed periodically to ensure that approved alternative or compensatory procedures continue to be effective and do not lessen regulatory security standards.

Chapter 1, Paragraph 1-22. Add the following sentence:

Forward all incident reports through command channels to the FORSCOM G-2.

Chapter 1, Paragraph 1-23. Add the following sentences:

Completed annual reports (SF 311) will be forwarded to the FORSCOM G-2 by 1 September of each year. Annual reports will contain consolidated information for the previous fiscal year. However, FORSCOM commands, units, and activities are required to locally capture and record required information by fiscal quarter. Quarterly reports will be maintained on file and available for audit purposes.

Chapter 1, Paragraph 1-24. Add the following paragraphs:

a. Security inspections will be conducted for all subordinate units and activities that handle, process, and/or store classified material. Inspections will be conducted annually, when adequate resources are available; otherwise, inspections will be conducted at least every two years. These inspections may be announced or unannounced. Inspections will include all applicable security areas identified in Annex F, Section F-3, AR 380-5, and any other security areas deemed appropriate by the Commander or DUSM. Inspection reports will be prepared for each completed security inspection, and will follow the general format provided at APPENDIX J, this supplement. A copy of each inspection report will be maintained on file by the inspecting agency and will be available for review

during FORSCOM staff visits. When security inspections are conducted as part of the Command Inspector General (IG) Inspection Program, completed IG inspection reports are acceptable, provided the security inspection includes all appropriate information identified above.

b. Unannounced after duty hour security inspections and spot checks will be conducted periodically by DUSMs or subordinate unit/activity security managers to ensure compliance with security directives. A written record of these inspections and spot checks will be maintained on file by the inspection agency, and will be available for review during FORSCOM staff visits. Records will include, at a minimum, the date of the inspection or spot check; specific areas and/or personnel involved; observations/findings identified; and, if necessary, corrective actions taken. A sample checklist is provided at APPENDIX K, this supplement.

c. A copy of all security inspection reports will be provided to the Installation Management Agency (IMA) Garrison Security Manager for the host installation.

Chapter 2, Paragraph 2-3a. Add the following subparagraphs:

(1) A list of current FORSCOM Delegated Original Classification Authorities (OCA) is maintained by the FORSCOM G-2. This list is updated each October, in conjunction with the annual SF 311 report. Updated listings will be provided to commands, units, and activities, as requested. Requests for changes or deletions to this list will be submitted to the FORSCOM G-2.

(2) Requests for additional delegated OCAs will be submitted to the FORSCOM G-2. Requests will include the position title of the OCA nominee, the level of OCA requested, and a detailed justification addressing all requirements specified in Paragraphs 2-3b and 2-3c, AR 380-5.

Chapter 2, Paragraph 2-4. Add the following sentence:

Individuals assigned to positions which are authorized to officially assume the position of the delegated OCA, in his/her absence, will also receive this training before exercising such authority.

Chapter 2, Paragraph 2-5. Add the following sentence and paragraphs:

Documents that are classified based on compilation of information will contain a statement or paragraph that includes, at a minimum, the following information:

a. The specific authority that classifies the document or raises the existing classification to a higher level, based on compilation of information.

b. The specific portions of the document which constitute the compilation and resulting level of classification.

c. Appropriate declassification instructions.

Chapter 2, Paragraph 2-6d. Add the following sentences:

When extracting information from classified documents without internal markings, the original classifier will be contacted to determine the proper classification of the extracted information. In time sensitive situations, the extracted information will be classified at the same level as the overall source document classification, until specific classification guidance is received from the original classifier. Upon receipt of guidance from the original classifier, all copies of documents containing the extracted information will be re-marked with the appropriate classifications, as required.

Chapter 2, Paragraph 2-6f. Add the following sentence:

When information is derivatively classified by “Multiple Sources,” a listing of sources will be included with all copies of the document, when feasible.

Chapter 2, Paragraph 2-16. Add the following sentences:

Proponents and activities involved in the planning and conduct of classified exercises will also ensure that adequate classification guidance is provided to all exercise participants, and prepared in accordance with this chapter and APPENDIX G, AR 380-5. Classification guidance may be published as separate documents or incorporated in exercise plans or directives.

Chapter 2, Paragraph 2-18. Add the following paragraphs:

e. In addition to the above distribution requirements, a copy of each security classification guide will also be provided to the FORSCOM G-2.

f. If an originator elects not to include a security classification guide in DoD 5200.1-I, a memorandum providing a full explanation and justification for this decision, will be forwarded through the FORSCOM G-2 to HQDA (DAMI-CD), Suite 9300, 2511 Jefferson Davis Hwy, Arlington VA 22202-3910.

Chapter 2, Paragraph 2-19. Add the following paragraph:

e. Original classifiers will notify the FORSCOM G-2 when required security classification guide reviews have been conducted. A copy of revised, re-issued, or cancelled classification guides will be provided to the FORSCOM G-2 in addition to those agencies identified in Paragraph 2-18, AR 380-5.

Chapter 2, Paragraph 2-22. Add the following paragraphs:

d. Original classifiers will establish local procedures for challenging classification decisions and submitting appeals to higher agencies. These procedures will be disseminated to all authorized holders of classified information. Original classifiers will also maintain records of all formal classification challenges, which will be available for review during FORSCOM staff visits.

e. Every effort will be made to informally resolve classification challenges, when possible. All challenges, whether informal or formal, will be promptly responded to by the original classifier, in accordance with the above procedures and timelines.

f. Classification challenges or conflicts that cannot be resolved by the original classifier will be forwarded to the FORSCOM G-2 for further review and assistance.

g. The FORSCOM G-2 will be provided a copy of all classification challenges submitted to original classification authorities of other agencies.

Chapter 3, Paragraph 3-1. Add the following sentences:

Within FORSCOM, requests for declassification or downgrading of classified files and records will be submitted to the respective OCA, for review and determination. If the OCA cannot be determined, submit the request for declassification/downgrading to the FORSCOM G-2 for further review and assistance.

Chapter 3, Paragraph 3-2. Add the following paragraphs:

d. The DUSM will establish local procedures to ensure that all classified information is reviewed for declassification or exemption determination, prior to the date for automatic declassification. Annual statistical results of declassification reviews will be provided to the FORSCOM G-2 as specified in Paragraph 1-23, AR 380-5, and this supplement.

e. Declassification review procedures will be evaluated during required security inspections, as specified in Paragraph 1-24, AR 380-5, and this supplement.

Chapter 3, Paragraph 3-3. Add the following sentence:

Classified files or records which are marked Restricted Data (RD) or Formerly Restricted Data (FRD), or are believed to contain RD or FRD information, will be submitted through the FORSCOM G-2 to the Department of Energy, for declassification review and determination.

Chapter 3, Paragraph 3-5. Add the following paragraph:

c. Classified files and records that are more than 25 years old will not be automatically declassified without prior review to determine if continued classification is warranted or authorized.

Chapter 3, Paragraph 3-8. Add the following paragraph:

c. Requests for mandatory reviews will be treated in the same manner as classification challenges. Original classifiers will establish procedures similar to those specified in Paragraph 2-22, AR 380-5, and this supplement, for resolving and reporting mandatory review requests.

Chapter 3, Paragraph 3-9. Add the following paragraph:

c. The DUSM will establish local procedures to ensure that periodic reviews are conducted for classified documents which have been exempted from the 25-year automatic declassification requirement, to determine continued need for classification. Annual statistical results of these declassification reviews will be provided to the FORSCOM G-2 as specified in Paragraph 1-23, AR 380-5, and this supplement.

Chapter 3, Paragraph 3-12. Add the following sentence:

Before a decision to upgrade classified information is made, OCAs must ensure that all holders of the classified information can be properly notified.

Chapter 3, Paragraph 3-14. Add the following paragraphs:

c. The DUSM will establish local procedures to ensure that the “secure volume” concept is employed when utilizing office-type approved security shredders.

d. The DUSM will establish local procedures to ensure that appropriately sized security screens are utilized for the destruction of high data density material, to preclude recognition or reconstruction of the classified material.

Chapter 4, Paragraph 4-4. Add the following sentences:

Classified documents that have no back cover will be conspicuously marked or stamped with the overall classification of the document at the top and bottom on the back of the last page, as an additional security measure to clearly alert holders of the overall classification of the document. Classification markings, warning notices, control markings, and classification/declassification instructions, will be marked or stamped by hand to ensure legibility when not clearly visible on reproduced copies.

Chapter 4, Paragraph 4-6b. Add the following sentence to the end of paragraph 4-6b, before subparagraphs:

All subparagraphs will be marked in the same manner as paragraphs, to eliminate any doubt about the classification of their contents.

Chapter 4, Paragraph 4-6d(3). Add the following sentence:

Requests for waivers or exceptions to policy will be submitted through the FORSCOM G-2.

Chapter 4, Paragraph 4-8b(2). Add the following sentence:

As previously stated in Paragraph 2-6f, this supplement, all copies of documents that are derivatively classified by "Multiple Sources," will include a listing of sources, when feasible.

Chapter 4, Paragraph 4-21. Add the following sentence:

Procedures for marking mock or "notional" classified information during military exercises are provided in Chapter 1-18b, this supplement.

Chapter 4, Paragraph 4-22. Add the following sentence and subparagraphs:

Cover sheets may remain attached to documents stored in security containers, under the following circumstances:

a. When the document is placed in a temporary suspense file.

b. When the document or file is being used daily and is kept in a hold box or folder, which is placed in the container overnight or during the day when not needed.

c. When permanently affixed to the outside front and back of a hard cover binder or other container, when classification markings cannot be adequately or legibly stamped otherwise. When possible, binders containing classified documents will be conspicuously marked on the front and back covers and on the spine, to indicate the highest level of classified information contained within.

Chapter 4, Paragraph 4-23. Add the following paragraph:

d. Classified products produced on an Automated Information System (AIS) will be reviewed to ensure that they contain the proper classification markings and instructions, before they are electronically transmitted or printed.

Chapter 4, Paragraph 4-28. Add the following paragraph:

c. When classified slides or transparencies are used together in a set, classification/declassification instructions will be placed on the first slide or transparency. Any classified slide or transparency removed and handled apart from the set, will be annotated with the appropriate classification/declassification instructions.

Chapter 5, Paragraph 5-3b. Add the following subparagraphs:

(5) FOUO documents or materials released to agencies outside the Department of Defense (DoD) will contain the following additional expanded marking on the front cover or first page:

"This document/material contains information exempt from mandatory disclosure to the public under the Freedom of Information Act. Exemption (indicate exemption(s) specified in AR 25-55, The Department of the Army Freedom of Information Act Program) applies."

(6) FOUO documents or materials, as well as all other Controlled Unclassified Information (CUI), require the consent of the originator or proponent before disclosing to foreign governments or representatives, IAW AR 380-10, Foreign Disclosure, Technology Transfer, and Contacts with Foreign Representatives.

Chapter 5. Add the following section:

Section VI
Law Enforcement Agency Sensitive Information

5-25. Description.

Law Enforcement Agency (LEA) sensitive information is unclassified information which is originated by various local, state, and federal law enforcement agencies and requires protection against unauthorized disclosure in order to protect sources and methods of criminal activities, investigations, and evidence.

5-26. Marking.

a. Unclassified documents or materials containing LEA sensitive information will be marked "LEA SENSITIVE," in letters larger than the rest of the text, where practical, at the top and bottom of the front cover (if there is one), the title page (if there is one), the outside of the back cover (if there is one), and on each page containing LEA sensitive information.

b. Classified documents containing LEA sensitive information will be marked as required in Chapter 4, AR 380-5, except that pages containing LEA sensitive information, but no classified information, will be marked "LEA SENSITIVE" top and bottom.

5-27. Access to LEA Sensitive Information.

Access to LEA sensitive information will be granted only to persons who have a valid need-to-know for the information. A security clearance is not required. LEA sensitive information will not be released outside the DoD, without prior authorization by the originating LEA.

5-28. Protection of LEA Sensitive Information.

a. To the maximum extent possible, LEA sensitive information will be transmitted via secure means, stored in a locked container, disseminated only when the need-to-know of the recipient has been established, and shredded when no longer required. However, LEA sensitive information may be processed on unclassified computers and local area networks. Data will not be stored on a system accessible via the Internet that does not have approved firewall protection. In the absence of secure transmission capabilities, the information may be transmitted over unsecure facsimile machines.

b. When mailing, LEA sensitive information will be double wrapped and sent via first-class mail, with no requirement for certified or registered mail.

c. LEA sensitive information may be stored in a locked container, with no requirement to use General Services Administration (GSA)-approved security containers.

d. Reproduction of LEA sensitive information will be kept to a minimum, and limited to operational requirements.

e. When no longer needed, LEA sensitive information will be destroyed by shredding.

Chapter 6, Paragraph 6-5c. Add the following sentence and subparagraphs:

All cleared military and civilian personnel transferring to another DA command or federal government agency will formally out-process through the command, unit, or activity security office. Out-processing will minimally include the following:

(1) A briefing regarding the individual's continued responsibility to protect classified information.

(2) Verification that all classified and other accountable material possessed by the individual has been properly accounted for and/or transferred to new custody, and that all classified combinations and passwords previously issued to the individual have been changed.

Chapter 6, Paragraph 6-8. Add the following paragraph:

g. Designated FORSCOM OCAs are authorized to make release determinations, with the exception of those situations described in paragraph 6-8d and f, AR 380-5, which will be forwarded to the FORSCOM G-2 for final determination.

Chapter 6, Paragraph 6-10. Add the following subparagraphs:

f. The name and telephone number of the DUSM or subordinate unit and activity security manager will be conspicuously posted within each separate unit, activity, and staff agency, utilizing FORSCOM Form 102-R, Security Manager Poster.

Chapter 6, Paragraph 6-10b. Add the following subparagraphs:

(6) All notations on the SF 702, Security Container Check Sheet, will be recorded in nonerasable ink.

(7) The proper method for ensuring that a security container is locked, is to rotate the combination dial in a counter-clockwise direction at least four times, and with the control drawer handle held in a depressed position, attempt to open each drawer of the container.

(8) No entry is required on the SF 702 on non-work days, unless the security equipment is under 24-hour surveillance or requires periodic security checks.

Chapter 6, Paragraph 6-10d(1). Add the following sentence:

Leave the container unlocked.

Chapter 6, Paragraph 6-11a. Add the following subparagraphs:

(1) Specific individuals will be designated by name to conduct end-of-day security checks.

(2) End-of-day security checks will also include the checking of all classified magnetic media and electronic processing devices (e.g. electronic memory typewriters, facsimile machines, printers) which process classified information, to ensure that classified information has been cleared, removed, destroyed, or properly stored in an approved security container.

Chapter 6, Paragraph 6-12. Add the following paragraphs:

a. Emergency plans for the protection, removal, and destruction of classified material will be conspicuously posted near each security container.

b. All personnel will be familiar with posted emergency plans and procedures.

Chapter 6, Paragraph 6-13b. Add the following subparagraphs:

(1) The FORSCOM DCS, G-6 (AFCI-J), 1777 Hardee Avenue SW, Fort McPherson, GA 30330-1062, is the MACOM proponent for issuing policy regarding the installation and operation of secure telephone units in personal residences. Approved users of secure telephone units in personal residences must fully comply with the procedures specified in Paragraph 6-13b, AR 380-5, Department of the Army Information Security Program.

(2) Classified document storage of SECRET and CONFIDENTIAL material in personal residences, either on or off a military installation, requires the approval of the FORSCOM G-2. Requests will be submitted through

command channels to the FORSCOM G-2. Requests will be fully justified and contain assurances that all requirements of Paragraphs 6-13 and 7-6, AR 380-5, have been met. The FORSCOM G-2 approval process and procedural requirements for the storage of classified information in personal residences are exclusive of, and in addition to, FORSCOM G-6 requirements for the approval and use of secure telephone units.

Chapter 6, Paragraph 6-14e. Add the following sentence:

A copy of the incident report will also be provided to the FORSCOM G-2.

Chapter 6, Paragraph 6-15. Add the following sentence:

Furniture items (e.g. desks, cabinets, etc.) used in protected areas where classified information is routinely accessed or stored, will also be inspected to ensure that the items are free of classified information, before removal from the protected area.

Chapter 6, Paragraph 6-16. Add the following paragraphs:

d. Visitors to FORSCOM commands, units, and activities will not be granted access to classified information until the individual's security clearance level and need-to-know have been verified.

e. It is the responsibility of the visitor's assigned command, unit, or activity to provide advance notice to the visited activity of anticipated visits which require access to classified information. This advance notice will be in the form of a visit request, and will include all required information specified in Paragraph 6-16b, AR 380-5. Visit requests will be authenticated and signed by the DUSM or subordinate unit/activity security manager, as determined by the commander or DUSM.

Chapter 6, Paragraph 6-18a(1). Add the following subparagraphs:

(a) Whenever possible, in-house classified meetings will be held in designated secure areas or facilities. When such an area or facility is not available or feasible, and the classified meeting must be held in an uncleared facility (e.g. host installation theater, training classroom, etc), the following minimum security measures will be taken:

(i) The commander or DUSM sponsoring the classified meeting will approve in writing the use of the uncleared facility.

(ii) Before the classified meeting is held, the facility will be visually inspected to ensure that it poses no unacceptable vulnerabilities or risks which may prevent the proper control of physical, auditory, and visual access to the classified information. Once inspected, the facility will be properly secured to prevent unauthorized access until the classified meeting is held.

(iii) Continuous physical and access control will be provided during the conduct of the classified meeting, to ensure that access to the classified information is limited to properly cleared and authorized persons, and that classified discussions cannot be heard outside the facility.

(iv) The overall classification level of oral discussions and visual presentations will be clearly announced before the information is discussed or presented.

(v) Upon completion of the classified meeting, the facility will be thoroughly inspected to ensure that all classified documents, recordings, audiovisual material, notes, and other materials from the classified meeting have been properly accounted for, marked, controlled, and removed from the facility.

Chapter 6, Paragraph 6-18d. Add the following paragraphs:

e. Requests to sponsor association-related classified meetings will be forwarded to the FORSCOM G-2 in sufficient time to be reviewed and forwarded to HQDA (DAMI-CD) Suite 9300, 2511 Jefferson Davis Hwy, Arlington VA 22202-3910 at least 120 days prior to the planned date of the meeting. Requests will include a detailed security plan, which sufficiently addresses all requirements specified in Paragraph 6-18, AR 380-5.

f. Approved association-related classified meetings will be held in designated secure areas or facilities, whenever possible. When an association-related classified meeting is held in an uncleared area or facility, the security measures specified in Paragraph 6-18a(1), this supplement, will also be taken in addition to those requirements specified in AR 380-5.

Chapter 6, Paragraph 6-19. Add the following sentence and subparagraphs:

Security procedures will be established to clearly identify all equipment used to process classified information, to include:

a. Overall level of classified information processed.

b. Temporary or permanent retention capabilities.

c. Procedures for properly safeguarding and storing the equipment while classified information is processed and retained in the equipment.

d. Procedures for sanitizing or removing classified information from the equipment with temporary retention capabilities.

Chapter 6, Paragraph 6-20. Add the following sentences and paragraphs:

All official mail, to include Official First Class Mail, as defined in the DoD Postal Manual, has the potential for containing classified information. Therefore, procedures will be established to ensure the adequate physical protection of official mail, until a determination can be made as to whether the mail contains classified information. The following additional guidance is provided:

a. Physical security requirements apply only to official mail that is addressed to official government activities, and not individuals.

b. In areas where the quantity of official mail is so large that it makes it impractical to protect all official mail in approved security containers or storage areas, commanders or DUSMs may, from a risk management perspective, determine that existing physical and postal security provisions already in place provide adequate and compensatory protection. Compensatory provisions will be clearly documented and approved in writing.

Chapter 6, Paragraph 6-21a. Add the following subparagraphs:

(1) TOP SECRET Control Officers (TSCOs) and alternate TSCOs must possess a final TOP SECRET security clearance. A TSCO will be officially appointed in writing within each unit or activity that handles TOP SECRET material. A sufficient number of Alternate TSCOs will be appointed to carry out the duties specified in paragraph 6-21, AR 380-5, and this supplement.

(2) Waivers to minimum rank/grade requirements established in paragraph 6-21a, AR 380-5, will be considered on a case-by-case basis, and must meet the requirements specified in paragraphs 6-30 through 6-33, AR 380-5. Requests for waivers will be submitted to the FORSCOM G-2.

(3) TOP SECRET material will not be copied, transferred, destroyed, downgraded, or declassified, without the approval of the designated unit/activity TSCO or alternate TSCO.

Chapter 6, Paragraph 6-21b. Add the following sentence:

TOP SECRET accountability registers, records, and receipt forms will also include the total number of pages in the document marked TOP SECRET.

Chapter 6, Paragraph 6-21c. Add the following sentence:

An annual inventory of 100 percent of TOP SECRET material on hand will be completed no later than 31 December of each year. This annual requirement may also be met by conducting monthly inventories of 10 percent of TOP SECRET material on hand, as long as a 100 percent reconciliation is accomplished by 31 December. Methods and results of inventories will be documented and retained on file, and available for review during FORSCOM staff visits.

Chapter 6, Paragraph 6-21d. Add the following sentences:

Units or activities that store exceptionally large volumes of TOP SECRET material may be authorized, as an exception, to perform limited inventories as specified in Chapter 6-21d, AR 380-5. Requests for limited inventory authorization, with detailed justification, will be submitted to the FORSCOM G-2.

Chapter 6, Paragraph 6-21f. Add the following sentence:

A TOP SECRET disclosure record (e.g. DA Form 969, TOP SECRET Document Record) is required within FORSCOM to record the identity of individuals to whom TOP SECRET information has been disclosed.

Chapter 6, Paragraph 6-22. Add the following paragraphs:

a. FORSCOM commands, units, and activities will use DA Form 3964, Classified Document Accountability Record, to verify receipt of SECRET material sent by mail outside the unit/activity. A copy of the DA Form 3964 will be maintained in a suspense file until the original form is signed and returned by the recipient. The DA Form 3964 will also be used to verify receipt of CONFIDENTIAL material sent by mail to cleared contractor facilities.

b. Within FORSCOM, continuous control and accountability of SECRET and CONFIDENTIAL information is prohibited, unless required by AR 380-5, other DA regulations or directives, or specifically requested by the originator. SECRET or CONFIDENTIAL information requiring continuous control and accountability will be treated in the same manner as TOP SECRET, with the exception of the use of disclosure records (e.g. DA Form 969). This includes controls such as accountability control records, continuous receipting, annual inventories, and certificates of destruction. FORSCOM commands, units, and activities desiring to provide continuous control and accountability for any SECRET document not required by regulation, directive, or originator, will submit a request, with detailed justification, to the FORSCOM G-2.

Chapter 6, Paragraph 6-24a. Add the following subparagraph:

(7) Within FORSCOM, all required markings will be in non-erasable ink.

Chapter 6, Paragraph 6-24b. Add the following subparagraph:

(4) Requests for exceptions for accountability, control, and marking requirements for working papers containing TOP SECRET information will be submitted, with detailed justification, to the FORSCOM G-2.

Chapter 6, Paragraph 6-25c. Add the following subparagraphs:

(1) FORSCOM Form 138-R, Equipment Designated for Reproduction of Classified Material, will be completed and conspicuously placed on or near each item of equipment authorized for reproduction of classified information.

(2) FORSCOM Poster 93-R, Warning Notice, will be conspicuously placed on or near each item of equipment prohibited from the reproduction of classified information.

Chapter 6, Paragraph 6-29b. Add the following sentences:

Records of destruction are also required for SECRET and CONFIDENTIAL material requiring continuous control and accountability. With the exception of NATO or foreign government SECRET material, only one signature is required on the record of destruction.

Chapter 6, Paragraph 6-30. Add the following sentences:

Requests for waivers will be submitted to the FORSCOM G-2. Waiver requests will sufficiently address all requirements specified in Chapter 6, AR 380-5, and this supplement.

Chapter 7, Paragraph 7-5a. Add the following sentence:

Requests for exceptions will be submitted to the FORSCOM G-2.

Chapter 7, Paragraph 7-6. Add the following paragraph:

d. As previously stated in Paragraph 6-13b, this supplement, the following additional provisions apply:

(1) The FORSCOM G-6 (AFCI-J) is the MACOM proponent for issuing policy regarding the installation and operation of secure telephone units in personal residences.

(2) Classified document storage of SECRET and CONFIDENTIAL material in personal residences, either on or off a military installation, requires the approval of the FORSCOM G-2. Requests will be submitted through command channels to the FORSCOM G-2. Requests will be fully justified and contain assurances that all requirements of Paragraphs 6-13 and 7-6, AR 380-5, have been met.

Chapter 7, Paragraph 7-8. Add the following paragraphs:

g. No two security containers located within the same unit, activity, or office area will have the same combination.

h. Memory/convenience keys, such as birthdays, telephone numbers, street addresses, or social security numbers, will not be used as combinations.

i. Units or activities which have more than one security container will designate a master container to store combinations to the other containers. The combination to the master container will be sent to the next higher headquarters; however, the combination will not normally be sent off the host installation. For this purpose, a United States Army Reserve (USAR) Center Facility is considered an installation.

j. New combinations will be tested at least three times before locking the container.

k. All entries on SF 700 will be typed or written in nonerasable ink.

l. A combination (SF 700, Part 2A) subject to investigation due to compromise or possible compromise will not be destroyed until it is no longer needed as evidence.

Chapter 7, Paragraph 7-9. Add the following paragraph:

e. Additional technical assistance may be obtained by contacting the DoD Lock Program Technical Support Hotline, at DSN 551-1212 or (800) 290-7607.

Chapter 7, Paragraph 7-11. Add the following paragraphs:

a. The container will be clearly marked to indicate that no classified material will be stored in the container without the approval of the DUSM or subordinate unit or activity security manager. In addition, a copy of the inspection certification will be placed on the outside front of the container.

b. An SF 700 is not required when the combination to the container is reset to the standard combination 50-25-50.

Chapter 7, Paragraph 7-12. Add the following paragraphs:

a. Within FORSCOM, open storage of classified information will be kept to a minimum, and only approved when necessary for mission accomplishment or when the volume or size of the classified information prohibits storage in GSA-approved security containers. Requests for open storage areas will be fully justified, and will include proposed systems, controls, or procedures to properly protect the classified information and sufficiently deter, detect, delay, or deny unauthorized penetration into the secure area.

b. Authority to approve open storage areas within FORSCOM is delegated to the DUSM. Approvals will be in writing, and will be granted only after the open storage area has been formally inspected and certified to meet the requirements and standards specified in Chapter 7, AR 380-5, and this supplement. Approval documents will include the following information:

(1) The physical location of the open storage area (i.e. Room, Building, Host Installation, Geographic Community, etc).

(2) A description of the physical composition and characteristics of the open storage area (i.e. Floor, Walls, Roof, Ceiling, Doors, Windows, Openings, IDS, AECS, CCTV, etc).

(3) Highest classification level and type of information for which open storage is authorized.

(4) A graphic floor plan of the open storage area.

(5) Certification by qualified physical security or information security specialists that the physical composition of the facility meets the construction standards specified in paragraphs 7-13 and 7-20, AR 380-5.

(6) Certification by qualified physical security or information security specialists that the IDS system (if applicable), access control procedures, and other supplementary controls, meet the standards specified in paragraphs 7-4, and 7-14 through 7-19, AR 380-5.

c. A copy of the approval documentation will be maintained on file within the open storage area. A copy will also be maintained on file by the DUSM and available for review during FORSCOM staff visits. A copy of approvals for TOP SECRET open storage areas will be provided to the FORSCOM G-2.

d. Open storage approvals are valid for up to five years, at the direction of the DUSM. Approvals may be renewed; however, they must be re-inspected and re-certified, as specified above. Open storage of classified information will be terminated immediately when structural modifications that degrade security are made.

e. Existing approved open storage areas based on previous standards in place before the effective date of this supplement may continue to be authorized for open storage for the current approval period, provided they have not been structurally modified. Approval renewals may be authorized only after meeting the requirements and standards of Chapter 7, AR 380-5, and this supplement.

Chapter 7, Paragraph 7-13. Add the following paragraphs:

c. Whenever possible, newly constructed open storage areas will meet the more stringent construction standards of a vault, to provide the classified information the maximum level of protection.

d. The open storage standards and requirements identified in Chapter 7, AR 380-5, and this supplement are only minimum standards, and whenever possible, should be augmented with other supplementary controls to provide maximum security of the classified information.

(1) When classified information is openly displayed in secure areas (i.e. maps, charts, etc.), it will be covered when not in use to prevent observation through windows, doors, and other openings, or by visitors in the secure area who do not have a need-to-know for the information.

(2) Sound attenuation or other security measures will be employed, if classified discussions occur that can be heard outside the secure area by unauthorized individuals.

Chapter 7, Paragraph 7-20. Add the following paragraphs:

f. Requests for deviations to construction standards for open storage areas will be fully justified, and will include proposed compensatory systems, controls, or procedures to properly protect the classified information and sufficiently deter, detect, delay, or deny unauthorized penetration into the secure area. The DUSM is authorized to approve deviations to the construction standards for open storage areas.

(1) Approvals for deviations to construction standards will be in writing, and will be granted only after the open storage area has been inspected and certified that it meets the minimum requirements and standards specified in paragraph 7-20, AR 380-5.

(2) A copy of the deviation approval documentation will be maintained on file within the open storage area. A copy will also be maintained on file by the DUSM and available for review during FORSCOM staff visits. A copy of deviation approvals for TOP SECRET open storage areas will be provided to the FORSCOM G-2.

Chapter 8, Paragraph 8-1. Add the following sentences:

Procedures will be established to ensure the adequate physical protection of incoming official mail until a determination can be made as to whether the mail contains classified information. Additional guidance is provided in Paragraph 6-20, this supplement.

Chapter 8, Paragraph 8-6. Add the following sentence:

Release of classified information to foreign government representatives will be fully coordinated in advance with the FORSCOM G-2 Foreign Disclosure Office (AFIN-SD), 1777 Hardee Avenue SW, Fort McPherson, GA 30330-1062.

Chapter 8, Paragraph 8-9. Add the following paragraph:

c. When hand carrying classified information, the recipient's security clearance and need-to-know will be verified before releasing the classified information to the individual. The recipient will also be advised of the classification level of the information being delivered.

Chapter 8, Paragraph 8-9a. Add the following subparagraphs:

(7) Classified information is not required to be double-wrapped when hand carried between buildings on a military installation or government facility. In these situations, a cover sheet will be attached, and the information will be concealed in an opaque, unmarked container, such as an envelope or briefcase.

(8) A briefcase may serve as the outer wrapper for classified information hand carried outside the military installation or government facility, to activities within the local surrounding area. In these situations, the inner wrapper will be properly wrapped, sealed, and marked as specified in paragraphs 8-9 and 8-10, AR 380-5. A briefcase may not be used as the outer wrapper for classified information hand carried outside the local surrounding area or aboard commercial aircraft.

Chapter 8, Paragraph 8-12a(3). Add the following sentence:

Authority to approve the escort and hand carry of collateral classified information aboard commercial aircraft and to locations outside the US, its territories and Canada, is delegated to the DUSM, subject to the provisions of Chapter 8, AR 380-5, and this supplement.

Chapter 8, Paragraph 8-13. Add the following paragraphs:

c. Written courier authorization is required when hand carrying classified information between buildings on a military installation or government facility, and to activities within the local surrounding area. DD Form 2501, Courier Authorization Card, may be used for this purpose when there is a recurrent need to locally hand carry classified information. The following additional provisions apply:

(1) Recurrent courier authorizations will only be issued to individuals with a demonstrated need to frequently handcar classified information on the military or government installation, and the local surrounding area. Local courier authorizations will not be issued as blanket authorization to randomly hand carry classified information.

(2) Recurrent courier authorizations will include specific geographical parameters, locations, and/or a maximum mileage radius allowed for locally hand carrying classified information. The mileage radius will be determined by the proximity of specific activities within the local surrounding area, for which the individual is authorized to hand carry classified information. Mileage radiuses will not exceed distances that would prevent the courier from traveling to the destination and returning to the departure point, within a normal duty day's time by ground vehicle.

(3) Recurrent courier authorizations are valid for no more than two years. Authorizations may be kept by the individual during the entire period of authorization or returned after each use. Individuals are required to possess the courier authorization when hand carrying classified information, and will immediately return the authorization to the issuing authority when no longer needed. Records of issued courier authorizations will be controlled and maintained on file by the issuing authority, and available for review during FORSCOM staff visits.

(4) The issuing authority or other official within the courier's chain of command will be knowledgeable of each instance when classified information is being hand carried, to include the description of the classified material, reason, destination, and anticipated time and date.

d. Individuals authorized to hand carry classified information 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 provided in Chapter 8, AR 380-5, and this supplement. Certifications will be maintained on file by the issuing authority. For local recurrent courier authorizations, individual couriers may be briefed at annual intervals. A sample courier briefing and certification are provided at APPENDIX L, this supplement.

Chapter 8, Paragraph 8-14. Add the following paragraphs:

g. Hand carry of classified information to OCONUS locations will be conducted only when no other acceptable method is available. More secure means will be used whenever possible. The following additional provisions apply:

(1) Requests will be evaluated and approved on a case by case basis.

(2) The designated courier will be issued a written courier authorization for each courier mission. Courier authorizations will contain all required information specified in Paragraph 8-15, AR 380-5. A copy of each courier authorization will be maintained on file by the issuing agency and will be available for review during FORSCOM staff visits. Courier authorizations will contain an expiration date not to exceed 7 days from the date of issue, or in the event of a round trip authorization, 7 days from the scheduled date of return. A sample courier authorization is provided at APPENDIX M, this supplement.

(3) Prior to execution of any courier mission to OCONUS locations, authorized couriers will be briefed concerning their duties and responsibilities. Individuals will certify in writing that they have received this briefing and fully understand their responsibilities, and the provisions provided in Chapter 8, AR 380-5, and this supplement. Certifications will be maintained on file by the issuing authority. Individuals who frequently conduct courier missions OCONUS may be briefed at annual intervals. A sample courier briefing and certification are provided at APPENDIX L, this supplement.

(4) Classified information which requires additional controls or handling procedures (i.e. NATO, COMSEC, etc.) will be hand carried in accordance with applicable governing regulations.

h. Requests to hand carry classified information for foreign disclosure will be coordinated in advance with the FORSCOM G-2, Foreign Disclosure Office (AFIN-SD). Foreign disclosure provisions specified in Chapters 8-6 and 8-7, AR 380-5, and this supplement, will be fully met before releasing classified information to a foreign government.

Chapter 8, Paragraph 8-15. Add the following paragraphs:

c. The provisions of paragraph 8-14, AR 380-5, and this supplement, also apply to the hand carrying of classified information aboard commercial aircraft.

d. A sample courier authorization is provided at APPENDIX M, this supplement.

Chapter 9, Paragraph 9-2. Add the following sentence:

APPENDIX N, this supplement, provides a suggested list of topics to be considered for the various security education briefings required in Chapter 9, AR 380-5. Specific topics to be selected and level of instructional detail should be based on the individual's clearance status, experience, and specific role or involvement in the information security program. FORSCOM recommends local coordination with the IMA Garrison Security Office for security education training assistance and materials.

Chapter 9, Paragraph 9-3. Add the following sentence to the end of paragraph 9-3, before subparagraphs:

Initial orientations for newly assigned personnel will be conducted within 60 days of arrival date.

Chapter 9, Paragraph 9-8. Add the following paragraph:

e. Force Protection Security Analysts (FPSA) should be contacted to provide specific OCONUS AOR threat briefings in conjunction with the Level I Antiterrorism Awareness Training requirement for individuals and units traveling to overseas areas.

Chapter 9, Paragraph 9-15. Add the following sentences after the second sentence of paragraph 9-15:

Termination briefings are required for individuals who are retiring, resigning, being discharged, or will no longer have access to classified information. Additional guidance is provided in paragraph 6-5 of this supplement.

Chapter 9, Paragraph 9-16. Add the following sentences:

Local procedures will be established to ensure that effective initial and refresher training requirements are accomplished, as specified in Chapter 9, AR 380-5. Records of training will be maintained on file and available for review during FORSCOM staff visits. Records will also include the training methods and products used.

Chapter 10, Paragraph 10-1d. Add the following sentence:

Forward all incident reports involving the loss or compromise of foreign government information through the FORSCOM G-2 to HQDA (DAMI-CD), Suite 9300, 2511 Jefferson Davis Hwy, Arlington VA 22202-3910.

Chapter 10, Paragraph 10-3. Add the following paragraphs:

g. The DUSM is responsible for ensuring preliminary inquiries are promptly and properly completed, that results are reported to the proper authorities, and that corrective actions are implemented.

h. The commander or chief of the unit/activity in which the suspected compromise has occurred, is responsible for appointing in writing an individual to conduct the preliminary inquiry. The appointee will be a disinterested individual who is senior to everyone known to be involved in the incident. A sample appointment memorandum is provided at APPENDIX O, this supplement. A copy of the appointment memorandum will be provided to the DUSM.

i. Preliminary inquiries will be conducted in accordance with the guidelines specified in Paragraph 10-3, AR 380-5, and this supplement, and will be prepared in the format provided at Figure 10-1, AR 380-5. The DUSM will provide advice and assistance, as needed.

j. Preliminary inquiries will be unclassified whenever possible. However, if classification is absolutely necessary, they will be classified to the highest degree of the classified information contained therein, and will contain appropriate classification authority and declassification instructions. Classified preliminary inquiries will be appropriately safeguarded, stored, and controlled.

k. Preliminary inquiries will be completed and submitted to the appointing authority within 20 working days from the date of discovery of actual or possible compromise. The DUSM may grant an extension to this deadline, based on extenuating circumstances.

l. The appointing authority will forward the completed preliminary inquiry through command channels, via memorandum, to the DUSM within 3 working days of receipt. The memorandum will include the appointing authority's concurrence or non-concurrence with the findings and recommendations of the inquiry; proposed corrective actions; and determination of whether additional investigation (i.e. AR 15-6) is warranted. A sample memorandum is provided at APPENDIX P, this supplement.

Chapter 10, Paragraph 10-4. Add the following paragraphs:

f. The DUSM will review the results of the completed preliminary inquiry report to determine if the findings, recommendations, and corrective actions are sufficient to resolve and close the issue, or if further actions are warranted, as specified in Paragraph 10-4, AR 380-5, and below supplemental guidance.

(1) When the results of the preliminary inquiry determine that compromise did not occur, or that damage to national security has not resulted from the compromise, the preliminary inquiry will be returned to the appointing authority for filing and recommended corrective actions. Corrective actions will be monitored through periodic reviews or inspections. Preliminary inquiry reports and follow-up reviews/inspections will be maintained on file and available for review during FORSCOM staff visits.

(2) When the results of the preliminary inquiry determine that compromise may have occurred, or that compromise did occur which may have resulted in damage to national security, the report will be forwarded through command channels to the FORSCOM G-2 for review and final disposition.

(3) When the results of the preliminary inquiry determine that compromise of foreign government information has occurred, or that unauthorized disclosure of classified to the public media has occurred, the report will be forwarded through the FORSCOM G-2 to HQDA (DAMI-CD) for review and further action.

g. The originator(s) of the classified information will be immediately notified upon determination that a possible or actual compromise has occurred, so that a damage assessment and reevaluation of the classification level may be conducted. Notification of originator(s) will not be delayed until completion of the preliminary inquiry.

h. The DUSM will immediately notify the FORSCOM G-2 of all incidents involving the probable compromise of classified information. The notification will be informal and will provide a brief summary of the circumstances

and ongoing actions regarding the incident. Periodic updates will be provided until the incident is resolved locally or forwarded to the FORSCOM G-2 for resolution.

Chapter 10, Paragraph 10-7a. Add the following subparagraphs:

(1) Security incidents involving minor violations of established security regulations in which no compromise has occurred, or damage to national security has not resulted from the compromise, may be considered an administrative discrepancy, and may not require a preliminary inquiry.

(2) Administrative discrepancies would normally not require any remedial, administrative, or disciplinary action; however, this decision will ultimately be determined by the proper local authority. If negligence is involved, or if the possibility of compromise or damage to national security exists, the violation will not be considered an administrative discrepancy.

Chapter 10, Paragraph 10-8. Add the following paragraphs:

a. Additional AR 15-6, Procedures for Investigating Officers and Boards of Officers, investigations should only be conducted for the purposes identified in Paragraph 10-8, AR 380-5, or when the commander determines that the investigation would be productive in providing further clarification of the causes and responsibility for a compromise or security violation. Investigations will be conducted in strict accordance with the provisions of AR 15-6 and command policy.

b. Corrective actions identified by the preliminary inquiry, notification of originators, and reporting requirements specified in Chapter 10, AR 380-5, and this supplement, will not be delayed pending the results of AR 15-6 investigations.

c. Appointed investigating officers will obtain legal review of the completed AR 15-6 investigation report before submitting to the appointing authority. The appointing authority will provide a copy of the finalized report to the DUSM for review and appropriate action, as required by Chapter 10, AR 380-5, and this supplement.

Chapter 10, Paragraph 10-9. Add the following paragraphs:

a. Any incident described in paragraph 10-9, AR 380-5, which involves DA military or civilian personnel who have had access to classified information, will be immediately reported to the DUSM and supporting counterintelligence (CI) element, to determine if further investigation or action is required.

b. If required, a preliminary inquiry will be conducted in accordance with the provisions specified in Chapter 10, AR 380-5, and this supplement.

APPENDIX D, Paragraph D-2b. Add the following sentence**:**

Within FORSCOM, this authority is delegated to the Senior Intelligence Officer (SIO) for each FORSCOM MSC and CONUSA, subject to the provisions of APPENDIX D, AR 380-5, and Director of Central Intelligence Directive (DCID) 1/7.

APPENDIX H, Paragraph H-5. Add the following paragraph:

d. FORSCOM Active and Reserve Component activities will submit requests for code words to the FORSCOM G-3/5/7 (AFOP-OCT). Requests must include the following information:

(1) Full meaning to be assigned.

(2) Classification to be assigned to the code word and its related meaning.

(3) Complete list of commands to which the code word will be disseminated.

(4) Date of activation and deactivation.

APPENDIX H, Paragraphs H-6 and H-7. Add the following sentences:

HQDA has allocated specific words to FORSCOM to be used for the first word of nicknames and exercise terms. FORSCOM Active and Reserve Component activities will submit requests for exercise terms and nicknames to the FORSCOM G-3/5/7 (AFOP-OCT), 1777 Hardee Avenue SW, Fort McPherson, GA 30330-1062. Requests must include the following information:

(1) Exercise term/nickname (second word only).

(2) Description of exercise or reason for nickname (include who, what, where, and when).

(3) Unit desiring the name.

(4) Effective date.

(5) Expiration date.

(6) Point of contact and alternate point of contact (name and telephone number) that can provide additional information, if needed.

HQ FORSCOM will assign a first name to the nickname or exercise term and inform the requester and HQDA of the approved name.

APPENDIX J
Sample Inspection Report Format

(Classification)

REPORT OF SECURITY INSPECTION
Of
(Unit and Location)
(Date)

SECTION I. INTRODUCTION

1. An (announced/unannounced) security inspection was conducted on _____ (Date), by the following representative(s) of _____ (Organization):

_____ (Full Name; Title)

_____ (Full Name; Title)

2. The following unit representatives accompanied the security inspection team:

_____ (Full Name; Title)

_____ (Full Name; Title)

3. The last security inspection was conducted on _____ (Date).

SECTION II. SCOPE

4. This inspection included the following (units/elements/offices/sections):
_____ (List each unit, element, office, or section)

5. Amount and Classification Level of Classified Holdings:

TOP SECRET: _____
SECRET: _____
CONFIDENTIAL: _____
OTHER: _____

(Indicate the amount, by classification level, of documents and material on hand, either by number and type or linear feet and type. Also indicate the percentage of each category of classified documents reviewed during the inspection)

APPENDIX J (Cont'd)

SECTION III. FINDINGS AND RECOMMENDATIONS

6. Uncorrected or repeat findings from previous security inspections:

_____

(Indicate each such finding, and appropriate recommendation. If there are no uncorrected or repeat findings, indicate "None.")

7. Current Findings: (Indicate new findings identified during the security inspection, and appropriate recommendations, to correct the finding. Parenthetical references to appropriate paragraphs of AR 380-5 may also be used to support each finding and recommendation.)

a. Finding:

Recommendation:

b. Finding:

Recommendation:

SECTION IV. COMMENTS

8. (Use this section to record weaknesses (those existing conditions and procedures which, although not in violation of, or at variance with published regulations or directives, may possibly have an adverse effect on the overall security posture) or any other comments considered pertinent to the inspection.)

SECTION V. EXIT BRIEFING

9. All findings and recommendations were discussed during an exit briefing on _____ (Date), presented to the following representatives:

_____ (Full Name; Title)

_____ (Full Name; Title)

_____
(Inspecting Authority)

APPENDIX K
Sample Unannounced Security Check (After Duty Hours)

UNANNOUNCED SECURITY CHECK
(AFTER DUTY HOURS)

1. DATE: _____

2. TIME: _____

3. UNIT/AGENCY: _____

4. LOCATION: _____

5. ITEMS CHECKED	**YES**	**NO**	**N/A**
a. Classified Containers Properly Secured	___	___	___
(1) Security Container Information Forms (SF 700) Not Posted on Exterior of Security Containers	___	___	___
(2) Security Container Check Sheet (SF 702) Properly Executed and Up-To-Date	___	___	___
(3) "Open/Closed" Signs Properly Used	___	___	___
b. Tops of All Classified Containers Clear of Extraneous Material (Books, Paper, etc.)	___	___	___
c. A Spot Check of Waste Cans, Desks, Cabinets, Book Shelves, etc. Revealed No Unsecured Classified Material	___	___	___
d. Destruction Devices Free of Classified Material	___	___	___
e. Copiers/Facsimile Machines Free of Classified information (Documents or Latent Images)	___	___	___
f. Typewriter Ribbons Properly Secured or Free of Classified Information	___	___	___
g. Memory Typewriters Properly Secured or Free of Classified Information	___	___	___
h. End-of-Day Security Checks (SF 701) Properly Conducted and Up-To-Date	___	___	___
i. For Official Use Only (FOUO) Material Properly Secured	___	___	___
j. Building/Office Properly Secured	___	___	___

APPENDIX K (Cont'd)

k. Computers and Other AIS Equipment Properly Secured	___	___	___
(1) Users Logged Off or Power Turned Off	___	___	___
(2) The Following Devices Not Within Six Feet of AIS Equipment Authorized to Process Classified Information			
Telephones	___	___	___
Telephone Lines	___	___	___
Telephone Distribution Boxes	___	___	___
Disconnected and Ungrounded Power Lines	___	___	___
(3) Diskettes/Removable Hard Drives Removed from AIS Equipment	___	___	___
(4) Disks/Removal Hard Drives Stored in a Locked Container	___	___	___
l. Required Warning Labels Are Affixed to Computers and Other AIS Equipment Used Solely for Processing Unclassified Information	___	___	___
m. Other: _____	___	___	___

6. COMMENTS:

_____

_____
(Inspector)

APPENDIX L
Sample Courier Briefing and Certification

General Instructions:

As a designated courier of classified material, you are authorized to hand carry or escort material while in an official travel status between your duty station and other locations, as specified in your courier authorization document. In some situations, you may not have actual access or specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become, as defined in AR 380-5, the custodian of that information.

All military personnel and DA civilian employees are subject to Title 18, United States Code, which deals with unauthorized release of national security information; however, as a courier, you are solely and legally responsible for the protection of the classified information in your possession. This responsibility lasts from the time you receive it until it is properly delivered to the station, agency, unit, or activity listed as the official addressee.

The intent of this briefing is to help you become familiar with your responsibilities as a courier, duties as a custodian, and the security and administrative procedures governing the safeguards and protection of classified information. You must be familiar with the provisions of AR 380-5, DA Information Security Program Regulation, and FORSCOM Supplement thereto, with special emphasis on the following areas:

Access. You will be given delivery instructions for the material when it is released to you. Follow those specific instructions given and seek assistance from a responsible official (Designated Unit Security Manager (DUSM) or Unit/Activity Security Manager) if you are unable to do so. Dissemination of classified material is restricted to those persons who are properly cleared and have an official need for the information. No person is entitled to access classified information solely by virtue of rank or position. To help prevent unauthorized access and possible compromise of the material entrusted to you, it must be retained in your personal possession or properly guarded at all times. You will **not** read, study, display, or use classified material while in public places or conveyances.

Storage. Whenever classified information is not under your personal control, it will be guarded or stored in a GSA approved security container. You will **not** leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, or storage compartments in the passenger section of commercial airlines, trains, or buses. You will **not** store the material in detachable storage compartments such as trailers, luggage racks, or aircraft travel pods. You will **not** pack classified items in regular checked baggage. Retention of classified material in hotel/motel rooms or personal residences is specifically prohibited. Safety deposit boxes provided by motels/hotels do not provide adequate storage for classified material. Advance arrangements for proper overnight storage at a US Government facility or, if in the United States, a cleared contractor facility, are required prior to departure. Arrangements are the responsibility of the activity authorizing the transmission of classified material.

Preparation. Whenever you transport classified information, it must be enclosed in two opaque, sealed envelopes, wrappings, packages, or containers, durable enough to protect the material from accidental exposure and to ease in detecting tampering. A briefcase, when used, will **not** serve as the outer wrapping or container when transporting classified information to locations outside your duty station and local surrounding area. The inner envelope or container shall be addressed to an official government activity (as if for mailing), stamped with the highest classification, and placed inside the second envelope or container. The outer covering will be sealed and addressed for mailing (in event of emergency) to the government activity. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission. Receipts will be exchanged when and if required.

Hand carrying. Your official courier authorization document should ordinarily permit you to pass through passenger control points within the United States without the need for subjecting classified material to inspection. Except for customs inspections, airports have established screening points to inspect all hand carried items. If you are hand carrying classified material, you should process through the ticketing and boarding procedures in the same manner as other passengers. When hand carrying a sealed package within a briefcase (carry-on luggage), it shall be

APPENDIX L (Cont'd)

routinely offered for inspection for weapons. The screening official may physically inspect or x-ray the package without opening the package. If the screening official is not satisfied with your identification, authorization document, or package, you will not be permitted to board the aircraft and are no longer subject to further screening for boarding purposes. Do **not** permit the screening official to open the package or read any portion of the classified information as a condition for boarding.

Escorting. When escorting classified material sealed in a container that is too bulky to hand carry or is exempt from screening, prior coordination is required with the Federal Aviation Authority (FAA) and the airline involved. This coordination is the responsibility of the approving authority. You will report to the airline ticket counter prior to starting your boarding process. You will be exempt from screening. If satisfied, the official will provide an escort to the screening station and exempt the container from physical or other type inspections. If the official is not satisfied, you will not be permitted to board and are no longer subject to further screening. The official will **not** be permitted to open or view the contents of the sealed container.

The actual loading and unloading of bulky material will be under the supervision of a representative of the airline; however, you or other appropriately cleared persons shall accompany the material and keep it under constant surveillance during the loading and unloading process. Appropriately cleared personnel will be available to assist in surveillance at any intermediate stop when the plane lands and the cargo compartment is to be opened. Coordination for assistance in surveillance is the responsibility of the activity authorizing the transmission of the material.

Our primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations cannot guarantee the protection of classified information nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information.

You are also reminded that any classified instructions you receive must also be protected. Do not discuss verbal instructions with anyone after you have delivered the material, and do not discuss where you were, what you did, or what you saw.

If you have questions at any time concerning the security and protection of classified and sensitive material entrusted to you, contact your Designated Unit Security Manager or Senior Intelligence Officer.

COURIER CERTIFICATION OF BRIEFING

As a designated courier of classified material, I, _____ (Name), received a briefing on _____ (Date). The briefing outlined my responsibilities as a courier; duties as a custodian; and the procedures for the proper safeguard and protection of classified information. I am cognizant of the provisions and restrictions imposed by Chapter 8, AR 380-5; and intend to fully comply, unless prevented by an outside force which I cannot control. I fully understand that I must not jeopardize my life or the lives of others when protecting the classified material in my trust; however, I will comply with the regulatory requirements.

The classified material to be transported is not available at my destination. There is neither time nor means available to move the information in the time required to accomplish operational objectives or contract requirements.

_____
(Designated Courier)

_____
(Date)

_____
(Issuing Authority)

APPENDIX M
Sample Courier Authorization

(Office Symbol) (Date of Issue)

TO WHOM IT MAY CONCERN

SUBJECT: Official Courier Designation

1. In accordance with Army Regulation 380-5, Department of the Army Information Security Program, the following individual, who is employed by or is a military member of this organization, is on official government business, and is a designated courier, authorized to hand-carry classified material in conjunction with the travel indicated below.

a. Name of Courier: _____

b. SSN or I.D. No.: _____

c. Organization Name and Address: _____

_____

2. Description of Material: Material is double wrapped in an 8" x ll" envelope, and addressed to: _____ (Insert Destination Address). A listing of the transported material is on file in the traveler's organization identified in paragraph 1c, above.

3. Travel Itinerary:

a. Departure Date: _____

b. Departure Point: _____

c. Destination(s): _____

d. Known Transfer Point(s): _____

4. There is neither time nor alternate means of transportation available to send the material referred to herein that would provide for timely accomplishment of operational objectives. This authorization may be confirmed by calling _____ (Insert Name and Telephone Number of Issuing Authority POC) during normal duty hours.

5. This authorization expires on _____ (Insert date not to exceed 7 days from date of issue, or in the event of a round trip, 7 days after scheduled date of return).

_____
(Issuing Authority)

APPENDIX N
Suggested Topics for Security Education Briefings

Principals of Security Program
Classification Levels
Security Clearance Requirements
Non Disclosure Agreement
Need-to-Know Concept
Legal Statutes
Consequences of Unauthorized Disclosure
Administrative and Criminal Sanctions
Reporting Derogatory Information
Reporting Suspicious Activities
Security Manager Program

Classification Principles
Original Classification
Derivative Classification
Duration of Classification
Security Classification Guide
Classification Challenges
Classification Markings
Declassification Principles
Declassification Exemptions
Automatic Declassification
Downgrading/Upgrading
Compilation of Classified

Classification Marking Principles
Document Marking
Electronic Transmitted Message Marking
Electronic Media Marking
Special Material Marking
Foreign Government Document Marking
Special Warning Notices

Safeguarding and Control Procedures
Safes and Combinations
Care During Duty Hours
End-of-Day Security Checks
Classified Conversations
Classified Telephone Conversations
Classified Visit Procedures
Classified Meeting Procedures
Residential Storage Restrictions

Accountability and Control Procedures
Continuous Control and Accountability Procedures
Receipt Procedures
Inventory Procedures
Reproduction Procedures
Accountability Records

Classification Destruction Principles
Destruction Standards
Destruction Methods
Approved Destruction Equipment
Destruction Records

Transmission and Transportation Standards
Approved Transmission Methods
Preparation of Classified Material
Approved Mail Methods
Escort and Hand carry Procedures
Courier Authorization Requirements
Overseas Transmission Requirements
Commercial Aircraft Courier Requirements

Physical Security Standards
Open Storage Restrictions
Vaults and Secure Rooms
Intrusion Detection Systems
Access Control Procedures
Combination Lock Standards
Individual Custodial Responsibilities

Protection of Controlled Unclassified Information
For Official Use Only Information
Sensitive But Unclassified Information
Sensitive Information (AIS) Information
Law Enforcement Sensitive Information

Protection of AIS Information
E-Mail Security Procedures
Website Security Procedures

APPENDIX N (Cont'd)
Suggested Topics for Security Education Briefings

Unauthorized Disclosure Reporting
Security Violations
Preliminary Inquiry Procedures
AR 15-6 Investigations
Damage Assessment Procedures
Deliberate Disclosure or Compromise
Suspected Espionage
Administrative and Criminal Sanctions

SCI/SAP Information
CNWDI/RD/FRD Information
NATO Information
Security Controls on the Dissemination of Intelligence Information

Industrial Security Principles
Classified Contractor Activities
Classified Contractor Visits
DD Form 254

Security Education Requirements
Initial and Refresher Briefings
Foreign Travel Briefings
Special Function Briefings
Intelligence Oversight Briefings
SAEDA Briefings
Termination Briefings
Security Manager Training

Foreign Disclosure Program
Foreign Government Information
Foreign Visitor Programs

APPENDIX O
Sample Preliminary Inquiry Appointment Memorandum

S: (20 Working Days)

(Office Symbol) (Date)

MEMORANDUM FOR: (Name/Organization)

SUBJECT: Preliminary Inquiry – Possible Compromise of Classified Information

1. You are directed to conduct a preliminary inquiry concerning the facts and circumstances surrounding _____.

2. The preliminary inquiry will be conducted in accordance with the provisions specified in Chapter 10, AR 380-5 and FORSCOM Supplement 1. The preliminary inquiry report will be prepared in the format provided at Figure 10-1, Chapter 10, AR 380-5. The completed report must be provided to this office NLT COB _____ (20 working days from date of memorandum).

3. You may obtain technical advice and assistance concerning your duties and responsibilities from _____ (Designated Unit Security Manager (DUSM) or Unit/Activity Security Manager). You may obtain legal advice, if needed, from _____ (Local SJA Representative).

_____
(Appointing Authority)

APPENDIX P
Sample Appointing Authority Review Memorandum

(Office Symbol) (Date)

MEMORANDUM FOR: (Designated Unit Security Manager)

SUBJECT: Preliminary Inquiry – Possible Compromise of Classified Information

1. I have reviewed the enclosed preliminary inquiry report, and concur with all findings and recommendations contained therein.

----- OR -----

I have reviewed the enclosed preliminary inquiry report, and concur with findings and recommendations contained therein, with the exception of _____ (List each nonconcurrence issue and reason for non-concurrence).

2. In my opinion, additional investigation into this incident is not warranted.

----- OR -----

In my opinion, additional investigation into this incident is warranted. I have appointed _____ (Name/Organization) to conduct a formal investigation, under the provisions of AR 15-6. The results of this investigation will be provided to you, upon completion.

3. The following corrective actions have been implemented, to prevent recurrence:

a. _____

b. _____

c. _____

4. The results of the preliminary inquiry have also been referred to _____ (responsible commander) for appropriate action as he or she deems necessary. Any action taken by the commander will be reported to you, upon completion. (If applicable)

_____
(Appointing Authority)

APPENDIX Q
FORSCOM Major Subordinate Commands, Senior Mission Commands, and Direct Reporting Units

Major Subordinate Commands and Senior Mission Commands:

First US Army
Fort Gillem, GA

Third US Army
Fort McPherson, GA

Fifth US Army
Fort Sam Houston, TX

US Army Reserve Command
Fort McPherson, GA

I Corps
Fort Lewis, WA

III Corps
Fort Hood, TX

XVIII Airborne Corps
Fort Bragg, NC

National Training Center
Fort Irwin, CA

Joint Readiness Training Center
Fort Polk, LA

3d Infantry Division
Ft Stewart, GA

7th Infantry Division
Fort Carson, CO

10th Mountain Division (LT)
Fort Drum, NY

24th Infantry Division (MECH)
Fort Riley, KS

101st Airborne Division (AASLT)
Fort Campbell, KY

Direct Reporting Units:

32d Army Air Missile Defense Command
Fort Bliss, TX

7th Transportation Group
Fort Eustis, VA

36th Engineer Group
Fort Benning, GA

49th Quartermaster Group
Fort Lee, VA

52d Ordinance Group (EOD)
Fort Gillem, GA

5th Engineer Battalion (CORPS) (MECH)
Fort Leonard Wood, MO