DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT JACKSON
2400 JACKSON BOULEVARD
FORT JACKSON, SC 29207-5015

AMIM-FJO-S (380) 15 June 2023

MEMORANDUM FOR All United States Army Garrison Fort Jackson Personnel

SUBJECT: USAG Policy Memorandum #31 – Management of the USAG, Fort Jackson Information Security and Industrial Security Programs

1. References:

a. Information Security Oversight Office Classified National Security Information Directive No. 1.

b. EO 12829, National Industrial Security Program

c. EO 13526, Classified National Security Information

d. DODI 5200.1 Vol 1, Information Security Program: Overview, Classification and Declassification

e. DODI 5200.1 Vol 2, Information Security Program: Marking of Information

f. DODI 5200.1 Vol 3, Information Security Program: Protection of Classified Information

g. DODI 5200.1 Vol 4, Information Security Program: Controlled Unclassified Information (CUI)

h. DODI 5200.1-PH, DoD Guide to Marking Classified Documents

i. DODI 5200.48, Controlled Unclassified Information

j. DODI 5220.22-M, National Industrial Security Program

k. AR 25-2, Army Cybersecurity

l. AR 25-400-2, The Army Records Information Management System (ARIMS)

m. AR 380-5, Information Security Program

n. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives

o. AR 380-40, Policy for Safeguarding and Controlling Communications Security Material

p. AR 380-67, Personnel Security Program

q. AR 381-12, Threat Awareness and Reporting Program (TARP)

r. AR 525-13, Anti-Terrorism

2. Purpose. This policy identifies and standardizes the processes, requirements, and procedures relating to the United States Army Garrison (USAG), Fort Jackson Information Security (INFOSEC) Program.

3. Applicability. This policy applies to all military, DA civilian, and contractor personnel assigned to or attached to USAG, Fort Jackson.

4. Scope. This implements the policy set forth in AR 380-5 (Army Information Security Program) and DoD Manual 5200.1 (DoD Information Security Program) for the classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security.

5. Responsibilities.

a. Directorate of Plans, Training, Mobilization, and Security (DPTMS), Fort Jackson. Security is a command function. DPTMS, Fort Jackson, has overall responsibility for security programs within the USAG, Fort Jackson. The DPTMS (Security Division) will:

(1) Establish written local security policies and procedures.

(2) Initiate and supervise measures or instructions necessary to ensure continual control of classified and sensitive information and materials.

(3) Ensure persons requiring access to classified information are properly cleared.

(4) Designate a security manager by written appointment.

(5) Ensure prompt and complete reporting of security incidents, violations, and compromises relating to classified and sensitive information.

(6) Approve annual inspection dates prior to being forwarded to USAG Plans and Operations for publishing.

b. DPTMS Security Manager. The DPTMS security manager will:

(1) Advise and represent the Commander, USAG, Fort Jackson, on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

(2) Establish and implement an effective security education program.

(3) Establish procedures for assuring all persons handling classified material are properly cleared.

(4) Advise and assist officials on classification problems and development of classification guidance.

(5) Ensure classification guides for classified plans, programs, and projects are properly prepared, distributed, and maintained.

(6) Conduct a periodic review of classifications, assigned at USAG, Fort Jackson, to ensure classification decisions are proper.

(7) Review and continually reduce unneeded classified and sensitive material.

(8) Supervise or conduct security staff assistance visits, inspections, and spot checks regarding the compliance of Reference 1.m.

(9) Ensure the inquiry and reporting of security violations is completed.

(10) Ensure proposed public releases on classified and sensitive information be reviewed to preclude the release of classified and sensitive unclassified information.

(11) Establish and maintain visit control procedures in cases in which visitors are authorized access to classified information.

(12) Issue contingency plans for the emergency destruction of classified and sensitive information/material.

(13) Be the single point of contact to coordinate and resolve classification or declassification problems.

(14) Report data as required by Reference 1.m and HQDA G-2.

(15) Provide expertise, guidance, management, and oversight for the USAG, Fort Jackson Information Security Program.

(16) Provide Security Education and Training Awareness (SETA) to USAG, Fort Jackson employees.

(17) Conduct Information Security staff assistance visits annually in those sections holding classified information, if requested.

(18) Provide annual inspection dates in accordance with (IAW) Appendix S of this policy to USAG Plans and Operations to be published in the USAG calendar.

c. Section Supervisors. Managers and supervisors assigned to USAG, Fort Jackson have a key role in the effective implementation of security programs. Managers and supervisors set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information relating to national security. Managers and supervisors will:

(1) Ensure subordinate personnel who require access to classified information are properly cleared and given access only to that information for which they have a need-to-know.

(2) Ensure subordinate personnel are trained in, understand, and follow security requirements.

(3) Oversee subordinate personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.

(4) Lead by example. Management and supervisors shall follow DA policies and procedures to properly protect classified and sensitive information, and classify/declassify information, as appropriate.

(5) Coordinate Staff Assistance Visit (SAV) dates with the security office and conduct self-inspections IAW Appendix S.

d. USAG, Fort Jackson Personnel.

(1) All USAG, Fort Jackson personnel have a personal, individual, and official responsibility to safeguard information related to national security and protect government property. Security regulations do not guarantee protection and cannot be written to cover all situations. Basic security principles, common sense, and a logical interpretation of regulations must be applied.

(2) USAG, Fort Jackson personnel will report, through their supervisor to the DPTMS Information Security Office, violations that could lead to the unauthorized disclosure of classified and sensitive information.

6. It is vital that we continually protect personnel who live, work, and visit Fort Jackson, and the classified and sensitive information stored within the Installation perimeter, in the interest of national security from natural and manmade threats and disasters.

Encl
Appendices A-Z

TIMOTHY R. HICKMAN
COL, AG
Commanding

APPENDIX A
INDEX

APPENDIX A
INDEX (CONTINUED)

APPENDIX B
ORIGINAL VS. DERIVATIVE CLASSIFICATION

1. Original Classification.

a. Original classification is the initial determination that information requires, in the interests of national security, protection against unauthorized disclosure. This decision will be made only by persons specifically authorized in writing to do so and who have received training. The decision to originally classify must be made based on the requirements of Reference 1.m. Delegations of original classification authority will be limited to the minimum required and only to officials who have a demonstrable and continuing need to exercise it.

b. These decisions can only be made by persons designated in writing who have received training in the exercise of this authority, and who have program(s) support responsibility or cognizance over the information.

c. The Original Classification Authority (OCA) must determine that, if classification is applied, there is a reasonable possibility that the information will be provided protection from unauthorized disclosure. Once a decision is made to classify, information will be classified at one of three levels:

(1) Top Secret - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) Secret - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) Confidential - Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

d. U.S. classification can only be applied to information:

(1) Owned by, produced by or for, or is under the control of the U.S. Government.

(2) Reasonably could be expected to result in damage to the national security, to include defense against transnational terrorism.

(3) The OCA is able to identify or describe the damage.

APPENDIX B
ORIGINAL VS. DERIVATIVE CLASSIFICATION (CONTINUED)

(4) Which falls within one or more of the following categories:

(a) Military plans, weapons systems, or operations.

(b) Foreign government information.

(c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology.

(d) Foreign relations or foreign activities of the United States, including confidential sources.

(e) Scientific, technological, or economic matters relating to the national security.

(f) United States Government programs for safeguarding nuclear materials or facilities.

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

(h) The development, production, or use of weapons of mass destruction.

2. Derivative Classification.

a. Derivative classification is incorporating, restating, paraphrasing, or generating in new form, information that has already been determined to be classified and ensuring it is classified and handled at the level the OCA has already determined. Derivative classification is most commonly accomplished by marking classified material based on the guidance from a security classification guide (SCG) or from the source document. The OCA decides what portion(s) of a plan, program, project, or mission need to be classified. The derivative classifier applies the decision to the same type of information restated or generated in a new form.

b. Officials who sign or approve derivative classified material are responsible for the accuracy of the derivative classification. Information taken from a classified document by multiple sources will identify the source document, its date, the classification authority, and the downgrading instructions. A list of all documents used to compile a document will be kept with the file copy.

APPENDIX B
ORIGINAL VS. DERIVATIVE CLASSIFICATION (CONTINUED)

c. The compilation of classified information may warrant higher classification than that of its component parts. If this is the case, the higher classification shall be fully supported, in writing, and accompany the compilation document.

APPENDIX C
CLASSIFICATION GUIDES

1. Security classification guides are issued for each system, plan, program, or project in which classified information is involved. The responsible OCA shall approve these guides, in writing, at the highest level designated by the guide.

2. Security classification guides will, at a minimum, include the following information:

a. Identify specific items/elements of information to be protected and the classification level to be assigned.

b. Provide declassification instructions for each item/element, to include any exemptions.

c. Provide a concise reason for classification for each item/element.

d. Identify any special handling caveats, warning notices, or instructions.

e. Identify by name or personal identifier, the OCA, along with the date of the approval.

f. Provide a point of contact, address, and telephone number for any questions, challenges, or suggestions, and include a statement encouraging personnel to informally question the classification of information before formally challenging.

3. Whenever necessary, security classification guides will be revised to promote effective derivative classification. Guides will only be cancelled if:

a. All classified information has been declassified.

b. When the system, plan, program, or project classified by the guide has been cancelled.

c. When a major restructure has occurred and the information has been incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification.

4. The decision to declassify the guide rests with the OCA and authorized Army authorities. Further guidance relating to security classification guide preparation can be found in Reference 1.m.

APPENDIX D
DECLASSIFICATION PROCEDURES

1. Information will be declassified as soon as it no longer meets the standards for classification. The OCA shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives.

2. Executive Order 13526, Section 3.3 sets forth policy on the automatic declassification of information. Specifically, all classified records that are 25 years old or older determined to have permanent, historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. However, no DA records will be automatically declassified without review. Subsequently, all classified records shall be automatically declassified on 31 December of the year that is 25 years from the date of its original classification. Exceptions follow:

a. Revealing the identity of a confidential human source, or a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

b. Revealing information that would assist in the development or use of weapons of mass destruction.

c. Revealing information that would impair U.S. cryptologic systems or activities.

d. Revealing information that would impair the application of state of the art technology within a U.S. weapon system.

e. Revealing formerly named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.

f. Revealing information, including foreign government information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States.

g. Revealing information that would impair the current ability of Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of national security, are authorized.

APPENDIX D
DECLASSIFICATION PROCEDURES (CONTINUED)

h. Revealing information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to national security.

i. Violates a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

3. Delays to the automatic rule may be authorized. See Sec. 3.3, Exec. Order 13526.

4. Downgrading information is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level.

APPENDIX E
DESTRUCTION PROCEDURES

1. Classified documents and other material will be retained only if they are required for effective and efficient operation of the command, or if their retention is required by law or regulation.

2. The USAG, Fort Jackson Security Office will establish at least one day a year in the month of June, when specific attention and effort is focused on disposing of unneeded classified material (clean-out day). This day will be identified and communicated to the agencies by the USAG, Fort Jackson Security Office.

3. Classified materials which are no longer required will be destroyed completely to preclude recognition or reconstruction of the classified information contained in or on the material. A cross-cut shredder that is listed on the NSA/CSS Evaluated Products List for Paper Shredders shall be utilized when shredding classified documents, using the "secure volume" method. The shredder must reduce paper documents to shards not exceeding 1 millimeter by 5 millimeters or less.

4. The "secure volume" destruction concept enhances security by restricting the chances of successful reconstruction of the material by either:

a. Prohibiting destruction until there are at least 20 similar pages of classified paper to destroy.

b. Adding similar type of unclassified pages of paper (not blank) to arrive at the minimum 20 similar page count.

c. Shredded material will be stirred before discarding to ensure the content is mixed up.

5. Other approved routine methods of destruction for destroying paper-based material include pulping, pulverizing, and disintegration. Pulverizers and disintegrators must have a 3/32 inch or smaller security screen. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water soluble material.

6. Shredding, pulping, and pulverizing machines shall not be used for destroying classified typewriter ribbons, microfilm, photographs, computer disks, CD-ROMs and other non-paper-based products. Paragraphs 3-16 through 3-18, Reference 1.m, and Paragraph 4-20, Reference 1.o, outline requirements for destroying non-paper-based classified materials.

APPENDIX E
DESTRUCTION PROCEDURES (CONTINUED)

7. Records of destruction are required for Top Secret, NATO, and foreign government documents and material. A DA Form 3964 may be used for this purpose. Two persons will sign the destruction record for above documents/materials as witnessing the destruction. Records of destruction will be maintained for five years from the date of destruction. Refer to Reference 1.m for destruction and retention standards for NATO classified materials.

8. Records of destruction are not required for Secret and Confidential materials unless required by the originator.

APPENDIX F
MARKING DOCUMENT PROCEDURES

1. Marking is the principal means of informing holders of classified and sensitive information of its classification/sensitivity level and protection requirements. Marking serves the following purposes:

a. Alerts holders to the presence of classified and sensitive information.

b. Identifies the exact information needing protection.

c. Indicates the level of classification/sensitivity assigned to the information.

d. Provides guidance on downgrading and declassification.

e. Gives information on the source(s) and reason(s) for classification of information.

f. Warns holders of special access, control, dissemination, or safeguarding requirements.

2. Classified material other than paper documents require the same markings and must have the same information either marked on it or made available to holders by other means of notification. Classified and sensitive material will bear the following markings:

a. The overall (highest) classification/sensitivity of the information. The overall (highest) classification marking will be conspicuously marked, stamped, or affixed, top and bottom, on the front and back covers (if any), on the title page (if any), and on the first page, in letters larger than those on the rest of the page.

b. The command, office of origin, date, and if not evident by the name of the command, the fact that the document was generated by DA.

c. Identification and date of the specific classified information in the document and its level of classification (page and portion markings).

d. Identification of the source(s) of classification ("Classified by" or "Derived from" line) and the concise reason(s) for classification if an original classification or the reason(s) the source of the classified portion(s) is/are derived from.

e. Declassification instructions ("Declassify on" line) and downgrading instructions, if downgrading applies.

APPENDIX F
MARKING DOCUMENT PROCEDURES (CONTINUED)

f. Warning and sensitivity notices and other markings, if any, applying to classified material.

3. Other Markings.

a. Downgrading instructions will be placed on the face of each document to which they apply.

b. Component parts of a document, i.e., annex, appendix, shall be marked as a separate document if it is likely the component will be removed and used or maintained separately.

c. When classified, transmittal documents, i.e., cover memo, FAX header, shall be marked the same as any other classified document. If unclassified, "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES" shall be marked on the face of the transmittal.

d. Documents marked as classified for training purposes shall have one of the following markings to clearly show that the document is actually unclassified:

(1) CLASSIFIED FOR TRAINING ONLY.

(2) CLASSIFICATION MARKINGS FOR TRAINING PURPOSES ONLY.

(3) UNCLASSIFIED SAMPLE.

e. Files, folders, and binders containing classified and/or sensitive information will be marked with the highest classification/sensitivity of information contained therein on the outside, front and back, and top and bottom of the file or folder. Document cover sheets will be removed upon placing the file in a secure storage container.

f. Any classification markings, warning notices, caveats, release, and declassification/downgrading instructions will be marked or stamped (in black ink) to ensure legibility when not clearly visible on reproduced copies.

4. Marking Special Types of Material.

a. When classified or sensitive information is contained in Information Technology (IT) equipment, hardware, media, or on film, tape, or other audio/visual media, the

APPENDIX F
MARKING DOCUMENT PROCEDURES (CONTINUED)

marking provisions of paragraph 18, Enclosure 3, Reference 1.e will be met in a way that is compatible with the type of material. This is to ensure holders and users are clearly warned of the presence of classified/sensitive information. These types of materials will be marked with the following labels:

(1) SF 706 - Top Secret label for IT media.

(2) SF 707 - Secret label for IT media.

(3) SF 708 - Confidential label for IT media.

(4) SF 710 - Unclassified label for IT media.

(5) SF 711 - Data descriptor label for IT media.

(6) SF 712 - Classified SCI label.

Note: The SF 710 is not required when there is no classified information created or used in the same vicinity.

b. Classified information contained on fixed or removable magnetic storage media will be stored in an authorized classified container or used in a facility that has been approved for open storage of classified material. Refer to Reference 1.e for additional marking requirements and guidance regarding removable AIS storage media.

c. Changes in Markings.

(1) When a document is marked for downgrading or declassification on a date or event, downgrading or declassification is automatic at the specified time unless notification to the contrary is received from the originator, the original classification authority, or other appropriate authority. If a holder of the document has reason to believe it should not be downgraded or declassified, the holder will notify the originator and OCA (if known) of the information.

(2) When a document is declassified IAW with its markings, the overall and page markings will be cancelled, if practical.

(3) If a document is downgraded IAW with its markings, the old classification/sensitivity markings will be cancelled and substituted with the new.

APPENDIX F
MARKING DOCUMENT PROCEDURES (CONTINUED)

(4) If a document is upgraded, all classification/sensitivity markings affected by the upgrading will be changed to the new markings, without exception. In addition, the date of the remarking and the authority for the action will be placed on the face of the document.

d. Foreign government information shall be marked IAW paragraph 19, Reference 1.e. Sample markings of foreign government information and equivalent foreign security classifications are contained in above chapter. Classified documents originated by NATO, if not already marked with the appropriate classification in english, will be so marked. Additional marking requirements can be found in paragraph 19, Reference 1.e.

APPENDIX G
CONTROLLED UNCLASSIFIED INFORMATION PROCEDURES

1. There are other types of information that require controls and protective measures for a variety of reasons. This information is known as Controlled Unclassified Information (CUI).

2. CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Law, regulation, or government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

3. In accordance with part 2002 of Title 32, Code of Federal Regulations (C.F.R.), CUI requires safeguarding or dissemination controls identified in a law, regulation, or government-wide policy for information that does not meet the requirements for classification in accordance with E.O. 13526. Unlike classified information, an individual or organization does not need to demonstrate a need-to-know to access CUI, unless required by a law, regulation, or government-wide policy, but must have a lawful governmental purpose for such access.

4. Marking requirements for CUI materials:

a. At a minimum, CUI markings for unclassified DoD documents will include the acronym "CUI" in the banner and footer of the document.

b. If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with "(CUI)." Use of the unclassified marking "(U)" as a portion marking for unclassified information within CUI documents or materials is required.

(1) There is no requirement to add the "U," signifying unclassified to the banner and footer as was required with the old FOUO marking.

APPENDIX G
CONTROLLED UNCLASSIFIED INFORMATION PROCEDURES (CONTINUED)

(2) Banners, footers, and portion marking will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 Information Security Oversight Office (ISOO) letter. If the document also contains CUI, it will be marked in accordance with paragraph 3.4, Reference 1.i.

(3) The first page or cover of any document or material containing CUI, including a document with comingled classified information, will include a CUI designation indicator. This CUI designation indicator is similar to the classification-marking block used for Classified National Security Information documents and materials. The CUI designation indicator must contain, at a minimum:

(a) The name of the DoD component determining that the information is CUI.

(b) The office making the determination.

(c) Identification of the types of CUI contained in the document.

(d) A distribution statement or dissemination controls applicable to the document.

(e) Phone number or office mailbox for the originating DoD Component or authorized CUI holder.

c. CUI markings in classified documents will appear in paragraphs or subparagraphs known to contain only CUI and must be portion marked with "(CUI)." "CUI" will not appear in the banner or footer.

d. The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

e. CUI materials will be protected from unauthorized disclosure during handling with the use of the Standard Form 901, CUI cover sheet. Electronic media that contains CUI information or is used for processing CUI information will be labeled using the Standard Form 902, CUI Label.

f. During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present.

APPENDIX G
CONTROLLED UNCLASSIFIED INFORMATION PROCEDURES (CONTINUED)

g. After working hours, CUI information will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

h. DoD personnel will not use unofficial or personal e-mail accounts, messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI.

i. CUI information and material may be transmitted via first class mail, parcel post, or bulk shipments. When practical, CUI information may be transmitted electronically (e.g. data website, or e-mail), via approved secure communication systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security.

j. CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission.

k. Handling and storage of hard copy CUI outside of the office will be kept to a minimum. Persons handling, traveling with, or storing CUI documents will comply with the following measures:

(1) Notify the Security Manager when removing CUI documents from the U.S. Government facility or office. Properly mark and protect the CUI documents with at least one physical barrier (e.g. place the documents in a folder, opaque envelope, or brief case) to avoid detection while transporting them.

(2) Keep the CUI documents protected and do not view CUI in public, including while using public transportation, to minimize the risk of unauthorized disclosure.

(3) Temporarily store CUI documents outside of government facilities (to include personal residences) in a locked desk, file cabinet, or similar secure area where only the authorized holder has access.

APPENDIX H
CONTROL MEASURE PROCEDURES

1. DA personnel are responsible for safeguarding classified information for which they have access. This responsibility includes ensuring they do not permit access to sensitive or classified information by unauthorized personnel. An unauthorized person is any person who does not have a need-to-know and who is not cleared or granted access to information at that level.

2. SF 312 (Classified Information Nondisclosure Agreement). Prior to granting access to classified information, personnel shall receive a security briefing outlining their responsibility to protect classified information and will sign an SF 312.

3. Debriefings. All personnel who are retiring, resigning, being discharged, or will no longer have access to classified information, will receive a debriefing and will sign a debriefing statement, normally the SF 312 debriefing acknowledgement.

4. NATO Access. The USAG, Fort Jackson Security Office, shall provide the appropriate NATO briefing and maintain acknowledgements for individuals requiring access to NATO information.

5. Care During Working Hours.

a. Classified material removed from storage will be kept under constant surveillance, and control, by authorized personnel. Classified document cover sheets, SFs 703, 704, and 705 (Top Secret, Secret, and Confidential Cover Sheets, respectively) will be placed on classified documents or files not in secured storage.

b. SF 702 (Security Container Check Sheet).

(1) An SF 702 will be displayed on each piece of equipment used to store classified material. The SF 702 is used to record the date and time of each instance when a security container is opened and closed and the initials of the individual(s) doing so.

(2) A person, other than the person who locked the container, when possible, will check the container to make sure it is properly secured. This person will record the time the container was checked and initial the form.

(3) Security containers not opened during the workday will be checked and the action recorded on the SF 702. Notations will also be made on the SF 702 if containers are opened after hours, on weekends, and on holidays.

APPENDIX H
CONTROL MEASURES PROCEDURES (CONTINUED)

(4) The SF 702 will be retained at least 24 hours following the last entry. Reversible open-closed or open-locked signs will be utilized on each security container or vault in which classified information is stored.

c. SF 700 (Security Container Information).

(1) Each security container, vault, and open storage area shall utilize the SF 700. The SF 700 provides the location of the container/vault, and the names, home addresses, and home phone numbers of the individuals having access to the container, vault, or secured room.

(2) Parts 1, SF 700, will be posted on the inside of the locking drawer/door.

(3) Parts 2 and 2A, SF 700, will be marked with the highest classification of material stored in the container. Part 2A will be detached and inserted in the envelope, and the envelope shall be sealed.

(4) Parts 2 and 2A will then be secured in the a separate security container approved for the storage of classified information and treated as information having a classification equal to the highest classification level of the classified information stored in the container, vault, or secured room. Part 2A, SF 700, used to record a Top Secret combination, will be accounted for in the same manner as other Top Secret documents.

d. Unattended, Open Security Containers/Areas. A person discovering an unattended, open security container or security storage area will:

(1) Keep the container/area under guard/surveillance.

(2) Notify one of the persons listed on Part 1, SF 700. If one of the individuals cannot be contacted, the unit Staff Duty Officer or the Fort Jackson Installation Operations Center (IOC) will be notified.

(3) The individual contacted when a container or area is found open or unattended will:

(a) Report to the location, and check the contents for visible indications or evidence of tampering, theft, or compromise.

APPENDIX H
CONTROL MEASURES PROCEDURES (CONTINUED)

(b) If there is evidence of tampering, theft, or compromise, a lock technician will be called to determine the nature of the tampering and whether the security container is operating properly.

(c) Change the combination and lock the container. If the combination cannot be changed immediately, the container will be locked and placed under guard until the combination can be changed, or the classified contents will be transferred to another container or secure area.

e. End-of-Day Checks.

(1) Areas that access, process, or store classified information will ensure security checks are performed at the close of each working day as well as after-hours, weekend, and holiday activity.

(2) The SF 701 (Activity Security Checklist) will be used to record such checks to ensure all classified material is properly secured prior to departing the area.

APPENDIX I
EMERGENCY PLANNING PROCEDURES

1. To minimize the risk of compromise, every section responsible for the storage of classified documents will develop an emergency plan to protect, remove, and/or destroy classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action.

2. The emergency plan will be posted to the outside of the security container. To serve a group of containers, the plan will be posted in the vicinity of the containers. For vaults or secure areas, the plan will be posted just inside the vault/secure area.

3. Each USAG, Fort Jackson agency that holds classified documents is required to maintain an approved emergency plan. Custodians of classified security containers, vaults, and open storage facilities will review approved emergency plans at least annually.

4. An example of an emergency plan is attached.

U.S. ARMY GARRISON, FORT JACKSON
EMERGENCY EVACUATION AND DESTRUCTION PLAN (SAMPLE)

1. Reference. AR 380-5, Army Information Security Program

2. Purpose. To prescribe procedures and assign responsibility for the emergency evacuation or destruction of classified material within (insert section), USAG, Fort Jackson, in the case of fire, natural disaster, civil disturbance, terrorist attack, or imminent hostilities, to minimize the risk of its compromise.

3. Applicability. This plan applies to (insert section).

4. Scope. This plan prescribes procedures for the emergency evacuation or destruction of classified material within (insert section), defines responsibility of personnel for executing this plan, and provides authority and guidance for implementation.

5. Responsibilities.

a. The Commander, USAG, Fort Jackson, or his designated representative, is the implementing authority for this plan.

b. (insert section) Directors or designated representatives are responsible for implementing Paragraph 6.b.4 below.

c. All personnel listed on the SF 700 (Security Container Information) are responsible for the implementation of this plan.

6. Procedures.

a. The responsible recipient will review all classified material for proper disposition, retention, destruction, classification/markings, or transfer.

b. Fire. To ensure risk of injury or loss of life is minimized, the following actions will be taken in regard to classified material:

(1) If there is little reaction time, leave classified material in place.

(2) Secure classified containers unless there is no time to do so.

(3) If possible, remove and safeguard any classified document accountability records.

U.S. ARMY GARRISON, FORT JACKSON
EMERGENCY EVACUATION AND DESTRUCTION PLAN
(SAMPLE CONTINUED)

(4) Designate and train authorized personnel to position themselves at selected locations around the affected area for the prevention of unauthorized removal of classified material.

c. Natural Disasters.

(1) Tornadoes. If time permits, secure all classified material within classified containers, and remove and safeguard any classified document accountability records.

(2) Flooding. Move classified material and equipment to a location to ensure their protection. Disconnect all electrical equipment from electrical outlets, and place the equipment above floor level by placing on desktops, cabinets, tables, etc.

d. Civil Disturbances. Secure classified material in appropriate security containers and post knowledgeable individuals at each entrance to control access. If the seriousness of the situation warrants, the Commander, USAG, Fort Jackson, or his designee will direct Fort Jackson Military Police to provide security.

e. Terrorist Activities/Imminent Hostilities. Unless otherwise directed or when emergency removal is impractical due to the volume of classified material, (insert section) personnel will ensure classified material is secured in authorized security containers, and all outside entrances into the area are secured. Total destruction will occur only at the direction of the Commander, USAG, Fort Jackson, his designated representative, or the USAG Security Office.

f. In situations not specifically anticipated by this plan or when circumstances warrant it, the senior individual present in an office containing classified material may deviate from procedures in this plan. Any deviation will be within basic security principles and guidelines.

g. When emergency evacuation or destruction procedures are complete, reconcile all accountable records, conduct a 100 percent inventory of accountable classified documents and material, and report immediately to the USAG, Fort Jackson Security Office any discrepancies.

h. A copy of this plan will be posted on each security container, near a group of containers, or on the inside doorway of approved vaults and open storage areas in which classified material is stored.

U.S. ARMY GARRISON, FORT JACKSON
EMERGENCY EVACUATION AND DESTRUCTION PLAN
(SAMPLE CONTINUED)

7. IMPLEMENTATION. Implement the provisions of this plan on the order of the Commander, USAG, Fort Jackson, his designated representative, or the USAG, Fort Jackson Security Office.

8. COORDINATING INSTRUCTIONS. Questions regarding this plan should be referred to the (insert section) Manager, (insert phone number), or the USAG, Fort Jackson Security Office, 803-751-6935/4258.

APPENDIX J
TELEPHONE DISCUSSION PROCEDURES

1. Classified discussions are not permitted in personal residences, in public, in transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces in a U.S. government or cleared contractor facility. Written requests for exception to policy will be forwarded to the USAG, Fort Jackson Security Office.

2. In telephone conversations, classified information will only be discussed over secure communication equipment, i.e. STU-III/STE. Steps will be taken to ensure individuals that are uncleared, or do not have a need to know, do not hear classified discussions.

APPENDIX K
REMOVAL OF CLASSIFIED STORAGE/EQUIPMENT PROCEDURES

1. Storage containers and information processing equipment which has been used to store or process classified information will be inspected by cleared personnel before removing from protected areas, and/or before unauthorized persons are allowed unescorted access to them.

2. This inspection ensures no classified information remains within or on the equipment. Items to be inspected include security containers, reproduction equipment, facsimile machines, micrographic readers and printers, Information Technology (IT) equipment, equipment used to destroy classified material, and other equipment used for safeguarding or processing classified information.

3. Desks, cabinets, and other furniture items located in protected areas where classified material is routinely accessed will be inspected to ensure the items are free of classified material before removing from protected area.

4. A written record of the inspection will be completed and retained by the Installation Security Manager for two (2) years.

APPENDIX L
CLASSIFIED VISITS PROCEDURES

1. Fort Jackson personnel visiting other Army commands, other U.S. government agencies, and/or U.S. government contractors will provide advance notification of any pending visit that is anticipated to involve access to classified information.

2. For classified visits within DoD, the Defense Information System for Security (DISS) will be utilized to verify/provide an individual's security access level.

3. When required by organizations outside DoD, classified visit requests will be forwarded to the visited organization and will include:

a. Visitor's full name, date, and place of birth, social security number, and rank or grade.

b. Visitor's security clearance and any special access authorizations required for the visit. Security clearance information will include security clearance level, date clearance granted, type of investigation completed, and investigation completion date.

c. A signature from the Security Officer or from an official other than the visitor who is in a position to verify the person's security clearance.

d. The full Fort Jackson address and the telephone number of a point of contact (usually the person signing the visit request, the Security Manager, or other official who can verify the security clearance status).

e. The name and address of the activity to be visited and the name of the person(s) and phone number(s) to be contacted at the visited activity.

f. The purpose of the visit in sufficient detail to establish an assessment of need-to-know and necessity of the visit.

g. The date and duration of the proposed visit. Intermittent visits on the same visit request are authorized for up to one year, when stated on the request and approved by the command/agency/company being visited.

4. Installation Security Managers will ensure individuals visiting USAG, Fort Jackson activities who require access to classified information have the appropriate security access level and need-to-know prior to granting classified material access.

APPENDIX L
CLASSIFIED VISITS PROCEDURES (CONTINUED)

5. Visit requests can be approved, denied, or rescheduled at the option of the command/agency/company being visited.

6. USAG, Fort Jackson activities having a classified contract will maintain a current visit certification on file for all contractor personnel having access to government classified material until the contractor Facility Security Officer (FSO) has implemented and populated contractor DISS Personnel Security data and access levels. Once implemented and populated, contractor access levels will be verified using DISS.

APPENDIX M
CLASSIFIED MEETINGS/CONFERENCES PROCEDURES

1. Meetings, conferences, classes, seminars, symposia, and similar activities at which classified information is to be presented or discussed are considered classified meetings.

2. The classified portions of these meetings present special vulnerabilities to unauthorized disclosure and will be limited to persons possessing an appropriate security clearance and access and the need-to-know for the specific information involved.

3. Security requirements contained within this policy and reference 1.m apply, without exception, to classified meetings.

4. Any USAG, Fort Jackson section requesting a classified meeting will ensure the following requirements are met:

a. The classified meeting or session is mission critical to the Army.

b. Use of other approved methods or channels for disseminating classified information or material are insufficient, impractical, and not cost effective.

c. The meeting or conference, or classified sessions take place only at an appropriately cleared Government facility or a contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless a waiver is approved in advance by the DCS, G-2.

5. Routine day-to-day classified meetings and gatherings at DA commands will be conducted only at an appropriately cleared government or contractor facility. Waivers will not be granted for routine meetings.

6. Access to the meeting or conference, or specific sessions thereof, where classified information may be discussed or disseminated is limited to persons who possess an appropriate security clearance and need-to-know.

7. Any participation by foreign representatives complies with Reference 1.n.

8. Information systems used during the meeting or conference to support creation or presentation of classified information will meet all applicable requirements for processing classified information in accordance with Reference 1.m.

APPENDIX M
CLASSIFIED MEETINGS/CONFERENCES PROCEDURES (CONTINUED)

9. The USAG, Fort Jackson agency sponsoring a classified meeting or conference will assign an official to serve as Security Manager for the meeting and be responsible for ensuring that, at a minimum, the following security provisions are met:

a. Attendees are briefed on safeguarding procedures.

b. Entry is controlled so only authorized personnel gain entry to the area.

c. The perimeter is controlled to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would result in the compromise of classified information.

d. Escorts are provided for uncleared personnel who are providing services to the meeting or conference (for example, setting up food or cleaning) when classified presentations or discussions are not in session.

e. Use of cell phones, Personal Electronic Devices (PED), 2 way pagers, laptop computers, and other electronic devices that record or transmit are prohibited.

f. Classified notes and handouts are safeguarded in accordance with paragraph 5-9, Reference 1.m.

g. Classified information is disclosed to foreign government representatives only in accordance with the provisions of Reference 1.n.

h. An inspection of the rooms(s) is conducted at the conclusion of the meeting or conference (or at the end of each day of a multi-day event) to ensure all classified materials are properly stored.

APPENDIX N
INFORMATION PROCESSING EQUIPMENT PROCEDURES

1. There is a variety of non-COMSEC equipment used to process classified information, including copiers, facsimile machines, computers, notebooks, and other IT equipment and peripherals, typewriters, hand-held personal data managers, etc.

2. Any USAG, Fort Jackson equipment used to process classified information that may retain all or part of the classified information shall be identified and brought to the attention of the USAG, Fort Jackson Security Office.

3. Digital copiers, printers, scanners, faxes, and similar information system devices employ embedded hard drives or other media that may retain residual classified or sensitive information. These devices will be included as part of the certification and accreditation process.

4. Cleared and technically qualified personnel will inspect the equipment before the equipment is removed from protected areas.

5. Replaced equipment parts shall be destroyed per classification level when removed. When classified information cannot be removed, as an alternative, the equipment can be designated as classified and appropriately protected at the retained information's classification level, i.e., installed within a vault or open storage area approved for the storage of classified information at that classification level.

6. USAG, Fort Jackson agencies will establish security procedures to clearly identify all classified information processing equipment to include:

a. The overall level of classified information processed.

b. Temporary or permanent retention capabilities.

c. Procedures for safeguarding 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.

7. The Office Manager will approve, in writing, all stand alone, non-network facsimiles used for classified processing. Approval documentation will be posted on or near the facsimile along with the security procedures. Facsimiles not approved for classified use will bear the marking, "This equipment will not be used to process classified material."

APPENDIX O
RECEIPT OF CLASSIFIED INFORMATION (INCOMING/OUTGOING MAIL)

1. All sections will protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained in the mail. Screening points will be established to limit access to classified information.

2. USAG, Fort Jackson agencies will utilize the following procedures for the processing of classified information received through the mail.

a. Once classified material is identified, the section receiving the mail will immediately provide protection as required by the level of classification as identified in reference 1.m, until it can be secured in a classified information storage container. There are two classified storage containers located in the USAG, Fort Jackson; one at the Installation Operations Center, and one at the Directorate of Emergency Services.

b. The addressee of the material will be notified immediately of the receipt of the classified material.

c. The classified material will be logged into the classified document register using the next available control number available for the classification level of the material received.

d. A DA Form 3964, Classified Document Accountability Record, will be initiated and placed in the container with the classified material.

e. Once the addressee arrives to claim the classified material, ensure he/she has a valid DD Form 2501, Courier Authorization Card, and is listed on the Security Clearance Access Roster for the organization.

f. Complete the DA Form 3964, Section B (Routing), ensuring the person signs for the material being received.

g. Remind the addressee that all classified information will have to be returned to the location for security prior to the end of normal operating hours, unless the organization has their own classified information storage container.

APPENDIX P
ACCOUNTABILITY PROCEDURES

1. Top Secret Information/Material. Top Secret information will be provided continuous control and accountability. The following minimum requirements for Top Secret information will be met:

a. A Top Secret Control Officer (TSCO) and alternate will be designated within each organization if handling/maintaining Top Secret material. The TSCO and alternate are responsible for receiving, dispatching, and maintaining accountability and access records for Top Secret material.

b. The TSCO will possess the appropriate security clearance and access level equal to or higher than the information to be handled and be a minimum grade of GS-07 or rank of E-7. There is no minimum grade/rank for an alternate TSCO. In those cases where the minimum grade/rank requires a waiver, contact the USAG, Fort Jackson Security Office for details.

c. The TSCO will maintain a current, accurate system of accountability within their agency for all Top Secret material. Top Secret material will not be copied, transferred, destroyed, downgraded, or declassified without the written approval of the original classification authority/designated unit or activity TSCO. Upon approval, the TSCO will record the receipt, dispatch, downgrade, movement from one command element to another, current custodian, and destruction of all Top Secret material.

d. Top Secret material will be accounted for by a continuous chain of receipts. These receipts shall be maintained for five years. A DA Form 3964 (Classified Document Accountability Record) shall be utilized as the Top Secret accountability record form. The Top Secret material description will be consistent with that which appears within the approved document register.

e. Top Secret material will be inventoried at least once annually. The inventory will reconcile the Top Secret accountability register and records with 100 percent of the Top Secret material held.

f. For agencies that hold a large number of classified holdings, monthly 10 percent Top Secret inventories may be conducted to meet this annual requirement, as long as 100 percent reconciliation is accomplished. The 10 percent will be randomly selected. The inventory methods and results will be documented and retained on file.

g. The Top Secret inventory will be conducted by two properly cleared individuals. One will be the TSCO or alternate and the other person will be a disinterested party who is not a subordinate to either official.

APPENDIX P
ACCOUNTABILITY PROCEDURES (CONTINUED)

h. During the inventory, each Top Secret document/material will be physically examined for completeness. The TSCO will ensure the accountability record accurately reflects the material held. Any discrepancies that cannot be resolved immediately will be referred to the USAG, Fort Jackson Security Office for further investigation.

i. Before leaving the assigned organization, the TSCO or alternate will conduct a joint inventory with the new TSCO or alternate of all Top Secret material for which they have custodial responsibility. A 100 percent inventory of all Top Secret material is advised but not required. However, the new TSCO or alternate will be held accountable for all Top Secret material for which they have custodial responsibility.

2. Secret and Confidential Information/Material.

a. Secret and Confidential information/material originated, received, distributed, or routed to sub-elements at Fort Jackson will be protected by measures outlined in this policy and Reference 1.m.

b. USAG, Fort Jackson Secret and Confidential information will be kept to a minimum and retained for only as long as the information/material is needed.

c. Except for controlled/accountable Secret and Confidential information/material, such information/material may be transferred to organizations located on Fort Jackson without utilizing a DA Form 3964.

d. A DA Form 3964 will be utilized for Secret and Confidential information/material forwarded outside USAG, Fort Jackson, to include local agencies and contractors. This same form will be utilized when transmitting such information over secure facsimile devices.

e. The DA Form 3964 executed and returned by the recipient will be maintained for two years.

3. NATO and Foreign Government Material. Accountability requirements for NATO material are contained in Reference 1.n.

4. Working Papers.

a. Working papers are documents or materials, regardless of media, accumulated or created in the preparation of a finished product. Working papers containing classified information will be:

APPENDIX P
ACCOUNTABILITY PROCEDURES (CONTINUED)

(1) Dated when created.

(2) Conspicuously marked as "working papers" on the first page of the document in letters larger than the text.

(3) Marked with the highest classification of any information contained in the material.

(4) Protected IAW the assigned classification.

(5) Destroyed when no longer needed.

(6) Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when:

(a) Released by the originator outside the command or transmitted electronically or through message center channels within USAG, Fort Jackson.

(b) Retained for more than 180 days from the date of origin.

(c) Filed permanently.

b. Exceptions for accountability, control, and marking requirements for working papers containing Top Secret information will be forwarded to the USAG, Fort Jackson Security Office.

APPENDIX Q
REPRODUCTION PROCEDURES

1. Documents and other material containing classified information will be reproduced only when necessary for the accomplishment of USAG, Fort Jackson's mission or for compliance with applicable statues or directives.

2. The USAG, Fort Jackson Security Office will approve, in writing, all copiers used for the reproduction of classified material as well as the procedures for such copiers. Approval documentation and procedures will be posted on or near each approved copier.

3. Reproduction equipment which leaves latent images in the equipment or on other material will not be authorized to reproduce classified material unless:

a. The equipment is in an approved vault/open storage facility;

b. The equipment is protected as classified material; and

c. The material on which the image resides is destroyed as classified waste.

4. All copies of classified documents are subject to the same safeguards and controls prescribed for the document from which the reproduction is made. Reproduced material will be clearly identified as classified at the applicable level.

5. Waste products generated during reproduction will be properly safeguarded to the level of classification contained within until such time as it can be destroyed in an approved manner at the appropriate classification level.

6. Personnel who operate this equipment will be made aware of the risks involved with the specific equipment and the procedures concerning the protection, control, accountability, and destruction of reproduced classified information/material.

7. Except for the controlled initial distribution of information processed or received electronically, or that containing COMSEC or SCI which are governed by separate requirements, reproduction of Top Secret and NATO information will be strictly controlled.

8. Written authorization by the TSCO or USAG, Fort Jackson Security Office is required for the reproduction of Top Secret material. The Fort Jackson Security Office will obtain approval by the originator of the Top Secret material prior to its reproduction. Copies will then be numbered serially, marked to indicate its copy number, and accounted for accordingly.

APPENDIX Q
REPRODUCTION PROCEDURES (CONTINUED)

9. Equipment not approved for the reproduction of classified material shall bear the warning notice, "Warning: Reproduction of classified material with this equipment is prohibited." Stated prohibition against reproduction of information at any classification level will be strictly observed.

APPENDIX R
WAIVER PROCEDURES

1. Waivers to the requirements in Appendices P and Q, of this policy, are granted only on a case-by-case basis where there is a unique or unusual situation/factor requiring deviation from Reference 1.m, and this policy.

2. The alternative compensatory measure will be tailored to ensure the intent of the protection requirement has been fulfilled by other measures not addressed in established policy.

3. The alternative compensatory measure must show the protection is sufficient to reasonably deter and detect the loss or compromise of the classified information.

4. Deviations will be based on the consideration of risk management factors, i.e., criticality, sensitivity, information value, analysis of the known and anticipated threat, vulnerabilities to exploitation, and countermeasure benefits versus cost (monetary and to national security).

5. Waivers must be revalidated no less than every five years and will require rejustification of the unique or unusual circumstances.

6. Request for waivers will be submitted to the USAG, Fort Jackson Security Office for approval.

APPENDIX S
INSPECTION PROCEDURES

1. Self-Inspections.

a. Supervisors of sections involved in the management, storage, distribution, classification/declassification, and destruction of classified materials will conduct self-inspections within his/her area of responsibility involving such classified material. These inspections are to evaluate and assess the effectiveness and efficiency of the USAG, Fort Jackson Information Security Program.

b. Directorates will complete a self-inspection no later than the end of the first quarter annually. Self-inspection results will be forwarded to the USAG, Fort Jackson Security Office. Section Supervisors will maintain a copy of the self-inspection results until the next comparable inspection.

2. USAG, Fort Jackson Security Office Organizational Staff Assistance Visits (SAV), if requested by the agency.

3. USAG, Annual Inspection:

a. The USAG, Fort Jackson Security Office will conduct inspections no later than the fourth quarter, annually. USAG, Fort Jackson Security office will coordinate with supported agencies for inspection dates no later than the first quarter annually. USAG supported agencies will receive written notification of inspection dates at least 90 days prior to the inspection.

b. The USAG, Fort Jackson Security Office will forward a copy of annual inspection results to the organization's commander/supervisor and will maintain a copy of results until the next comparable inspection.

4. A sample SAV checklist is attached.

***US Army Garrison, Fort Jackson Information Security Program Checklist**	
ORGANIZATION:	
ORGANIZATION LOCATION:	
TYPE OF INSPECTION:	
POCs:	
UNIT SECURITY MANAGER/POC:	
ALTERNATE UNIT SECURITY MANAGER	
INFORMATION SECURITY POC:	
INSPECTION TEAM COMPOSITION:	
INFORMATION SECURITY PRIMARY:	
INFORMATION SECURITY ALTERNATE:	
OVERALL ASSESSMENT/COMMENTS:	

*This checklist was adapted from the IMCOM Information Security Program checklist			
	INFORMATION SECURITY PROGRAM AR 380-5	**ASSESS YES/NO/NA**	**REMARKS**
1.	**Reference Materials**		
	Does the organization maintain, at a minimum: a. DoD 5200.1, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification, 24 Feb 12.		
	b. AR 380-5, DA Information Security Program, 25 Mar 22.		
	c. AR 25-2, Army Cyber Security, 4 Apr 19.		
	d. AR 381-12, Threat Awareness and Reporting Program, 1 Jun 16.		
	e. AR 525-13, Antiterrorism, 3 Dec 19.		
2.	**Appointments and Authorizations**		
	a. Are courier cards accounted for and courier orders issued IAW AR 380-5, Paras 7-12(b)?		
	b. Are procedures in place to ensure the requirements for conducting classified meetings/ conferences accomplished properly? (AR 380-5, Para 5-15)		
3.	**Classified Document Control**		
	a. Are classified documents properly marked? -Overall markings -Portion markings -Declassification or downgrading instructions -Name of organization and date -Derivative sources or OCA -Reason for classification (DODI 5200.01, Volume 2, par 1-15(a))		

	b. Are Top Secret documents inventoried at least annually and are the documents maintained in a Top Secret Register for 5 yrs.? (AR 380-5, Para 5-18(b))		
	c. Are classified materials retained only as required for effective and efficient operations, or as required by law? (AR 380-5, Para 5-22(a))		
	d. Have specific reproduction equipment been designated for reproduction of classified information and are procedures posted? (AR 380-5, Para 5-21(b))		
	e. Are working papers dated, safeguarded, and either destroyed or finalized after 180 days? (AR 380-5, Para 5-20)		
4.	**Security Container Control**		
	a. Are security container combinations changed when placed in service, when persons no longer require access or are reassigned, when a combination may have been compromised, or when taken out of service? (AR 380-5, Para 6-8(c))		
	b. Is SF 700 posted within each vault, secure room, and security container indicating individuals having knowledge of the combination, and is it placed in an opaque envelope marked "Security Container Information?" (AR 380-5, Para 6-8(d)(1))		
	c. Is the SF 702 being filled out properly, indicating each time the security container is opened or closed, or when a container is not opened during a workday? (AR 380-5, Para 5-9(b))		
	d. Are end of day security checks conducted and recorded on a SF 701?		

	(AR 380-5, Para 5-10)		
	e. Is there an Emergency Evacuation and Destruction Plan posted on or near each container? Has the plan been rehearsed? (AR 380-5, Para 5-11)		
	f. Are magnetic signs indicating when the container is opened or closed located on the front of each security container? (AR 380-5, Para 5-9(c))		
	g. Has each security container designated for classified storage been assigned a number or symbol? (AR 380-5, Para 6-8(a))		
	h. Are the tops of security containers free of any extraneous materials? (AR 380-5, Para 6-8(a))		
	i. Are security containers ready for turn-in inspected for any leftover classified material, and are the combinations reset to the factory set combination (50-25-50)? (AR 380-5, Para 6-8(c)(4) and 6-11)		
5.	**Transmission Controls**		
	a. Are classified couriers briefed on their responsibilities before being assigned a courier card (DD Form 2501)? (AR 380-5, Para 7-12(a))		
	b. Are issued courier cards only valid for 2 years or less? Are requirements for authorization to handcarry classified materials reevaluated biennially? (AR 380-5, Para 7-12(b)(4))		
	c. Do personnel understand the proper controls in the preparation of transmitting classified materials, i.e., double wrapping, addressing, and shipment methods? (AR 380-5, Paras 7-8)		

	d. Is a courier authorization letter given to each classified courier traveling aboard a commercial passenger aircraft? (AR 380-5, Para 7-13(c))		
	e. Is a foreign travel briefing given to all DA military and civilians within 6 month of departure to an overseas area? (AR 380-67, Para 9-9)		
6.	**Destruction Controls**		
	a. Are approved methods being utilized for the destruction of classified material? (AR 380-5, Para 3-17)		
	b. Are records of destruction (DA Form 3964) being utilized when destroying Top Secret, NATO Secret, and foreign government materials? (AR 380-5, Para 5-24)		
	c. Are destruction records maintained for 5 years? (AR 380-5, Para 5-18(b))		
7.	**Violations and Infractions**		
	a. Are possible and actual security violations being reported immediately to the DCS, G-2 (DAMI-CD)? (AR 380-5, Para 9-2)		
	b. Are preliminary inquiries conducted IAW AR 380-5, Para 9-3?		
	c. Are debriefings conducted in cases of unauthorized access? (AR 380-5, Para 9-7)		
8.	**Security Education and Awareness**		
	a. Are initial briefings being conducted before access is granted to classified? (AR 380-5, Para 8-3)		
	b. Are all DA personnel provided refresher training at least once a year? (AR 380-5, Para 8-4)		
	c. Are debriefings being conducted IAW AR 380-5, Para 5-5?		

	d. Are security education program records and the listings of the participants maintained for 2 years? (AR 380-5, Appendix B, Para B-4(k)(14))		
	e. Are all DA personnel receiving TARP training at least annually? (AR 381-12, Para 2-4(a))		

APPENDIX T
STORAGE PROCEDURES

1. Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked, GSA-approved security container, vault, or secure room/area, pursuant to the level of classification and Reference 1.m.

2. Top Secret information will be stored as follows:

a. GSA-approved security container with one of the following supplemental controls:

(1) An employee cleared to at least the Secret level, will inspect the security container once every two hours, but not in a way that indicates a pattern.

(2) The location that houses the security container is protected by an Intrusion Detection System (IDS), meeting the requirements of section III, Chapter 6, Reference 1.m, with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

b. In a GSA approved container equipped with a lock meeting Federal Specification FF-L-2740, provided the container is located within an area that has been determined to have security in depth.

c. In an open storage area (also called a secure room) constructed in accordance with section III, Chapter 6, Reference 1.m, and equipped with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area has been determined to have security in depth; or within five minutes of alarm annunciation if it has not.

d. In a vault, or GSA approved modular vault, meeting the requirements of Federal Standard (FED-STD) 832 as specified in section III, Chapter 6, Reference 1.m.

3. Secret information will be stored by one of the following methods:

a. In the same manner as prescribed for Top Secret information.

b. In a GSA-approved security container or modular vault, or vault built to FED-STD 832 without supplementary controls.

c. In an open storage area meeting the requirements of this regulation, provided that security in depth exists, and one of the following supplemental controls is used:

APPENDIX T
STORAGE PROCEDURES (CONTINUED)

(1) An employee cleared to at least the Secret level will inspect the open storage area once every four hours.

(2) An IDS meeting the requirements of section III, Chapter 6, Reference 1.o, with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

4. Confidential information will be stored in the same manner as Top Secret or Secret information except that supplemental controls are not required.

5. Specialized Security Equipment.

a. GSA-approved field safes and one and two drawer, light-weight, GSA-approved security containers are used primarily for storage of classified information in the field and in military platforms, and will be used only for those or similar purposes. These containers will use locks conforming to Federal Specification FF-L-2740 or FF-L-2937 as required by Federal Specification AA-F-358. Special size containers will be securely fastened to the platform; field safes will be under sufficient control and surveillance when in use to prevent unauthorized access or loss.

b. GSA-approved map and plan files are available for storage of odd sized items such as computer media, maps, charts, and classified equipment.

c. GSA approved modular vaults, meeting Federal Specification AA-V-2737, can be used to store classified information as an alternative to vault requirements as described in section III, Chapter 6, Reference 1.m.

6. Unrelated unclassified documents or equipment, i.e., cash, keys, jewelry, will not be stored in security containers in which classified material is stored.

7. Residential Storage. Classified information will not be stored in a personal residence, on or off Fort Jackson. Classified information will not be stored in any location outside an approved U.S. Government location or cleared contractor facility. Exceptions follow:

a. In extreme and exceptional situations, the Commander, USAG, Fort Jackson, may approve an exception for the storage of Secret and below classified material. Requests for exception to policy by USAG, Fort Jackson employees, will be submitted through the USAG, Fort Jackson Security Office.

APPENDIX T
STORAGE PROCEDURES (CONTINUED)

b. The Secretary of the Army is the only DA official that can authorize the removal of Top Secret materials from designated work areas for temporary storage outside a government or cleared contractor facility, to include the storage at a personal residence on a government facility.

8. Equipment Designations.

a. There will be no external markings that reveal the level of classified information authorized to be stored in a security container, vault, or secure area/room. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of the storage container, vault, or secure area/room.

b. For identification/inventory purposes, each vault, container, and secure room will bear an external, assigned number. Section supervisors having approved security containers, vaults, and/or secure rooms are responsible for assigning such identification numbers, maintaining a current inventory, and providing a copy of the inventory and any updates to the USAG, Fort Jackson Security Office.

c. The assigned number, the SF 702, the "open-closed" or "open-locked" signs, and the emergency evacuation and destruction plan are the only items permitted on the exterior of the security container.

d. The top of the security container will not be used as a bookshelf or paper storage area.

9. Security Combinations.

a. Combinations to security containers, vaults, and secure rooms will be changed only by authorized individuals assigned that responsibility.

b. Combinations will be changed:

(1) When placed in use.

(2) Whenever an individual knowing the combination no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

(3) When the combination has been subject to possible compromise.

APPENDIX T
STORAGE PROCEDURES (CONTINUED)

(4) When taken out of service. In such instances, combination locks will be reset to the standard combination 50-25-50, and padlocks will be reset to the standard combination 10-20-30.

c. A record will be maintained for each vault, secure room, and GSA-approved container used for storing classified information showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. A SF 700 (Security Container Information) shall be utilized for this purpose.

(1) Type or write in non-erasable ink all entries on the SF 700.

(2) Complete Part 1 and Part 2A, SF 700. Include the name and signature of the person making the combination change in Item 9, Part 1.

(3) Part 1, SF 700, will be posted on the inside of the lock drawer of the security container or on the inside of authorized vault and secure room doors in an enclosed opaque envelope marked "security container information."

(4) Parts 2 and 2A, SF 700, will be marked with the highest classification of material stored in the container.

(5) Part 2A, SF 700, will be detached and inserted in the envelope. Part 2A, SF 700, used to record a Top Secret combination, will be accounted for in the same manner as other Top Secret documents.

(6) For two-person control material, only Part 1, SF 700, will be completed for security containers. Parts 2 and 2a need be used only if there is a specific need for recording the combination.

(7) Once Part 2A, SF 700, is detached and inserted in the envelope, the envelope will be sealed. Part 2, SF 700, will then be marked with the classification markings of the highest material stored in the container, and will be stored in a secure container located at the next higher level within the organization.

(8) If the next higher level does not have storage capability, contact the USAG, Fort Jackson Security Office for further guidance. Top Secret combinations will be stored in a separate security container approved for the storage of Top Secret materials.

APPENDIX T
STORAGE PROCEDURES (CONTINUED)

(9) New combinations will be tested several times before locking the security container, vault door, or secure room door to avoid the expense of a lock-out.

10. Repair of Damaged Security Containers.

a. Neutralization and repair of a security container or door to a vault approved for storage of classified information will be accomplished only by appropriately cleared or continuously escorted U.S. personnel specifically trained in the methods specified by reference FED-STD 809.

b. Neutralization or repair by, or using, methods and procedures other than described in FED-STD 809 is considered a violation of the security container's or vault door's security integrity, and the GSA label shall be removed. Thereafter, the containers or doors may not be used to protect classified information until repaired per FED-STD 809, inspected by a qualified inspector, and certified for use in writing.

11. Maintenance and Operating Inspections.

a. Section supervisors will schedule periodic maintenance for security containers and vault/secure room doors to detect and correct any problems in their early stages and define symptoms of developing problems.

b. It is important to never use force to try to correct the problem. Critically needed materials should not be stored in containers showing any of the following symptoms, since they cannot be depended upon to open again:

(1) A dial that is unusually loose or difficult to turn.

(2) Any jiggling movement in the dial ring. This is often detected when a twist motion is applied to the dial.

(3) Difficulty in dialing the combination or opening the container.

(4) Difficulty with the control drawer or other drawers. Examples are as follows:

(a) Drawers rubbing against container walls. This can be caused if the container is not leveled, or the tracks or cradles are not properly aligned.

APPENDIX T
STORAGE PROCEDURES (CONTINUED)

(b) Problems with opening or closing drawers because the tracks or cradles need lubricant, material is jammed in behind the drawer, or the internal locking mechanism is tripped.

(5) Difficulty in locking the control drawer. Examples are as follows:

(a) The control drawer handle or latch will not return to the locking position when the drawer is shut.

(b) The locking bolts move roughly, slip, or drag, or the linkage is burred or deformed.

(6) GSA approved labels are missing or in need of replacement. If missing, contact the DoD lock program to obtain information on retaining an authorized inspector. GSA approved security containers and vault doors must have a GSA approved label or a GSA recertification label on the front of the equipment in order to store classified information.

12. Turn-In or Transfer of Security Equipment.

a. In addition to having combinations reset before turn-in, security equipment will be inspected before turn-in or transfer by the USAG, Fort Jackson Security Office to ensure classified material is not left in the container.

b. Each security container drawer will be removed and the interior inspected to ensure all papers and other material are removed and the container is completely empty.

c. Shredders, other classified material destruction devices, copiers, and facsimiles used for the reproduction and transmission of classified information, and furniture located within authorized vaults and secure rooms will be thoroughly inspected by the USAG, Fort Jackson Security Office prior to turn-in or transfer to ensure no classified material remains.

d. A written, signed record certifying above inspection has been accomplished and that no classified material remains will be retained by the USAG, Fort Jackson Security Office for two years.

APPENDIX U
PHYSICAL SECURITY STANDARDS

1. Detailed physical security standards for areas requiring the open storage of classified information are contained in Section III, Chapter 6, Reference 1.m, to include:

a. Construction standards.

b. IDS standards.

c. Access control requirements.

2. Open storage areas will only be approved when storage in other approved security containers is not feasible due to the size, shape, or volume of material stored.

3. Requests for open storage inspections shall be forwarded to the Fort Jackson Provost Marshal Physical Security Office.

4. Upon completion of the inspection, section supervisors will forward to USAG, Fort Jackson Security Office the following information:

a. Justification.

b. Construction standards.

c. IDS system standards, if required.

d. Open storage inspection results.

5. Section supervisors will ensure written security controls and procedures are in place to properly protect classified material and sufficiently deter, detect, delay, or deny unauthorized penetration into the secure area.

6. The USAG, Fort Jackson Security Office will provide open storage certifications to those areas meeting regulatory requirements. Certifications are valid for five years or until structural modifications are made to the area, whichever comes first. Open storage certifications will immediately terminate if structural modifications are made that degrade security.

7. Section supervisors will coordinate with the USAG, Fort Jackson Security Office and the Fort Jackson Provost Marshal Physical Security Office on new construction and upgrades to existing facilities involving the open storage of classified equipment or the

APPENDIX U
PHYSICAL SECURITY STANDARDS (CONTINUED)

certification of classified meeting sites to ensure all applicable security requirements are incorporated into the initial planning.

8. Requests for deviations to open storage construction requirements will be forwarded to the USAG, Fort Jackson Security Office for approval. Requests will include justification and proposed compensatory systems, controls, or procedures to properly protect classified information.

APPENDIX V
TRANSMISSION PROCEDURES

1. Authorized transmission procedures for each level of classified information follow:

a. Top Secret Information.

(1) Direct contact between appropriately cleared persons.

(2) Electronic means over an approved secure communications system. This applies to voice, data, message, and facsimile transmissions.

(3) The Defense Courier Division (DCD) if the material qualifies under the provisions of DODI 5200.33.

(4) Authorized command courier or messenger services.

(5) The DOS diplomatic Courier Service.

(6) Appropriately cleared U.S. Military and U.S. Government Civilian personnel, specifically designated to carry the information and traveling by surface transportation, or traveling on scheduled commercial passenger aircraft within and between the U.S., its territories, and Canada.

(7) Appropriately cleared U.S. Military and U.S. Government Civilian personnel, specifically designated to carry the information and traveling on scheduled commercial passenger aircraft on flights outside the U.S., its territories, and Canada.

(8) DoD contractor employees with the appropriate clearances traveling within and between the U.S., and its territories, when the transmission has been authorized, in writing, by the appropriate Cognizant Security Agency (CSA), or a designated representative.

b. Secret Information.

(1) Any of the means approved for transmission of Top Secret information.

(2) U.S. Postal Service registered mail, within and between the U.S., the District of Columbia, and the Commonwealth of Puerto Rico.

(3) U.S. Priority Mail Express (formerly referred to as Express mail) within and between the 50 states, District of Columbia, and the Commonwealth of

APPENDIX V
TRANSMISSION PROCEDURES (CONTINUED)

Puerto Rico. The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed under any circumstances. The use of external (street side) express mail collection boxes is prohibited.

(4) U.S. Postal Service and Canadian registered mail with registered mail receipt between U.S. Government and Canadian Government installations in the U.S. and Canada.

(5) U.S. Postal Service registered mail through Military Postal Service facilities outside the U.S. and its territories if the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection.

(6) As an exception, in urgent situations requiring next-day delivery within the U.S. and its territories, commanders may authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations in accordance with chapter I of Title 39, C.F.R. are met. Any such delivery service will be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract will require cooperation with U.S. Government inquiries in the event of a loss, theft, or possible compromise. The sender is responsible for ensuring that an authorized person at the receiving end is aware that the package is coming and will be available to receive the package, verifying the mailing address is correct, and confirming (by telephone or e-mail) that the package did in fact arrive within the specified time period. The package may be addressed to the recipient by name. The release signature block on the receipt label will not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified COMSEC, NATO information, SCI, and FGI will not be transmitted in this manner. See Multiple Award Schedule 48, (Transportation, Delivery and Relocation Solutions), on the GSA eLibrary website at https://www.gsaelibrary.gsa.gov/elibmain/home.do for a listing of commercial carriers authorized for use under the provisions of this paragraph.

(7) Carriers authorized to transport Secret information by way of a Protective Security Service (PSS) under the National Industrial Security Program (NISP). This method is authorized only within CONUS when other methods are impractical, except that this method is also authorized between U.S. and Canadian government approved locations documented in a transportation plan approved by U.S. and Canadian government security authorities.

APPENDIX V
TRANSMISSION PROCEDURES (CONTINUED)

(8) Appropriately cleared contractor employees, provided that the transmission meets the requirements specified in DODM 5220.22, Volume 2 and DoD 5220.22-M.

(9) U.S. Government and U.S. Government contract vehicles including aircraft and certain ships.

c. Confidential information may be transmitted by any of the means approved for Secret information. However, U.S. Postal Service registered mail will only be used for Confidential material in certain instances. Refer to paragraph 7-5, Reference 1.m, for details.

2. The DD Form 2501 (Courier Authorization) may be used to identify appropriately cleared DA personnel who have been approved to hand-carry classified material in accordance with the following:

a. The individual has a **recurrent** need to hand-carry classified information.

b. The form is signed by an appropriate official in the USAG, Fort Jackson Security Office.

c. Stocks of the form are controlled to preclude unauthorized use.

d. The form is issued no more than two years at a time. The requirement for authorization to hand-carry will be reevaluated and/or revalidated on at least a biennial basis, and a new form issued, if appropriate.

3. COMSEC material will be transmitted IAW Reference 1.o.

4. Prior to releasing any classified information to a foreign government, coordinate with the IMCOM Foreign Disclosure Office.

5. Preparation of Material for Transmission.

a. When classified information is transmitted, two opaque, sealed envelopes, wrappings, or containers durable enough to properly protect the classified information from accidental exposure and to ease in detecting tampering will be utilized.

b. Documents will be packaged so classified text is not in direct contact with the inner envelope or container.

APPENDIX V
TRANSMISSION PROCEDURES (CONTINUED)

6. Addressing.

a. The outer envelope or container for classified material:

(1) Will be addressed to an official government activity or to a DoD contractor with a verified facility clearance and appropriate storage capability.

(2) The outer envelope/container will not be addressed to an individual.

(3) Will show the complete return address of the sender.

(4) Will not bear a classification marking or any unusual marks that might invite special attention to the fact that the contents are classified.

b. The inner envelope or container will show the address of the receiving activity, the address of the sender, and the highest classification of the contents and any special markings. The "attention line" may have a person's name.

APPENDIX W
HANDCARRYING CLASSIFIED MATERIAL PROCEDURES

1. Appropriately cleared personnel may be authorized to escort or hand-carry classified material between locations when other means of transmission or transportation cannot be used.

2. Hand-carrying of classified material will be limited to situations of absolute necessity and will be carried out to make sure it does not pose an unacceptable risk to the information. Generally, two-way hand-carrying (carrying the material to and from the destination) is not authorized unless specific justification is provided.

3. Hand-carrying will be authorized only when:

a. The information is not available at the destination and is required by operational necessity or a contractual requirement.

b. The information cannot be sent by a secure facsimile transmission or by other secure means, i.e., Federal Express mail.

c. The hand-carry has been authorized by the appropriate official in writing.

d. The hand-carry is accomplished aboard a U.S. carrier or a foreign carrier if no U.S. carrier is available, and the information will remain in the custody and physical control of the U.S. escort at all times.

e. Arrangements have been made in advance for secure storage during overnight stops and similar periods. The material will not be stored in hotels, personal residences, vehicles, or any other unapproved storage location.

f. A receipt for the material, for all classification levels, is obtained from an appropriate official at the destination and a copy of the receipt is returned to the USAG, Fort Jackson Security Office.

4. DD Form 2501 (Courier Authorization Card).

a. The DD Form 2501 will be used to identify appropriately cleared USAG, Fort Jackson military and Civilian personnel who are authorized to hand-carry classified material within CONUS, except when utilizing commercial aircraft. The USAG, Fort Jackson Security Office or designated individual will issue a DD Form 2501 when:

(1) An individual has a **recurrent** need to hand-carry classified information.

APPENDIX W
HANDCARRYING CLASSIFIED MATERIAL PROCEDURES (CONTINUED)

(2) An individual has acknowledged receiving a courier briefing (sample at Attachment 1).

(3) The DD Form 2501 is completed and signed by the USAG, Fort Jackson Security Office.

b. The DD Form 2501 is good for two years. The requirement for authorization to hand-carry will be reevaluated and/or revalidated biennially prior to a new form being issued.

c. Contractor employees who are required to hand-carry classified information will coordinate with the contractor Security Officer and the respective Security Manager for issuance of an authorization letter, courier letter, or courier card.

5. Courier authorization orders (see sample -Attachment 2) will be provided by the USAG, Fort Jackson Security Office for the hand-carrying or escorting of classified material within CONUS utilizing commercial aircraft when:

a. The Security Office has received a written justification for the need to hand-carry or escort classified information.

b. The individual has acknowledged receiving a courier briefing.

c. The individual is in possession of a DoD identification card.

d. Advance coordination with appropriate authorities has been made, i.e., overnight storage when appropriate, Federal Aviation Administration (FAA), transshipping activities for shipment of bulky materials.

6. For Operations Security purposes, courier authorization orders will not stipulate that the courier is hand-carrying classified material, only that the courier is authorized to hand-carry certain items, i.e., laptop computer with CDROM/3.5 media drives, computer power and connectivity accessories, media storage devices, paper documentation, maps.

7. Security requirements outlined in Para 7-11 through Para 7-13, Reference 1.m, will be strictly enforced and approved by the USAG, Fort Jackson Security Office when an individual is required to hand-carry classified information outside the United States.

APPENDIX W
HANDCARRYING CLASSIFIED MATERIAL PROCEDURES (CONTINUED)

8. Blanket courier authorizations are not authorized.

Courier Authorization Briefing
To Hand-carry/Escort Classified Material (Sample)

1. General Instructions.

a. As a designated courier of classified material, you are authorized to hand-carry or escort material. Upon receipt of the classified material, you become, as defined in AR 380-5, Army Information Security Program, the custodian of that information.

b. 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 protection of the 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 address.

c. 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 with special emphasis on the following areas:

(1) Access.

(a) You will be given delivery instructions for the material when it is released to you. Follow those specific instructions given and seek assistance from your Security Office if you are unable to do so.

(b) Dissemination of classified material is restricted to those persons who are properly cleared and have an official need for the information. No person has a right or is entitled to access of classified information solely by virtue of rank or position.

(c) To help prevent unauthorized access and possible compromise of 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.

(2) Storage.

(a) 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 in commercial airlines passenger storage compartments and while aboard trains or buses.

Courier Authorization Briefing
To Hand-carry/Escort Classified Material (Sample Continued)

(b) 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.

(c) Retention of classified material in hotel/motel rooms or personal residences is specifically prohibited. Safety deposit boxes provided by hotels/motels do not provide adequate storage for classified material.

(d) Advance arrangements for proper overnight storage at a U.S. government facility or, if in the United States, a cleared contractor's facility are required prior to departure. Arrangements are the responsibility of the activity authorizing the transmission of classified material.

(3) Preparation.

(a) Whenever you transport classified information, it must be enclosed in two opaque sealed envelopes, similar wrappings, or two opaque sealed containers such as boxes or other heavy wrappings without any metal bindings/clips.

(b) A briefcase, when used, will not serve as an outer wrapping or container. 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.

(c) 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.

(d) If the classified material is to be retained by the official government activity you are visiting, a DA Form 3964 (Classified Document Accountability Record) will be completed, and a copy will be returned to your Security Office.

(4) Hand-carrying.

(a) The Courier Authorization and a picture ID should ordinarily permit you to pass through airport passenger control points within the U.S. without the need for subjecting the classified material to inspection.

Courier Authorization Briefing
To Hand-carry/Escort Classified Material (Sample Continued)

(b) If you are carrying classified material in envelopes, you should process through the ticketing and boarding procedures in the same manner as other passengers. The sealed envelope shall be routinely offered for inspection for weapons. The screening official may check the envelope by X-ray machine, flexing, feel, weight, etc., without opening the envelope.

(c) If the screening official is not satisfied with your identification, authorization statement, or envelope, 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 envelopes or read any portion of the classified document as a condition for boarding.

(5) Escorting.

(a) When escorting classified material that is sealed in a container and too bulky to hand-carry or is exempt from screening, prior coordination is required with the Federal Aviation Authority (FAA) and the airline involved.

(b) This coordination is the responsibility of the approving authority. You will report to the airline ticket counter prior to starting your boarding process. If satisfied, the official will provide an escort to the screening station and exempt the container from physical or other type inspection.

(c) 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.

(d) 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.

(e) Appropriately cleared personnel will be available to assist in surveillance at any intermediate stop when the plane loads and the cargo compartments are to be opened. Coordination for assistance in surveillance is the responsibility of the activity authorizing the transmission of the material.

Courier Authorization Briefing
To Hand-carry/Escort Classified Material (Sample Continued)

2. 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 protect official national security information.

3. You are reminded any classified instructions you receive must also be protected. Do not discuss verbal instructions with anyone not having a need-to-know, i.e., do not talk about where you were, what you did, or what you saw.

4. If you have questions at any time concerning the security and protection of classified and sensitive material entrusted to you, contact your USAG, Fort Jackson Security Office.

Courier Certificate (Sample)

As a designated courier of classified material, I, _____ received a briefing on _____. The briefing outlined my responsibilities as a courier, duties as a custodian, and the safeguard and protection of classified information. I am cognizant of the provisions and restrictions imposed by Chapter 7, AR 380-5, and intend to comply unless prevented by an outside force which I cannot control. I fully understand 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, i.e., secure facsimile transmission or Federal Express mail.

_____
Designated Courier

_____
Date

_____
Staff Security Manager

- S A M P L E -

CUI

(Insert Letterhead)

(Office Symbol) (300A) (Date)

MEMORANDUM FOR (Insert Courier's Name, Organization, and Full Address)

SUBJECT: CONUS Courier Authorization

1. The following (Insert Organization Name) individual is authorized to hand-carry (Insert Organization Name) (Insert item(s) to be hand-carried, i.e., laptop computer with CDROM/3.5 media drives, computer power and connectivity accessories, media storage devices, documentation, maps) to/from (Insert Destination):

Name	Rank/Grade	Identification Type and Number
(Insert Name)	(Insert Rank/Grade)	(Insert ID Type and Number)

2. The complete itinerary is enclosed.

3. This authorization is valid for above named individual through (Insert TDY End Date).

4. The destination point of contact is (Insert Destination POC Name, Phone Number, and Email Address).

5. The point of contact is the undersigned, (Insert Phone Number, and Email Address).

Encl (Insert Security Manager Signature Block)

CUI

- SA M P L E –

CUI

CONUS COURIER AUTHORIZATION ITINERARY
(Insert Dates)

DATE	DEPART	ARRIVE	AIRLINES	FLIGHT	TIME
(Insert All Dates, Departures, Arrives, Airlines, Flight Numbers, and Times - Example Below)					
15 Sep 04	Fort Monroe, VA				1700
15 Sep 04		Norfolk, VA			1800
15 Sep 04	Norfolk, VA		Delta Airlines	879	1925
15 Sep 04		Atlanta, GA			2111
15 Sep 04	Atlanta, GA		Delta Airlines	938	2155
15 Sep 04		Nashville, TN			2200
16 Sep 04	Nashville, TN		Delta Airlines	4571	1950
16 Sep 04		Atlanta, GA			2158
16 Sep 04	Atlanta, GA		Delta Airlines	4564	2253
16 Sep 04		Norfolk, VA			0027
16 Sep 04	Norfolk, VA				0100
16 Sep 04		Fort Monroe, VA			0200

APPENDIX X
UNAUTHORIZED DISCLOSURE PROCEDURES

1. The compromise of classified information can cause damage to our national security. Loss of classified material is just as serious. When one or both of these occur, immediate action is required to minimize any damage and eliminate any conditions that might cause further compromises.

2. Prompt and effective investigation of the situation and prompt reporting of results are critical to minimize/eliminate further compromises. Each incident must be the subject of a preliminary inquiry to:

a. Determine whether classified information was compromised and, if so, whether there is damage to the national security.

b. Determine the persons, situations, and/or conditions responsible for or which contributed to the incident.

3. Incident Discovery.

a. Anyone finding classified material out of proper control, will take custody of and safeguard the material and immediately notify their supervisor or the USAG, Fort Jackson Security Office.

b. Any person who becomes aware of the possible loss or compromise of classified information will immediately report it to their supervisor or the USAG, Fort Jackson Security Office during duty hours or the Fort Jackson Emergency Operations Center after duty hours.

c. If classified information appears in the public media, personnel will not make any statement or comment that would confirm the accuracy or verify the classified status of the information and will immediately report it to the USAG, Fort Jackson Security Office.

d. Any incident in which the deliberate compromise of classified information or involvement of foreign intelligence agencies is suspected will be reported to the USAG, Fort Jackson Security Office.

4. Preliminary Inquiry.

a. When an incident of possible loss or compromise of classified information is reported, a preliminary inquiry will be initiated. If the information was in the custody of another activity at the time of the possible compromise, that activity will be notified and will assume responsibility for the preliminary inquiry.

APPENDIX X
UNAUTHORIZED DISCLOSURE PROCEDURES (CONTINUED)

b. Examples of instances that will be reported include, but are not limited to, the following:

(1) Top Secret documents lost to accountability.

(2) Security container open and unattended.

(3) Classified documents left unsecured and unattended.

(4) Disclosure of classified information to a person not authorized access.

(5) Appearance of classified material in public media.

(6) Classified information discussed or sent over an unsecured means of communication or processed on an IT system not approved for classified processing.

c. A person not involved directly or indirectly with the incident will be appointed to conduct the preliminary inquiry. This person will have the appropriate security clearance, the ability and available resources to conduct an effective inquiry, and will conduct the inquiry according to the guidelines outlined in Para 6(d), Reference 1.f.

d. The Section supervisor will ensure the preliminary inquiry is promptly and properly completed, the results are reported to the USAG, Fort Jackson Security Office within 10 working days from the date of discovery (extensions may be granted), and corrective actions are implemented.

e. The appointing authority will forward the following information to the USAG, Fort Jackson Security Office:

(1) The completed preliminary inquiry with written concurrence/non-concurrence.

(2) The findings and recommendations of the inquiry.

(3) Proposed corrective actions.

(4) The determination of whether additional investigation is warranted, i.e., AR 15-6.

APPENDIX X
UNAUTHORIZED DISCLOSURE PROCEDURES (CONTINUED)

5. Preliminary Inquiry Results. If, at the conclusion of the preliminary inquiry, it appears a compromise of classified information could have occurred, or did occur, and damage to national security can result, the Section Supervisor will:

a. Notify the originator of the information/material involved;

b. Report the matter to the USAG, Fort Jackson Security Office; and

c. Maintain a copy of the entire preliminary inquiry for a minimum of two years.

6. Unauthorized Access. In cases where a person has had unauthorized access to classified information, the individual concerned may receive a debriefing and sign a statement acknowledging the debriefing and their understanding of its contents.

7. Unauthorized Absences, Suicides, Incapacitation, or Revocation of a Security Clearance. The USAG, Fort Jackson Security Manager will be immediately notified of any of these incidents where military or civilian personnel have had access to classified information.

APPENDIX Y
SECURITY EDUCATION

1. The USAG, Fort Jackson Security Office is responsible for providing Security Education, Training, and Awareness (SETA) to USAG, Fort Jackson employees. SETA is aimed at promoting quality performance of security responsibilities by personnel to:

a. Provide the necessary knowledge and information to enable quality performance of security functions.

b. Promote an understanding of Information Security Program policies and requirements and their importance to the national security.

c. Instill and maintain continuing awareness of security requirements.

d. Assist in promoting a high degree of motivation to support USAG, Fort Jackson mission and goals.

2. Periodic briefings, training sessions, formal presentations, video tapes, computer-generated security training, and published articles may be used in providing SETA.

3. Initial orientations will be provided to all personnel who could be expected to play a roll in the Information Security Program and/or have an IT account, i.e., electronic mail. Newly assigned personnel will be given an initial security briefing within 30 days of their arrival date.

4. As a minimum, all DA employees, especially those who have access to, create, process, or handle classified/sensitive information, will be provided refresher training at least once a year, i.e. TARP/OPSEC/INFOSEC.

5. All personnel will execute a SF 312 (Classified Information Nondisclosure Agreement) and have the appropriate security clearance prior to having access to classified information.

6. As required by Reference 1.r, Anti-Terrorism/Force Protection (AT/FP) Level 1 training will be provided annually by each organization's AT/FP Officer for all military and civilian personnel. Soldiers, family members and DOD employees who travel OCONUS as a result of PCS, TDY, or Leave/Pass will receive an area-specific briefing prior to departure from home station. This training will be provided by the USAG, Fort Jackson Security Office.

APPENDIX Y
SECURITY EDUCATION (CONTINUED)

7. Special briefings, i.e., NATO, Critical Nuclear Weapons Design Information (CNWDI), will be provided by the USAG, Fort Jackson Security Office.

8. All personnel having access to classified information will receive a security debriefing prior to his/her PCS, ETS, retirement, etc.

9. The USAG, Fort Jackson Security Office will maintain records of SETA Programs to include attendee lists for two years.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT

1. The purpose of the Industrial Security Program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of government. The national security also requires that our industrial security program promote the economic and technological interests of the United States.

2. The objective of this policy is to provide USAG, Fort Jackson employees, contracting offices, logistics management divisions, and any other affected offices with basic security-related procedures for implementing specific aspects of the USAG, Fort Jackson industrial security program.

3. Responsibilities.

a. USAG, Fort Jackson Security Office.

(1) Monitor and implement security procedures to protect against unauthorized disclosure of classified national security information.

(2) Designate, in writing, an Industrial Security Specialist who will implement the USAG, Fort Jackson's Industrial Security Program as part of his/her area of responsibility.

(3) Provide guidance to USAG employees, contracting offices, logistics management specialists on contractor and industrial security policies and procedures.

(4) Review contracts that include requirements for contractors to have access to classified information, and ensure a clause is present requiring the appropriate level of personnel clearances to be initiated at the Contractor Facility.

(5) Ensure classified contracts contain a clause requiring classified visits to be prepared in accordance with the National Industrial Security Program Operating Manual (NISPOM) and certified by the USAG, Fort Jackson Security Office prior to forwarding to the organization to be visited.

(6) Review DD Form 254, Contract Security Classification Specification, for all USAG, Fort Jackson classified contracts.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT (CONTINUED)

(7) Notify the Contracting Officer, in writing, of any contractor employee found unsuitable for access to USAG facilities, sensitive information, and/or resources and request action to deny such access.

(8) Consult with the Contracting Officer and direct appropriate action to be taken whenever any information is received which raises a question about a contractor's suitability.

(9) Maintain records of contractor-certified visit requests for visits by foreign nationals and immigrant aliens to USAG facilities.

(10) Periodically evaluate the Industrial Security Program to ensure it is operating effectively.

b. Contracting Office. The contracting office will:

(1) Ensure all new, modified, or renewed USAG contracts, including, but not limited to, purchase orders, consulting agreements, and MOA's containing work, services, or other duties to be performed or provided by contractor employees have been coordinated with the USAG Security Office for review and determination of applicable personnel security investigative requirements prior to solicitation. Additionally, ensure the USAG Security Office is notified whenever the status of a contract changes (i.e., replaced, defaulted, terminated, etc.) impacting personnel security requirements and/or access to USAG, Fort Jackson facilities, sensitive information, and/or resources.

(2) Ensure all proposed contracts requiring contractor employees or other persons not employed by the USAG, Fort Jackson to have access to classified information contain language that clearly identifies this requirement prior to solicitation in coordination with the USAG, Fort Jackson Security Office.

(3) Review all proposed contracts to determine whether the USAG, Fort Jackson will need to share classified information with a contractor, consultant or other non-USAG persons during pre-contract negotiations.

(4) Coordinate with the appropriate Defense Security Service (DSS) office to determine if any prospective bidders require processing for a security clearance in accordance with the NISPOM and/or other applicable DoD regulations. When this is required, sign and issue a DD Form 254 for each affected proposal, invitation for bid, request for quotation, or other solicitation.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT (CONTINUED)

(5) Coordinate with the USAG, Fort Jackson Security Office and section requiring contract to develop appropriate security clauses for classified contracts to ensure that USAG, Fort Jackson and DSS can process all contractor employees for any needed facility or security clearances, and to do so according to requirements and procedures stated in the NISPOM and/or other applicable DOD regulations.

(6) Ensure security clauses for classified contracts also contain language specifying that requests for classified visits be made and prepared in accordance with the NISPOM, and certified by the contracting office prior to forwarding to the organization to be visited.

(7) Issue a completed DD Form 254 with the award of each classified contract, and provide a copy of the completed DD Form 254 to the USAG, Fort Jackson Security Office

(8) Ensure that whenever the USAG, Fort Jackson Security Office has determined that a contract requires investigation of any contractor employee, the contract contains language sufficient to achieve this objective in an orderly and expeditious manner. The language will also require the contractor to take appropriate action including removal of an employee from working on a USAG, Fort Jackson contract if it is determined that that person is unsuitable.

(9) Ensure no contractor employee works in any position until the USAG, Fort Jackson Security office has reviewed all required investigative forms, resolved any issues, and authorized them to work.

(10) Ensure the USAG, Fort Jackson Security Office is notified of any information that raises a question about the suitability of a contractor employee.

(11) Ensure appropriate action is taken immediately upon notification that a contractor employee is determined to be unsuitable for access to USAG, Fort Jackson facilities, sensitive information, classified information, and/or resources. Appropriate action may include removal of such employees from working on any aspect of the USAG contract.

4. Classified Contracts Requirements. Due to the damage to the national security that can be caused by the unauthorized disclosure of classified information, the following requirements apply to USAG, Fort Jackson classified contracts in addition to any standard security clauses that may apply.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT (CONTINUED)

a. All classified solicitations and Department of Defense (DD) Forms 254, Contract Security Classification Specification will be reviewed and approved by the USAG, Fort Jackson Security Office prior to award.

b. All USAG, Fort Jackson classified contracts must contain a DD Form 254. This form is designed to provide the contractor with the security requirements and classification guidance needed to perform under a classified contract.

c. Investigations of contractor personnel to be cleared under the NISPOM are:

(1) Coordinated by the USAG, Fort Jackson Security Office.

(2) Conducted by the DSS, who will also conduct inspections of cleared contractor facilities.

(a) At any given time, the USAG, Fort Jackson may retain the right to perform site inspections, which should be addressed in the contract.

(b) The contractor submits the necessary investigative forms for the affected contractor employees directly to DSS.

5. Post Award Actions. An effective relationship must be established between the USAG, Fort Jackson Security Office, the Contracting Office, and the responsible operating office. In addition to constant communication, the following actions are essential to maintaining effective liaison.

a. All amendments, modifications, revisions, and renewals to/of existing contracts with security implications must be routed through the USAG, Fort Jackson Security Office for review, whether or not the original document contained security implications. For example, if the original contractual document was not reviewed by the USAG Security Office because it did not involve work or services to be performed or provided by contractor employees, and an amendment, modification, change, etc., to that original document does contain such work or services, then the amendment modification, change, etc., must be reviewed by the USAG Security Office.

(1) In cases where changes do not affect the security posture of the contract, review is not required.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT (CONTINUED)

(2) In cases where changes do affect the security posture, the contracting office must submit the proposed changes to the USAG Security Office for review prior to inclusion in the contract.

b. The contracting officer must ensure notification is provided to the USAG Security Office when a contractor employee is terminated or leaves his or her position within 5 days of the event.

c. The USAG Security Office must ensure the contracting office is notified in writing, when:

(1) Interim suitability determinations are made that contractor employees may begin work under the contract.

(2) Final suitability determinations are made in accordance with AR 380-67, and NISPOM Manual.

(3) Any contractor employee is found unsuitable for access to USAG, Fort Jackson facilities, sensitive information, and/or resources and to request action to deny such access.

d. Operating offices must ensure contractor employees who work in or provide services to facilities within their area of responsibility are provided necessary security related information, i.e., facility access controls, identification media, protection of USAG, Fort Jackson sensitive information, and Automated Information Systems (AIS) security.

6. Position Risk/Sensitivity Level Designations.

a. Every contractor position must be designated at a risk or sensitivity level commensurate with the described duties, functions, and/or tasks that are performed under a given contract and whether access to classified information is required in order to perform those duties, functions, and/or tasks

b. There are three position risk levels:

(1) High Risk. These are public trust positions that have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority. This level includes positions that have major program responsibilities affecting AIS.

APPENDIX Z
INDUSTRIAL SECURITY PROGRAM MANAGEMENT (CONTINUED)

(2) Moderate Risk. These are public trust positions that have the potential for moderate to serious impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public. This level includes positions that have significant program responsibilities that affect AIS.

(3) Low Risk. These are positions that have potential for impact involving duties of limited relation to the agency mission with program responsibilities that affect the efficiency of the service. This level includes positions that have limited impact on AIS.

c. There are three levels for designating the sensitivity of positions with regard to the national security:

(1) Special-sensitive. These are positions involving the highest degree of trust that require access, or afford ready opportunity to gain access, to any information which is controlled under a Special Access Program as Sensitive Compartmented Information (SCI).

(2) Critical-sensitive. These are positions with the potential for causing serious to exceptionally grave damage to the national security and that require access, or afford ready opportunity to gain access, up to Top Secret classified information and material as described in E.O. 12958, Classified National Security Information.

(3) Noncritical-sensitive. These are positions with the potential for causing serious damage to the national security and that require access, or afford ready opportunity to gain access, to Secret classified information and material as described in E.O. 12958.

d. All position sensitivity/risk designations will be performed using the Position Sensitivity Tool on the National Background Investigation Services website located at https://pdt.nbis.mil/.

e. Background investigations for contractors assigned to classified contracts will be conducted by the contract organization by the designated Facility Security Officer, and will meet the requirements of Chapter 2, Reference 1.j.