Headquarters
US Army Armor Center and Fort Knox
Fort Knox, KY 40121-5721
10 March 2008

*Fort Knox Reg 380-5

Security

FORT KNOX INFORMATION SECURITY PROGRAM

Summary. This regulation outlines implementing instructions, responsibilities, and guidance to implement and enhance management of the Fort Knox Information Security Program.

Applicability. This regulation applies to all commanders, directors, supervisors, and security managers (SMs) of commands/organizations supported by Fort Knox, including those organizations with an approved Intra-Service Support Agreement (ISSA) that specifies support will be provided for any facet of Army Regulation (AR) 380-5 or 380-10.

Proponent. The proponent of this regulation is Security Division, Directorate of Plans, Training, Mobilization, and Security (DPTMS), Fort Knox, KY.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Security Division, DPTMS (IMSE-KNX-PLS), Fort Knox, KY 40121-5721.

Table of Contents

*This regulation supersedes Fort Knox Reg 380-5, 5 February 2002.

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Chapter 1
General Provisions and Program Management

Section I
Introduction

1-1. Purpose. This regulation establishes internal policy and procedures for inclusion in the local management and execution of the Department of the Army (DA) Information Security Program, prescribed in AR 380-5, and is to be used in conjunction with AR 380-5. Additionally, this regulation provides guidance on the duties and responsibilities of local commanders, directors, supervisors, and SMs, including those organizations with an approved ISSA that specifies support will be provided for any facet of AR 380-5 or 380-10.

1-2. Definitions.

a. Commander. The commander, officer in charge (OIC), director, or head of an agency or activity.

b. Command(s). Commands, directorates, agencies, activities, or areas of responsibility assigned or attached to Fort Knox, including those organizations with an approved ISSA that specifies support will be provided for any facet of security governed by AR 380-5 or 380-10.

c. Department of Defense (DOD) Personnel. Any Active, Reserve, or National Guard military personnel or government civilian employee assigned/attached to a local command, including any person employed by, assigned to, or acting for a local command, including contractors, licensees, certificate holders, grantees, and any person acting at the direction of such a command.

d. DA Retention (and Destruction) Requirements. The disposition instructions applied to a file as directed by AR 25-400-2. AR 25-400-2 implements the provisions of the Federal Records Act (44 USC, Chapters 21 and 23).

e. Security Manager (SM)/Command SM. The principal advisor on information security in the command who is responsible to the commander for management and administration of the program. The SM is also the key member of the information security program responsible for ensuring the command's security posture is maintained at optimum levels, ensuring our national assets are properly protected against subversion, espionage, and pilferage.

f. Fort Knox-Owned Information. Information concepts, requirements, etc., that is/are originally developed, visualized, and controlled by Fort Knox or a Fort Knox command.

Section II
Responsibilities

1-3. Commander. Security is a command function. Commanders will effectively manage the information security program within their commands. Commanders may delegate the authority

to execute the requirements of this regulation, where applicable, but not the responsibility to do so. Security, including the safeguarding of classified and sensitive information and the appropriate classification and declassification of information created by command personnel, is the responsibility of the commander. The commander will:

a. Designate a (command) SM, primary and alternate, by written appointment. The SM will be of sufficient rank or grade to effectively discharge assigned duties and responsibilities. As a general requirement, the SM will be a commissioned officer, warrant officer, noncommissioned officer (E-7 or above), or government civilian employee (GS-07 or above, in NSPS a GS-07 equivalent or above). In instances where the command is not sufficiently staffed to meet these rank or grade requirements, and a lower rank or grade individual is sufficient to effectively discharge assigned responsibilities, the commander must initiate a request for exception to policy (see paragraph 1-9), in writing to Chief, Security Division, DPTMS. The SM appointed must possess at least a SECRET clearance.

b. Establish written local information security policies and procedures and an effective information security education program.

c. Initiate and supervise measures or instructions necessary to ensure continuous control of classified and sensitive information and materials.

d. Ensure that persons requiring access to classified information are properly cleared.

e. Continuously assess the individual trustworthiness of personnel who possess a security clearance.

f. Ensure the SM has direct access to the appointing commander and the Chief, Security Division, DPTMS, on matters affecting the information security program.

g. Ensure the SM is afforded security training consistent with the duties assigned.

h. Ensure adequate support and resources are available for allowing the SM to manage and administer applicable information security program requirements.

i. Review and inspect the effectiveness of the information security program in subordinate commands.

j. Ensure prompt and appropriate responses are given or forwarded for higher echelon decisions, such as problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation.

k. Ensure prompt and complete reporting of security incidents, violations, and compromises related to classified and sensitive information.

l. Ensure prompt reporting of credible derogatory information on assigned/attached personnel, including recommendations for or against continued access (see Fort Knox Pamphlet 380-67).

1-4. Security Manager (SM). The SM will:

a. Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

b. Establish and implement an effective security awareness and education program that continuously encompasses all aspects pertaining to the protection of classified and sensitive information. As a part of this program, ensure each major work and break area has a completed FK Poster 380-5-1 and at least one other security poster visible to all personnel.

c. Establish procedures for ensuring that individuals handling classified material are properly cleared. The clearance status of each individual must be recorded and accessible for verification.

d. Advise and assist officials on classification problems and development of classification guidance.

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

f. Conduct a periodic review of classifications assigned within the activity to ensure that classification decisions are proper.

g. Consistent with operational and statutory requirements, review all classified and sensitive documents, in coordination with the Security Division, DPTMS, and Directorate of Information Management (DOIM), with the goal of continuous reduction by declassification, destruction, or retirement of unneeded classified and sensitive material.

h. Submit Standard Form (SF) 311 (Agency Information Security Program Data) to Security Division, DPTMS, per this regulation (see paragraph 1-10).

i. Supervise or conduct security inspections and spot checks and notify the commander regarding compliance with this regulation, AR 380-5, and other security regulations and directives.

j. Assist and advise the commander in matters pertaining to the enforcement of regulations governing the access, dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified and sensitive material.

k. Make recommendations, based on applicable regulations and directives, on requests for visits by foreign nationals and provide security and disclosure guidance if the visit is approved.

l. Ensure inquiry and reporting of security violations is completed, including compromises or other threats to safeguarding of classified and sensitive information, per AR 380-5.

m. Ensure proposed public releases on classified and sensitive programs are forwarded to the Chief, Security Division, DPTMS, per AR 380-5, AR 380-10, and this regulation.

n. Establish and maintain visit control procedures in cases where visitors are authorized access to classified information.

o. Issue contingency plans for emergency destruction and/or evacuation of classified and sensitive information and material.

p. Be the command's single point of contact to coordinate and resolve classification or declassification problems.

q. Report data, as required by this regulation, AR 380-5, and other applicable regulations and directives that apply to the information security program.

r. Notify the Commander or Security Division, DPTMS, within 8 hours of any incident discussed in Chapter 10, AR 380-5, and/or thefts involving computer equipment.

1-5. Supervisor. Supervisory personnel (to include those in command positions) have a key role in effective implementation of the command's information security program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information related to national security. The supervisor will:

a. Ensure subordinate personnel who require access to classified information are properly cleared and given access only to that information, including sensitive information, which they have a need-to-know.

b. Ensure subordinate personnel attend training and understand and follow the requirements of this regulation and AR 380-5, as well as all other local command policies and procedures concerning the information security program(s).

c. Continuously assess the eligibility for access to classified and sensitive information of subordinate personnel and report any information that may have a bearing on that eligibility to the SM.

d. Supervise personnel in the execution of procedures necessary for allowing continuous safeguarding and control of classified and sensitive information consistent with established information security programs.

e. Include the management of classified and sensitive information as a critical element/item/objective in personnel performance evaluations, where deemed appropriate, per Army personnel policy and paragraph 1-5c of AR 380-5. Supervisors should include the

protection of classified and sensitive information as a performance evaluation factor objective for other personnel as the supervisor deems appropriate.

f. Lead by example. Follow command and Army policy and procedures to properly protect classified and sensitive information and to appropriately classify and declassify information as stated in AR 380-5.

1-6. Individual. All DOD personnel, regardless of rank, grade, title, or position, have a personal, individual, and official responsibility to safeguard information related to national security. All DOD personnel will report, to the proper authority, violations by others that could lead to unauthorized disclosure of classified and sensitive information. This responsibility cannot be waived, delegated, or in any other respect, excused. All DOD personnel will safeguard all information and material related to national security, especially classified information, which they access and will follow the requirements of this regulation, AR 380-5, and other applicable regulations.

Section III
Program Management/Direction

1-7. Applicability. This regulation implements local initiative to enhance the command's management and execution of the DA Information Security Program and applies to all DOD personnel. This regulation is to be used in conjunction with AR 380-5. Information relating to national security will be protected by DOD personnel and employees against unauthorized disclosure.

1-8. Chief, Security Division, DPTMS. As the command SM for USAARMC and Fort Knox and US Army Garrison Command, the Chief, Security Division, DPTMS, is delegated responsibility for implementation and monitoring functions associated with all information security programs and requirements.

Section IV
Exceptional Situations

1-9. Waivers and Exceptions to Policy.

a. In the event a command cannot comply with the requirements of this regulation or AR 380-5, a waiver or exception to policy, with full justification, should be requested (example at appendix B of this regulation).

b. There may be unique situations in which a command may need an exception to the requirements of this publication or AR 380-5; for example, a waiver might be appropriate for a supply or warehouse receiving area that historically received Federal Express (FEDEX) shipments of unclassified materials. A waiver in this instance would eliminate the requirement to use only cleared personnel to screen packages or store unopened packages in locked containers.

c. All waivers and exceptions to policy will be processed through appropriate command channels to the Chief, Security Division, DPTMS, for determination on local issues and forwarding to US Army Training and Doctrine Command (TRADOC) for higher-level issues.

Section V
Reports and Inspections

1-10. Reporting Requirements.

a. Violations of the provisions contained in AR 380-5 will promptly be reported by commanders and/or SMs to the Chief, Security Division, DPTMS, especially those cases involving incidents that can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. See Chapter 10, AR 380-5.

b. Unless otherwise directed, SMs will submit, to the Security Division, DPTMS, a consolidated quarterly report, SF 311, for all elements under their security responsibility. This report should be received no later than the 2nd working day of the new quarter. During 4th quarter of each fiscal year, the report will be submitted no later than the 1st working day of September, because this will allow a consolidated USAARMC report to be compiled and submitted to TRADOC and ensure the command's compliance with AR 380-5. (Instructions for SF 311 are at appendix F of this regulation.)

c. By 4 January each year, SMs will report their command's compliance with the annual declassification, regrade, and destruction requirements described in Chapter 3 of this regulation.

1-11. Command Security Inspections.

a. Each commander will establish and maintain a self-inspection program from their command, and if applicable, a program to inspect their subordinate units.

b. The Security Division, DPTMS, will conduct mandatory information security program inspections for the command (see appendix C of this regulation for the inspection checklist). These inspections can be announced or unannounced. A tentative announced inspection schedule will be published at least 90 days in advance of an inspection. For unannounced inspections, Security Division will notify the commander of the organization to be inspected, a maximum of 48 hours and a minimum of 8 hours prior to arrival of the inspector(s).

Chapter 2
Local Production of Classified Information and Classification Challenges

Section I
US Army Armor Center (USAARMC)-Originated Classified Information

2-1. General. As the only authorized Original Classification Authority (OCA) in the command, the CG, USAARMC, is the only person that can apply original classification to "USAARMC-owned information."

2-2. Producing Classified "USAARMC-Owned Information." When the Fort Knox command generates "USAARMC-owned information" that is believed to be classified, the producer of the information must take the following actions:

a. Provide protection to subject information that is equal to, or above, the classification level of the information (i.e., information that is believed to be CONFIDENTIAL must be afforded, at a minimum, the same protection as known CONFIDENTIAL information but may be protected at the same level as known SECRET information).

b. Review Chapter 2 of AR 380-5.

c. Determine if the product must contain classified or potentially classified information.

(1) If it does not, eliminate any such information from the product.

(2) If it does, minimize any such information contained in the product and be able to fully justify its necessity to the product.

d. Have the information reviewed by your SM and immediate supervisor.

e. Forward, through your SM, the product to Chief, Security Division, DPTMS, for review and coordination.

Section II
Classification Challenges

2-3. General.

a. One of the information security program's functions is to ensure information is not improperly or unnecessarily classified. AR 380-5 provides guidance for formal challenges to classification; however, informal questioning is also possible and should be accomplished to resolve any questions prior to submitting a formal challenge.

b. While AR 380-5 provides guidelines for informal and formal challenges of information under a command's OCA, challenges may also be generated to derivative or compiled information. This factor is one of the major reasons to comply with the requirement of making a

list of all sources (and if possible, which portion of each source) used to produce these types of information. Additionally, producers of these types of information are encouraged to provide each recipient with a copy of the source list. Providing this will reduce the possibility of a challenge and facilitate easier declassification review.

2-4. Receiving or Submitting a Classification Challenge. Any USAARMC or US Army Garrison Command that received a challenge on information that was locally produced, or wishes to submit a challenge, shall ensure the challenge is properly routed through the Chief, Security Division, DPTMS.

Chapter 3
Declassification, Regrading, and Destruction

Section I
General

3-1. The Owner (OCA). The owner (OCA) of any information is the only authority that can decide whether information meets the criteria for continued classification and/or exemption from automatic declassification.

3-2. Possession of the Information. When a command possesses information that is deemed to no longer be necessary for operational, historical, or reference purposes, and/or has completed its DA retention requirements (AR 25-400-2), such information shall be destroyed per this regulation and AR 380-5.

3-3. Local Command Compliance. To ensure local commands are complying with the provisions of this regulation, DA retention and destruction requirements, and AR 380-5, as applied to this chapter, each document, file, etc, containing classified information will be reviewed annually for declassification, regrading, and/or destruction. This annual review will be conducted during the 1st quarter of each fiscal year. Each SM will report compliance with this annual review to the Chief, Security Division, no later than 4 January each year.

Section II
Declassification and/or Regrading

3-4. Declassification or Regrading Actions. Upon receipt of instructions/notification of a declassification or regrading action, the SM will ensure the action is completed. If the action affects:

a. An entire document, the markings throughout the document will be changed to reflect the new classification level, the cover page will annotated to indicate the source of the change, and the instructions/notification will be filed per AR 380-5 and AR 25-400-2.

b. A portion of a document, the affected portions will be re-marked to reflect the change, each portion should be annotated to indicate the source of the change, and the instructions/notification will be filed per AR 380-5 and AR 25-400-2.

c. Declassification marking, documents created on or after 22 September 2003, bearing the exemption categories X1 through X8 are re-marked per Secretary of Defense Memo, 1 May 2007, subject: Policy Regarding Exemption Categories X1-X8 Declassification Markings.

3-5. USAARMC-Owned Classified. If the information is "USAARMC Owned," the Chief, Security Division, DPTMS, shall be notified and will guide the producing command through the appropriate, required procedure.

Section III
Destruction

3-6. General. 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. Once information has completed it's DA retention requirement or is no longer necessary for operational, historical, or reference purposes, the following actions shall be completed.

a. **USAARMC-Owned Classified.** If the information is "USAARMC Owned" (the CG, USAARMC, is the OCA), contact the Chief, Security Division, DPTMS, for instructions.

b. **US Government Classified.** For US Government information that is not "USARMC Owned" and non-North Atlantic Treaty Organization (NATO) foreign government information, destroy per AR 25-400-2 and AR 380-5.

c. **NATO.** For NATO information, destroy per AR 380-15.

3-7. Destruction Methods.

a. **Equipment or Technique.** The equipment or technique used to destroy classified information varies and is dependent on the material makeup of the item containing the classified information. Within this command, the majority of our classified information is stored or produced on paper, transparencies, CD ROM, or some type of (computer) magnetic media. The approved method of destruction for these and all items is described in AR 380-5.

b. **Shredding.** Shredding is the most frequently used method of destruction. However, not all shredders meet required specifications. Only approved crosscut shredders may be used to shred classified documents. Therefore, the SM will ensure every shredder in his/her command is clearly marked to indicate the level of information and type of "media" the shredder is approved to destroy. If the SM is not 100 percent certain of the approved capabilities of a piece of equipment that is going to be used for destruction of classified information, contact the Chief, Security Division, DPTMS, for assistance.

3-8. Destruction Equipment Available for Command-Wide Use.

a. **Security Division.** The Security Division, DPTMS, has authorized equipment available, by appointment, that is capable of destroying paper and CDs.

b. **Directorate of Information Management (DOIM).** The DOIM has authorized equipment available, by appointment, that is capable of destroying hard disk drives, zip drives, jazz drives, floppy diskettes, magnetic tape, and videotapes.

c. **Fort Knox.** Fort Knox does not use burning as a means of destruction.

Chapter 4
Marking

4-1. General. DOD personnel who produce classified or controlled unclassified information are responsible for ensuring the information and media used to produce, manipulate, or store the information is marked per AR 380-5.

4-2. Document Custodians. DOD personnel, particularly classified documents custodians, are responsible for reviewing and storing documents in their possession or ensuring the information was properly marked by the producer.

4-3. Security Managers (SMs). The SMs are responsible for the following:

a. Ensuring all personnel in their command, with a valid clearance, are aware of the marking requirements in AR 380-5.

b. Advising and assisting classified information producers and handlers in complying with the proper marking procedures set forth in AR 380-5 and ensuring all users of the SIPRNET are properly trained (see appendix G this regulation).

c. Spot checking information produced, handled, or stored within their command for proper marking procedure application.

d. Reporting to the commander and/or Chief, Security Division, DPTMS, the following:

(1) DOD personnel within their command who refuse to adhere to the marking requirements of AR 380-5.

(2) Any incident that resulted or may have resulted in the disclosure of improperly marked information (see Chapter 10, AR 380-5).

4-4. Additional Marking Requirements. The following marking requirements shall be observed in this command:

a. **Page Marking.** Mark or stamp the top and bottom of the back of the last page of a classified document with the same markings as the first page.

b. **File Folders.** Conspicuously mark or stamp the front and back of file folders containing classified material. These markings shall be placed so classification of the contents is readily visible when the folder is placed in the security container drawer.

4-5. Telephones, Facsimile (FAX) Machines, Copiers, Printers, Shredders, and SIPRNET.

a. All telephones and FAX machines will have a DD Form 2056 affixed to them. Secure telephones and FAX machines will have a modified version, reminding users to always ensure sending and receiving systems are in the secure mode prior to transmitting.

b. All copiers will be clearly marked to indicate the level of information authorized to be reproduced on the equipment. If the equipment is authorized to reproduce classified material, see Chapter 6, Section III, of this regulation, for additional markings.

c. All shredders will be clearly marked to indicate the level of information authorized for destruction.

d. All SIPRNET equipment (computer, hard drive, and printer) will be labeled in accordance with (IAW) published security directives.

Chapter 5
Controlled Unclassified Information

5-1. Controlled Unclassified Information (CUI) Protection. While not classified, the protection of CUI is a must. The CUI is information that does not require the degree of protection afforded by the application of a security classification but is so sensitive it warrants placing a degree of control over its use and dissemination. Examples include Privacy Act protect information (such as social security numbers, dates of birth, and home address/phone numbers). For Official Use Only (FOUO) information and information exempt from release under the Freedom of Information Act (FOIA). Of all the different types of information that require protection, CUI is the least recognizable and is also a **high payoff target for individuals/organizations striving to gain unauthorized disclosure.**

5-2. Handling CUI. On a daily basis, we handle a tremendous amount of CUI, particularly FOUO, sensitive information (Computer Security Act of 1987), and technical documents. A great percentage of CUI handlers are not aware of proper handling and protection requirements.

5-3. Maintain a Compiled List. Producers of compiled information must maintain a list of all sources and provide this list, on demand, to the disclosure officer or the FOIA officer.

5-4. Authorization to Release CUI. In this command, there are only two offices authorized to release CUI to non-DOD entities:

a. The FOIA Officer, Administrative Services Division, Directorate of Human Resources (DHR).

b. The Disclosure Officer, Security Division, DPTMS.

5-5. Education. Commanders and SMs must aggressively educate all members of their commands on:

a. What CUI is.

b. Where it exists in their commands.

(This page intentionally left blank)

Chapter 6
Access, Control, Safeguarding, and Visits

Section I
Access

6-1. Responsibilities.

a. As a condition of providing access to anyone, the holder of classified information must ensure the recipient:

(1) Has a need-to-know.

(2) Has clearance authorization (see para 6-7 for contractors, consultants, and visitors).

(3) Understands the information is classified.

(4) Knows how to protect the information.

(5) Has the ability to protect the information.

(6) If transporting the information to another location, has the proper credentials.

b. If any of the conditions above do not exist, access to the information should be delayed, and the holder's SM should be notified for guidance.

6-2. Non-Disclosure Agreement (NDA). The SMs will maintain documentary proof that DOD civilians and locally-hired DOD consultants have executed an NDA. Follow the guidelines explained in AR 380-5, Chapter 6. The preferred proof is a photocopy of the signed NDA. The NDA also has to be entered into the Joint Personnel Security Adjudication System (JPAS). Record of execution of the NDA in JPAS will be sufficient.

Section II
Reassignments, Transfers, Retirements, Resignations, Separations, and Terminations.

6-3. General.

a. All DOD personnel and local-hire consultants will outprocess through the SM.

b. All personnel that have been designated, on orders, as a courier will have their orders revoked immediately.

c. All personnel issued a DD Form 2501 (Courier Authorization card) must turn the card in to their SM.

6-4. Reassignments and Transfers.

a. Military Personnel. The SM will forward the "local" file copy of the individual's NDA to the gaining SM. This action can be accomplished either by providing a copy to the Soldier for hand carrying or by official mail. If the Soldier is hand carrying, the copy should be placed in an envelope and addressed to: S2/SM.

b. Civilian Personnel. If the SM is maintaining a copy of the NDA, the same procedure described in 6-4a of this regulation applies.

6-5. Retirements, Resignations, Separations, and Terminations. All DOD personnel and local-hire consultants will be debriefed by the SM. The debriefing will be conducted, documented, and filed per AR 25-400-2, AR 380-5, and AR 380-67.

Section III
Control Measures

6-6. Emergency Planning.

a. All commands with classified material shall establish emergency plans that provide for protection of classified material in a manner that minimizes the risk of personal injury or loss of life to personnel. In case of fire or natural disaster, this requires immediate placement of authorized personnel around the affected area, pre-instructed and trained to prevent removal of classified material and reduce casualty risk.

b. Post emergency plans in a conspicuous place, such as on a wall near the storage container(s) or on the container itself. Such plans shall provide for emergency destruction or evacuation to preclude capture, compromise, or loss of classified material when determined to be required. This determination shall be based on an overall common sense evaluation of the following factors:

(1) Level and sensitivity of classified material held by the activity.

(2) Sensitivity of operational assignment.

(3) Potential for aggressive action of a hostile entity.

c. When preparing emergency plans, consideration shall be given to the following:

(1) Reduction of the amount of classified material held by your command.

(2) Transfer of retained classified material to an "other than paper" type of media as much as possible.

(3) Emphasis on the priorities for destruction/evacuation, designation of personnel responsible for destruction/evacuation, and designation of places and methods of

destruction/evacuation. Additionally, if any destruction site's particular piece of destruction/evacuation equipment will be used by more than one activity or entity, the order or priority for use of the site or equipment must be clearly delineated.

(4) Identify the individual(s) authorized to receive/disseminate the execution order once the Security Division, DPTMS, has determined an emergency destruction/evacuation is to begin. Additionally, identify how the order will be disseminated to all subordinate elements (emergency plans will clearly identify the position titles of these individuals).

(5) Authorization for the senior person present to deviate from established plans when circumstances warrant.

(6) Emphasis on the importance of implementing the plan early to preclude loss/compromise of material. The effect of premature destruction is considered inconsequential when measured against the possibility of compromise.

d. Classified material holdings shall be prioritized for emergency planning. Priorities should be based on the potential effect on national security, should such holdings fall into unauthorized hands. The following guidelines are provided:

(1) Priority One. (TOP SECRET) Exceptionally grave damage. (Secret Special Access Programs (SAPs) should also be labeled as priority one.)

(2) Priority Two. (SECRET) Serious damage.

(3) Priority Three. (CONFIDENTIAL) Damage.

e. In determining the method of destruction of other than Priority One (TOP SECRET) material, any method specified for routine destruction of any means that will ensure positive destruction of the material may be used. Ideally, any destruction method should provide for early attainment of a point the destruction process is irreversible. If time and circumstances of the emergency permit, the destruction methods specified in paragraph 3-7 above and/or AR 380-5 should be used.

6-7. Visitors/Contractors/Consultants.

a. On occasion, personnel from this command visit activities and organizations off the installation. Many times, these visits involve classified information/material, creating a need to certify individual security clearance information. To facilitate the certification of security clearances, SMs will prepare and authenticate FK Form 5060-E, May 2001. The JPAS can also be used to pass security clearance and visit request information.

b. When a command is contacted by or is inviting, hosting, or sponsoring a visit of any person or organization, the SM will be notified.

c. The SM will notify Security Division, DPTMS, when a visit involves foreign personnel. Information on visits by foreign personnel/organizations will be handled per AR 380-10.

d. Ensure the procedures of Chapter 6, AR 380-5, are adhered to if the pending or proposed visit is anticipated to involve access to classified material/information. (FK Form 5060-E, May 2001, may be used to verify clearance/access information.)

e. Maintain information on all visits to their organization. This information will be retained and filed per AR 25-400-2.

f. Maintain the following for contractors and consultants working in your command who require access to classified material:

(1) Confirmation of security clearance and level of clearance.

(2) Confirmation of execution of NDA.

(3) Copy of the contracts "statement of work" (to assist in establishing a need-to-know).

(4) Contact information for the contracting officer representative, SM of the US Government sponsoring agency, and SM for the contracted organization.

6-8. Classified Presentations. Holding classified presentations (meetings, conferences, classes, lectures, and other presentations) will be held only in facilities approved for classified discussion. Command activities that hold or sponsor any type of classified presentation will appoint a security representative to be responsible for overall security at the site of the presentation. The security representative will ensure the following requirements are met:

a. The date, location, and subject of the presentation are furnished to Security Division, DPTMS, at least 3 working days prior to commencement.

b. Conversations or discussions involving classified material are not held in areas where they can be overheard by unauthorized personnel. This includes ensuring that public address systems are set at a level which precludes classified discussions/presentations from being overheard outside of the presentation area.

c. Individual speakers/presenters will announce the security classification of the subject matter at the beginning and end of the presentation.

d. All slides and material used during the briefing will bear the appropriate security classification markings.

e. Access rosters (name, rank, SSN, clearance, and organization) to verify authorized attendees are compiled and used at a controlled entrance point. These rosters shall be maintained/destroyed as FOUO in order to protect the contents from unauthorized access.

f. Attendees must be identified by presenting a picture ID (military/civilian employee ID card, passport, driver's license, etc.,) before admittance into the presentation area. Support personnel (i.e., guards, monitors, etc.,) will verify personal information by comparing the access roster and presented ID. If there are discrepancies, the attendee must be referred to the security representative. Under no circumstances will the attendee be allowed to enter the presentation area until the security representative verifies their need-to-know and security clearance.

g. Doors and windows are closed and covered during the presentation.

h. Sufficient, appropriately cleared guard/monitor personnel are pre-positioned at all entrances, exits, and adjacent areas to prevent unauthorized access or loitering.

i. Briefcases, cameras, video recorders, computers, cell phones, beepers, electronic recording devices, or any other similar electronic device(s) will not be allowed to enter the presentation area.

j. Care is exercised to reduce the possibility of clandestine surveillance listening devices being installed in areas where classified information is discussed/presented. A physical check will be made of the area to detect any obvious device that could be used to transmit or record the presentation (i.e., adjacent rooms, hallways, heating/air condition vents or ducts, inside/outside of perimeter walls, window ledges, dropped/false ceilings, etc.,).

k. Only electronic equipment that has been accredited for processing classified information may be used to conduct the presentation.

l. Note taking, unless strictly controlled, is prohibited. If notes are taken, the security representative is responsible for ensuring the material is properly marked and protected until properly secured in an approved container.

m. The presentation site is checked immediately following the departure of all attendees to ensure no classified material has been inadvertently left in the area.

6-9. Receipt of Classified Material. All commands will establish a procedure for protecting incoming official first class mail, registered mail, and express mail/packages until a determination is made on whether classified information is contained therein. As part of these procedures, official first class mail recipients/openers and registered/express mail/package recipients/openers will be appointed on orders.

a. Individuals appointed as recipients or openers of official first class mail must possess, at a minimum, a CONFIDENTIAL clearance.

b. Individuals appointed as recipients or openers of registered/express mail/packages must possess, at a minimum, a SECRET clearance.

Section IV
Reproduction of Classified Material

6-10. General. Unnecessary, non-mission essential reproduction of classified material increases the possibility for security violations and compromise.

6-11. Approval for Reproduction.

a. Commanders that feel their commands have a requirement to make mission-essential reproductions of classified material will submit a written request to Security Division, DPTMS (IMSE-KNX-PLSS), for authorization to reproduce classified material. This request will:

(1) Include a justification for reproduction authority.

(2) List the equipment to be used (make, model, serial number, etc.,).

(3) Denote the equipment's location.

(4) Provide the name or position of the individual to be designated as the classified material reproduction control officer.

(5) Include a copy of the internal control procedures to be used.

(6) Provide a time period the request is to cover (may not be more than 12 months).

b. Approval for the reproduction of TOP SECRET, SAPs, NATO, and other categorized material may only be granted by the appropriate installation control officer. However, such requests shall be submitted through Security Division, DPTMS, to the proper control officer.

c. All reproduction equipment will be clearly marked, with the appropriate notice, reflecting the highest level of information that may be duplicated on it.

Section V
Additional Inspections

6-12. Entry Exit Inspection Program (EEIP).

a. The EEIP will be managed and executed at the installation level. The Security Division, DPTMS, will randomly conduct EEIP inspections. Prior to conducting an EEIP inspection, the SM will be given a minimum of 4 working hours notice. This does not prevent commands from conducting EEIP inspections on their own. Instructions and procedures for conducting these inspections are at appendix D of this regulation.

b. The SMs are responsible for EEIP awareness and education. This should be accomplished by inclusion in the command's standing operating procedures (SOP) and annual security training.

c. The SMs are responsible for ensuring FK Poster 380-5-8 is clearly, and continuously, posted at the entrance(s) of their building(s) that house classified material.

6-13. M1 Series (Abrams) Tank Security. Although this is a physical security requirement, breaches of the external armor are reportable as a potential compromise under AR 380-5. Further information is contained in the installation Force Protection and/or Physical Security Plans.

6-14. Additional Inspections. Requirements and procedures for additional inspections relating to the DA Information Security Program will be coordinated, under separate cover, with the affected command(s).

(This page intentionally left blank)

Chapter 7
Storage and Physical Security Standards

7-1. Purchase or Turn in of Equipment. All elements in this command will contact Security Division, DPTMS, prior to purchasing or turning in any equipment discussed in Chapter 7, AR 380-5. This is strictly a cost saving measure, because this office may have information on a requirement change or the location of a command that has or desires transferable equipment.

7-2. Security Managers (SMs) Responsibility. The SMs are responsible for changing combinations on security containers storing classified material. Assistance or training for changing combinations may be obtained by contacting the Security Division, DPTMS.

7-3. Locksmiths. Locksmiths will not be utilized to assist in routine combination changes. In cases where locksmith services are required, SMs must coordinate with the Security Division, DPTMS, prior to initiating the request.

7-4. Master Container. Commands having more than one security container will designate one container as the master container. The master container will contain Part 2 and 2a of SF 700 for all other security containers. Part 2 and 2a of the master container's SF 700 will be maintained in the master container of the next higher command if the command is located on this installation; otherwise, they will be maintained in the DHR Classified Files Section, Bldg. No. 1227. The DHR will be notified upon transfer or turnin of master containers so the SF 700s on file can be properly annotated or destroyed. The only authorized exception is for containers storing 2-person control material; for these containers, complete only Part 1, SF 700.

(This page intentionally left blank)

Chapter 8
Transmission and Transportation

Section I
Methods of Transmission and Transportation

8-1. SECRET and CONFIDENTIAL Information.

a. If US Postal Service services cannot meet an urgent requirement, DOD policy authorized the use of FEDEX. This service is only authorized for use within CONUS and only between DOD commands. FEDEX is not authorized to transmit material to contractors or non-DOD agencies. Additionally, classified communications security material, sensitive compartmented information (SCI), or classified SAP material will not be transmitted using FEDEX.

b. Material to be shipped will be prepared per Chapter 8, AR 380-5. The sender will ensure a proper address is used to ensure the package is received by a cleared person with appropriate need-to-know or who will ensure delivery of the package to the person or office with the need-to-know. After packaging, classified material must be taken to the Fort Knox Post Office (Bldg. No. 1359, Post Locator side) for processing by postal officials. Under no circumstances will a classified FEDEX package be dropped off in the FEDEX drop box.

c. Packages shipped via FEDEX will be shipped Monday through Thursday only.

d. Customers will retain the receipt given to them by postal officials until notification is received that the material has arrived at its final destination. Classified Document Accountability Record, DA Form 3964, will be utilized and retained per AR 380-5.

Section II
Transmission of Classified Material to Foreign Governments

8-2. Release of Classified Information. Prior to release or transmission of classified information or material, approval must be obtained from the installation Foreign Disclosure Officer. For further information/assistance contact Security Division, DPTMS.

Section III
Escort or Hand Carrying of Classified Material

8-3. General.

a. Within the confines of Fort Knox, personnel that hand carry/transport classified material outside their immediate work areas (to another building) must have, in their possession, either a DD Form 2501 (Courier Authorization) or an original copy of a courier authorization letter or memorandum. The individual command's SM is the only issuing authority for either of these documents. The following requirements pertain only to classified material transported within the confines of Fort Knox:

(1) Classified material shall only be transported from one working area or building directly to another working area or building and only when absolutely necessary.

(2) When transporting classified material between working areas or buildings, the material must, at a minimum, have the appropriate cover sheet attached (inner wrapping) and be enclosed in a sealed opaque envelope or container (outer wrapping). A locked briefcase qualifies as an outer wrapping.

b. Authorization to hand carry classified material off the installation using commercial conveyance or outside the continental US is reserved for the Chief, Security Division, DPTMS. These authorizations will only be granted when all other authorized means of transmission have been evaluated and cannot be utilized to complete a critical mission requirement. For further information and procedural guidance, contact Security Division, DPTMS.

8-4. Courier Authorization.

a. Security Managers.

(1) Must, prior to issuance of any courier authorization, verbally brief the individual on the duties, responsibilities, and limitations of authorization pertaining to their specific courier authorization. An example of what this briefing might contain is located in appendix E of this regulation.

(2) Upon completion of the verbal briefing, the designated courier must sign the appropriate statement (appendix E of this regulation) to verify he/she has been briefed and understands his/her responsibilities. The SM retains the statement with the individual's FK Form 1378 (Record of Personnel Security Clearance/Action).

(3) Are authorized to sign DD Forms 2501 and courier authorization letters or memorandums for their command members determined to have a need to hand carry classified material within the continental US and are traveling only by government conveyance. All other authorizations must be granted by Security Division, DPTMS.

b. DD Form 2501 is an accountable form and is only available from the Security Division, DPTMS. DD Form 2501 will:

(1) Be used when ground transportation or military air is the mode of travel.

(2) Not to be used when hand carrying classified material aboard commercial aircraft.

(3) Be issued for a period not to exceed 2 years. Upon expiration of the form or reassignment, transfer, retirement, resignation, separation, or termination of an individual issued a DD Form 2501, the card will be returned to the SM for destruction.

(4) Semi-annually, will be inventoried on a "show" basis.

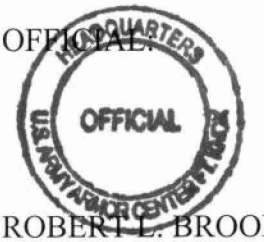
(5) Be limited to personnel that frequently hand carry classified information or material.

c. Written authorization from the SM is acceptable means of courier identification on the installation. An example of written authorization is at appendix E of this regulation.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

OFFICIAL:



ROBERT L. BROOKS
Director, Information Management

DISTRIBUTION:
A

(This page intentionally left blank)

Appendix A
References

DOD Publications

DOD 4525.6-M, Department of Defense Postal Manual, 15 August 2002.

DOD 5200.1-R, Information Security Program, 14 January 1997.

Army Regulations

AR 25-2, Information Assurance, 24 October 2007.

AR 25-55, The Department of the Army Freedom of Information Act Program, 11 November 1997.

AR 25-400-2, The Army Records Information Management System (ARIMS), 2 October 2007.

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

AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, 22 June 2005.

AR 380-49, Industrial Security Program, 15 April 1982.

AR 380-67, The Department of the Army Personnel Security Program, 9 September 1988.

AR 380-381, Special Access Programs (SAPs) and Sensitive Activities, 21 April 2004.

AR 381-12, Subversion and Espionage Directed Against the US Army (SAEDA), 15 January 1993.

AR 525-13, Antiterrorism, 4 January 2002.

AR 530-1, Operations Security (OPSEC), 19 April 2007.

TRADOC

TRADOC Reg 525-13, TRADOC Force Protection Program (FPP), 12 December 1997.

Memo, HQ TRADOC, ATOB-JC, 20 December 1994, subject: Transmission of DOD Classified Material via Federal Express (FEDEX).

Local Regulations/Policies

Fort Knox Regulation 25-70, Procedures for the Entry of Information into the Fort Knox World Wide Web (WWW) and Army Knowledge Online and Use of Fort Knox Communications Resources, 7 January 2008.

Fort Knox Pamphlet 380-67, Personnel Security Program, 21 October 1994.

Forms/Labels/Posters

Standard Form 75, Request for Preliminary Employment Data, August 1998.

Standard Form 311, Agency Information Security Program Data, November 2004.

Standard Form 312, Classified Information Nondisclosure Agreement, January 2000.

Standard Form 700, Security Container Information, April 2001.

DD Form 2056, Telephone Monitoring Notification Decal, May 2000.

DD Form 2501, Courier Authorization, March 1998.

DA Form 3964, Classified Document Accountability Record, July 1979.

FK Poster 380-5-1-E, Your Security Team, August 2001.

FK Poster 380-5-8, Entry/Exit Inspection, October 1989.

FK Poster 380-5-9, Warning – Reproduction of Classified Material, May 2002.

Appendix B
Example of Exception to Policy/Request for Requirement Waiver

Security Manager's Office Symbol Date

MEMORANDUM FOR Security Division, DPTMS

SUBJECT: Request for Requirement Waiver

1. Request you grant a waiver for the "security manager grade" requirement listed in paragraph 1-3a of Fort Knox Reg 380-5.

2. After reviewing our current staffing level, I have determined that I do not have any military or civilian personnel assigned that have either a reasonable amount of retainability or the ability to effectively discharge the duties of a security manager and/or that meet said grade requirement.

3. I am aware the Information Security Program is my responsibility, and if granted this waiver, I will ensure the appointed security manager receives the full cooperation of my organization.

I. M. AWARE
Director, Mastermind Development

(This page intentionally left blank)

Appendix C
Inspection Checklist

INSPECTION CHECKLIST
For use of this form, see Fort Knox Pam 25-31

FUNCTIONAL AREA:	SUBJECT AREA:	
Information Security	Information Security Program, AR 380-5	
PROPONENT/PHONE NO: Security Division, DPTMS/4-1655		DATE OF REVISION: (MM-DD-YYYY)
UNIT INSPECTED:	DATE: (MM-DD-YYYY)	INSPECTOR'S NAME/PHONE NO:

YES	NO	N/A	INSPECTION ITEM
			1. REFERENCES:
			AR 25-2, Information Assurance, 24 October 2007.
			AR 380-5, Department of the Army Information Security Program, 29 September 2000.
			AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, 22 June 2005.
			AR 380-49, Industrial Security Program, 15 April 1982.
			AR 380-67, Department of the Army Personnel Security Program, 9 September 1988.
			AR 381-10, US Army Intelligence Activities, 3 May 2007.
			AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA), 15 January 1993.
			AR 525-13, Antiterrorism, 4 January 2002.
			AR 530-1, Operations Security (OSPEC), 19 April 2007.
			DA Pamphlet 25-16, Security Procedures for the Secure Telephone Unit, Third Generation (STU-III), 1 April 1993.
			Fort Knox Regulation 25-70, Procedures for the Entry of Information into the Fort Knox World Wide Web (WWW) and Army Knowledge Online (AKO) Websites and Use of Fort Knox Communication Resources, 7 January 2008.
			Fort Knox Regulation 380-5, Fort Knox Information Security Program, 10 Mar 08..
			Fort Knox Pamphlet 380-67, Personnel Security Program, 21 October 1994.
			DOD 5220.22-M, National Industrial Security Program Operating Manual, 1 February 2006.
			Are the listed references readily available to the Primary and Alternate Security Managers?
			REMARKS: _____
			2. APPOINTMENTS AND AUTHORIZATIONS: (AR 380-5, paras 1-6 and 6-11; Fort Knox Reg 380-5, paras 1-4 and 6-9)
			a. Has a primary and alternate security manager been appointed in writing? Do those appointed meet the grade/rank requirement? If not, has an exception to policy been granted?
			b. Have individuals with appropriate clearances been appointed as official first class (CONFIDENTIAL) and registered/express mail (SECRET) openers?
			c. Has an official been designated to authorize reproduction of classified material?
			REMARKS: _____

FK FORM 331-E, FEB 2008 PREVIOUS EDITIONS ARE OBSOLETE. Page 1 of 7
FK PE V1.00

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM
			3. ACCESS: (AR 380-5, chap 6, section I and II; Fort Knox Reg 380-5, chap 6, Section I and II) a. Have classified information nondisclosure agreements (SF 312) been executed on all government personnel with access to classified information? (1) Are SF 312s completed as a condition of access? (2) Are SF 312s properly prepared and annotated in JPAS? (3) Are SF 312s for civilian personnel sent to CPAC for placement in the OPF? (4) Are SF 312s for military personnel forwarded to PERSCOM or EREC? b. Are individuals debriefed? Are files maintained IAW AR 380-5, chap 6-2a? c. Does the security manager have the following for all contract/consulting personnel working in their command: (1) Confirmation of security clearance and level of clearance. (2) Confirmation of execution of nondisclosure agreement. (3) Copy of the contracts "statement of work" (to assist in establishing the need-to-know). (4) Contact information for the contracting officer representative, security manager of the US Government sponsoring agency, and security manager for the contracted organization. d. If the command has visitors, are the procedures of chapter 6, AR 380-5, adhered, to if the visit involves access to classified material/information? e. Is visitor information retained on all visits to the command? f. What are your controlled measures for personnel authorized TOP SECRET information? (1) Are these individuals read-on to SCI, NATO, CNWDI, or SAP? (2) Have they attended the required annual SCI update brief? (3) Are they deleted when access is no longer required? Are files appropriately maintained? REMARKS: _____ 4. SECURITY POLICIES AND PROCEDURES: (AR 380-5; Fort Knox Reg 380-5, para 1-4) a. Have supplemental security policies and procedures been developed for this activity? b. Do the policies and procedures include: (1) Guidance on access? (2) A security education program (SAEDA, OPSEC, Disclosure, AT/FP, Information Security, Personnel Security, and Intelligence Oversight)? (3) Information on duplicating/copying classified files?

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM
			(4) Guidance on violations/compromises/infractions?
			(5) Information on destruction of classified/controlled unclassified information?
			(6) Guidance on hand carrying classified information?
			(7) Guidance on sending classified mail/packages?
			(8) Guidance on receipt of classified mail/packages?
			(9) STE telephone use?
			(10) Conducting classified meetings, conferences, briefings, etc?
			(11) Required travel briefings?
			(12) Guidance about visitors/contractors/consultants?
			(13) Emergency Action Plans for evacuation and destruction of classified?
			(14) Guidance on release of official government information to contractors and foreign nationals?
			(15) Guidance on SIPRNET use?
			REMARKS:
			5. SAFEGUARDING: (AR 380-5, section VII, chapter 6, para 35; DA Pam 25-16; Fort Knox Reg 380-5 chap 4, para 5, and chap 6, sec II)
			a. Has the activity conducted self-inspection/spot checks to determine the effectiveness of their security program?
			(1) Are these self-inspections/spot checks recorded?
			(2) Are these records properly maintained?
			b. Does the command have a website/webpage/homepage? If so, has the information been appropriately staffed for release?
			c. Are procedures in place to ensure the requirements for conducting classified meetings, conferences, or briefings are accomplished properly?
			d. Do all telephones (and FAX machines) have a DD Form 2056 affixed to them?
			e. Does the command have a STE telephone or classified FAX?
			(1) Do they have a modified version of DD Form 2056 affixed to them? Additionally, FAX machines should also be labeled indicating the level of information authorized to receive.
			(2) Are Fortezza cards inventoried and controlled as required?
			(3) Are proper security procedures employed when using the equipment?
			f. Are classified systems accredited and controlled as required?

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM
			REMARKS:
			6. DOCUMENT MARKINGS: (AR 380-5, chap 4; Fort Knox Reg 380-5, chaps 2 and 3) a. Are classified documents properly marked with the overall classification level? b. Are interior pages of classified documents properly marked? c. Are paragraphs marked as required? d. Is the classification authority properly identified on the classified by/derived from line? e. Are downgrading or declassification instructions properly displayed on the document? f. If the command created the document: (1) Under the CG's OCA authority, does the document reflect the creating organization name, justification for classification, and date of classification decision? (2) From derivative sources, does the record copy have a list of all sources? g . Are working papers datèd when created, safeguarded and destroyed, or finalized after 180 days. h. Are SIPRNET documents created/downloaded brought under the control and marked as required by AR 380-5? i. Are file folders and binders containing classified material marked with the overall classification level of the information contained inside? j. Are classification challenges made to the proponent when an incorrectly or unmarked document is received?
			REMARKS:
			7. DESTRUCTION: (AR 380-5, chaps 3 and 6; Fort Knox Reg 380-5, chaps 3 and 4) a. Are approved methods being utilized for the destruction of classified material? b. Are all shredders clearly labeled to reflect the level of information authorized for destruction in the equipment? c. Is the activity destroying documents that are 5 years old, or older, that are not permanently valuable records of the government? d. Has the annual classified document clean-out day been accomplished? e. Are destruction certificates and witnesses used and maintained as required?
			REMARKS:
			8. REPRODUCTION: (Fort Knox Reg 380-5, section IV, paras 6-10 and 6-11) a. Has equipment been approved to reproduce classified information?

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM

b. Are appropriate notices and procedures posted on or near equipment used to reproduce classified information?

c. Is a reproduction control sheet used to log the amount of classified material reproduced?

d. Is reproduction of classified material limited to only mission essential standard?

REMARKS:

---

9. SECURITY CONTAINER MANAGEMENT:
(AR 380-5, chaps 6 and 7; Fort Knox Reg 380-5, chaps 6 and 7)

a. Is classified information properly stored in GSA-approved security containers?

b. Are SF 700s posted in the mechanical drawer of each security container indicating individuals with knowledge of the combination and the contents?

c. Have containers used for storage of classified information or material been designated and a number or symbol annotated on the SF 700 affixed to the inside of each container?

d. Are safe combinations changed at least annually and as otherwise required?

e. Was the combination changed by the security manager?

f. Are safe combinations maintained in a master safe?

g. Are records of combinations assigned a security classification equal to the highest category of classified material authorized to be stored in the container?

h. Is the master combination at DOIM?

i. Is the SF 702 being filled out properly, indicating each time the security container is opened, closed, and checked?

j. Are end-of-day security checks conducted and recorded on SF 701 ?

k. Is there an Emergency Action Plan (EAP) posted on each container?

l . Are magnetic signs indicating when the container is opened or closed located on the front of each container?

m. Are security containers, ready for turnin, inspected for any left over classified, and are the combinations reset to the factory combination (50-25-50)? Are signed statements affixed to these containers attesting to the combination settings and inspection for classified material for the Property Book Officer?

REMARKS:

---

10. TRANSMISSION:
(AR 380-5, chaps 7 and 8; Fort Knox Reg 380-5, chap 8)

a. Are Courier Authorization cards (DD Form 2501) issued only to those individuals who carry classified information on a frequent basis?

b. Are Courier Authorization cards properly controlled and inventoried? Control log, current inventory, destructions, and out processing?

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM
			c . Are classified couriers briefed and given a statement on their responsibilities before being assigned a Courier Authorization card (DD Form 2501) or courier orders? Are their signed statements being maintained in their security personnel file? d. Are issued courier cards only valid for 2 years or less, and are individuals that need to carry classified being reevaluated annually? e. Are all assigned personnel aware of proper methods of transportation of classified information/material? Are proper controls such as double wrapping, registered mail, and locking brief cases enforced? f. Is a travel security and espionage briefing given to couriers traveling off the installation? g. Are couriers traveling OCONUS given a courier authorization letter to travel abroad with classified aboard a commercial aircraft? REMARKS: _____ 11. SECURITY EDUCATION AND AWARENESS: (AR 380-5, chap 9; Fort Knox Reg 380-5, chap 6) a. Does the command have a security education program that meets the criteria/objectives of AR 380-5, chapter 9? (Inspector has the option of asking "check on learning" security related questions to members of the command.) b. Does the program provide for continual re-enforcement of security? c. Are there records reflecting date, subject, and attendees for all education programs sessions? d. Are the sessions tailored to meet the education/awareness needs of the individual, as well as the activities mission? (1) Are initial briefings being conducted before access is granted? (2) Are debriefmgs being conducted to ensure all personnel are aware of security procedures and individual responsibilities regarding basic security disciplines? (3) Are all personnel receiving an annual SAEDA briefing? (4) Are all personnel receiving an annual OPSEC briefmg? (5) Are all personnel receiving an annual Disclosure briefing? (6) Are all personnel receiving an annual Information Security briefing? (7) Are all personnel receiving an annual AR 381-10 briefing? (8) Are all personnel receiving an annual Information System Security briefing? (9) Are all personnel receiving an annual AT/FP Level l briefing? (10) Are individuals traveling abroad or PCSing abroad receiving a foreign travel and force protection briefing? For those with access to SCI, have they received an SCI brief? (11) When an individual is authorized to hand carry or escort classified material, locally, inside CONUS and OCONUS? (12) When an individual is indoctrinated into different SCI programs, i.e., SAP, NATO, CNWDI, etc., is there a tailored security education briefing?

INSPECTION CHECKLIST (continued)

FUNCTIONAL AREA:	SUBJECT AREA:
Information Security	Information Security Program, AR 380-5

YES	NO	N/A	INSPECTION ITEM
			(13) Are supervisors and individuals informed of their responsibilities?
			e. Are security awareness posters sufficiently displayed throughout the activity to remind personnel of their responsibility to safeguard classified material?
			f. Is FK Poster 380-5-1 posted on the commander's bulletin boards to identify the command's Security Manager?
			REMARKS: _____
			12. VIOLATIONS AND INFRACTIONS: (AR 380-5, chap 10, and Fort Knox Reg 380-5, chap 1)
			a. Are possible and actual security violations being reported immediately to the Security Manager/Commander and Security Division, DPTMS?
			b. Are preliminary inquiries conducted per policy and regulations? Is a system in place to conduct preliminary inquiries?
			c. Are completed preliminary inquiries maintained on file for 2 years?
			REMARKS: _____

(This page intentionally left blank)

Appendix D
Entry Exit Inspection Procedures

D-1. Who is to be Inspected. All individuals entering or exiting the building during the inspection period, regardless of rank or grade, are subject to inspection by designated personnel.

D-2. The Purpose of the Inspection. Inspections will be conducted for the sole purpose of detecting and deterring the unauthorized introduction or removal of classified information. Inspections will not be used to target, single out, harass, or otherwise treat any individual differently than other individuals entering and exiting the activity.

D-3. What to Look for. Inspector personnel will examine envelopes, packages, diskettes, diskette containers, and other ADP media, tapes, films, microfiche, etc., likely to contain classified material. Sealed envelopes and packages are also subject to inspection. If an individual refuses to open a sealed envelope or will not allow the inspector to open a sealed envelope, he or she will be asked for written courier orders, DD Form 2501, or other proof of authorization to hand carry classified material. If the person does not have such authorization, the incident will be recorded, and they will be referred to the Security Division, DPTMS, for further action.

D-4. What is to be Inspected. While inspections are conducted, authorized personnel will inspect all briefcases, luggage, athletic bags, packages, shoulder/handbags, and other similar containers carried in to and out of the activity by visitors and employees. Inspectors will not open or handle a woman's shoulder/hand bag. The woman will be asked to open her bag and rearrange or remove all items necessary to allow the inspector to view the contents. Personnel conducting the inspections are expected to use discretion in inspecting any item that could reasonably be expected to contain classified information.

D-5. What Will Not be Inspected. Inspectors will not search items that are obviously personal, such as wallets, change purses, clothing, or cosmetic cases. Inspector personnel will not inspect the individual's person.

D-6. How to Inspect. Personnel designated to conduct inspections will be polite, professional, and courteous at all times. During the designated period, inspectors will inform each person to be inspected of the requirement to inspect items brought in to and out of the facility.

D-7. Methods of Inspection. Either of two methods will be used: random or continuous. Once the method is determined by the security official, inspectors will consistently follow that method during that particular inspection period (i.e., if a random inspection of every third person is selected, every third person will be inspected). An inspection log will be maintained by the inspectors and turned in to the inspection supervisor at the end of the inspection period. This log will consist of:

a. Name of the inspector.

b. Date, time, and location of inspection.

c. Method of inspection (random or continuous).

d. Sign in and out sheet for all personnel entering or exiting the activity during the inspection period. If random is the method of inspection chosen, inspectors will place an asterisk beside the name of individuals inspected.

e. Comments/problems.

D-8. Procedures in the Event Classified Material is Discovered. If classified information is discovered, the individual inspected will be asked to produce courier orders, DD Form 2501, or other documented proof of authorization to hand carry classified material. If the individual does not have such authorization, the incident will be recorded, and they will be referred to the Security Division, DPTMS, for further action.

D-9. Brief Inspector Personnel. Prior to commencement of the inspection, inspector personnel will be briefed on these procedures by the SM/official. Throughout the inspection period, inspector personnel are free to seek additional guidance or assistance from the activity security official.

Appendix E
Example of Courier Duties and Responsibilities Briefing

General Instructions.

E-1. As a designated courier of classified material, you are authorized to hand carry or escort material while traveling between your duty section and (be as specific as possible on area of limitations, i.e., Fort Knox, Installation Operations Center, Fort Knox DOIM, HQ TRADOC, etc.,). In some situations, you may not have a specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become the custodian of that information.

E-2. All government employees (military and civilian) are subject to Title 18, United States Code, which deals with unauthorized release of national security information. As a courier, you are solely and legally responsible for protection of the material in your possession. This responsibility lasts from the time you receive the material until it is properly delivered to the station, agency, activity, unit, or individual listed as the official addressee.

E-3. The intent of this briefing is to help you become familiar with your responsibilities as a courier, duties as a custodian of classified material, and the security and administrative procedures governing the safeguarding and protection of classified material. You must also familiarize yourself with the provisions of AR 380-5, paying special attention to the following areas:

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

b. **Storage.** Whenever classified material is not under your personal control, it will be guarded or stored in a General Services Administration (GSA)-approved security container. You will **NOT** leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, or storage compartments in the passenger section of commercial transportation (plane, bus, or train). You will **NOT** store the material in detachable luggage racks or aircraft travel pods. You will **NOT** pack classified material in regular checked baggage. Retention of classified material in hotel/motel rooms or personal residences is prohibited. Safety deposit boxes and room safes provided by hotels/motels do not provide adequate protection for classified material. Advance arrangements for proper overnight storage at a US Government facility or, if in the United States, a cleared contractor facility, is required prior to your departure. Arrangements are the responsibility of the activity authorizing transmission of the classified material.

c. **Preparation.** Whenever you transport classified information, it must be enclosed in two opaque, sealed wrappings (envelopes, boxes, or containers) without metal bindings. While traveling, a briefcase will not be used as the outer wrapping. The inner envelope or container shall be addressed to an official government activity, stamped with the highest classification of the material contained, and placed inside an outer wrapping, envelope, or container. If transporting on post, the inner wrapping can be the classified cover sheet, indicating the highest level of classified material instead of a sealed wrapping. The second or outer wrapping envelope or container will be sealed and addressed to the proper government agency. The second, outer wrapping, envelope, or container will **NOT** be stamped or marked with classification markings. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission. Receipts will be exchanged, when and if required.

d. **Hand Carrying.** The authorization statement contained in your orders (courier designation) should ordinarily permit you to pass through passenger control points within the United States, without the need for subjecting classified material to inspection. Except for customs inspections only, airports have established screening points to inspect all hand carried items. If you are hand carrying classified material in envelopes, you should process through the ticketing and boarding procedures in the same manner as other passengers. When the sealed envelopes are carried in briefcases, the case may be routinely opened for inspection to ensure no weapons are concealed. The sealed envelope may be checked by x-ray machine, bending, flexing, and weight. It should not be necessary for the screening official to open the envelope. 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. If you are denied boarding, contact either the activity authorizing transmission, receiving activity, nearest Defense Courier Service Office, or nearest US Embassy or Consulate to report your situation and request further guidance. **UNDER NO CIRCUMSTANCES** should you permit the screening official to open sealed envelopes or read any portion of the classified document as a condition for boarding.

e. **Escorting.**

(1) 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 and the airline involved. You will report to the airline ticket counter prior to starting your boarding process. You will be exempt from screening. If satisfied, the official will provide an escort to the screening station and exempt the container from physical inspection. If the official is not satisfied, you will not be permitted to board and are no longer subject to further screening. **UNDER NO CIRCUMSTANCES** will the official be permitted to open or view the contents of the sealed container.

(2) The actual loading and unloading of bulky material will be under supervision of a representative of the airline; however, you or other appropriate cleared individuals shall accompany the material and keep it under constant surveillance during the loading and unloading process. Appropriately cleared personnel should be available to assist in

surveillance at any intermediate stops, when the plane lands, and when the cargo compartment is opened. Coordination for assistance is the responsibility of the activity authorizing the transmission of the material, but it is your responsibility to ensure this coordination has been accomplished.

(3) 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 material, nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information.

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

f. **Preferred Method** of transmitting classified information is by utilizing the SIPRNET. This will cut down on the possibility of improper disclosure and the loss of classified information.

E-4. If you have any questions concerning the security protection of classified or sensitive material entrusted to you, contact your security manager, the activity authorizing transmission, the receiving activity, the nearest Defense Courier Service Office, or the nearest US Embassy or Consulate.

UNDERSTANDING OF COURIER DUTIES AND BRIEFING VERIFICATION
(Prior to Receiving DD Form 2501)

I, ____(Printed Name and SSN)_____have been briefed on and understand the following:

1. My Courier Authorization (DD Form 2501) can only be used when transporting classified material by ground transportation or military aircraft.

2. The packaging requirements for classified material, as outlined in AR 380-5.

3. The custody and storage requirements for classified material, as outlined in AR 380-5.

4. I will not discuss or view classified material in public areas or with unauthorized persons.

5. I must use the most direct route to my destination.

6. My DD Form 2501 has an expiration date, and upon expiration, it must be turned in to my security manager for destruction.

7. My DD Form 2501 is only valid while I am assigned to my current position, and upon release from my current position, it must be turned in to my security manager for destruction.

8. I must participate in a "show" inventory of the DD Form 2501 at least semi-annually.

9. If my DD Form 2501 is lost or misplaced, I must immediately report this to my security manager.

10. I know who my security manager is and how/where to locate him/her.

11. I will immediately report any unusual incident(s) to the local Counter Intelligence Officer or my security manager.

By my signature, I verify the listed items were briefed to me and I understand my duties and responsibilities as a courier of classified material. I further verify that: (1) I have thoroughly read Chapter 8 of AR 380-5 and understand my responsibilities described. (2) I understand the consequences of improper or inappropriate handling of classified material while performing my duties as a courier.

SIGNATURE _____ DATE _____

UNDERSTANDING OF COURIER DUTIES AND BRIEFING VERIFICATION
(Temporary Written Authorization)

I, (Printed Name and SSN) have been briefed on and understand the following:

1. My written authorization can only be used when transporting classified material by ground transportation or military aircraft.

2. The packaging requirements for classified material, as outlined in AR 380-5.

3. The custody and storage requirements for classified material, as outlined in AR 380-5.

4. I will not discuss or view classified material in public areas or with unauthorized persons.

5. I must use the most direct route to my destination.

6. My written authorization is temporary and has an expiration date, and upon expiration, it must be turned in to my security manager for destruction.

7. My written authorization is only valid while I am assigned to my current position, and upon release from my current position, it must be turned in to my security manager for destruction.

8. If my written authorization is lost or misplaced, I must immediately report this to my security manager.

9. I know who my security manager is and how/where to locate him/her.

10. I will immediately report any unusual incident(s) to the local Counter Intelligence Officer or my security manager.

By my signature, I verify the listed items were briefed to me and I understand my duties and responsibilities as a courier of classified material. I further verify that: (1) I have thoroughly read Chapter 8 of AR 380-5 and understand my responsibilities described. (2) I understand the consequences of improper or inappropriate handling of classified material while performing my duties as a courier.

SIGNATURE _____ DATE _____

TEMPORARY COURIER AUTHORIZATION

Security Manager's Office Symbol — Date Authenticated

MEMORANDUM FOR (Office material is to be picked up from)

SUBJECT: Authority to Hand Carry Classified Information – Courier Designation

1. The following individual is authorized to pick up and transport classified material, including for (your organization):

   a. Full Name.

   b. Rank and SSN or ID Number.

   c. Type of ID.

   d. Verified Clearance Level.

   e. Pickup point. (i.e., Fort Knox Installation Operations Center, DPTMS, and DOIM).

   f. Limits of Authorization Area. In and around the confines of Fort Knox, KY.

   g. Expiration Date (cannot exceed 30 days from authentication date).

   h. Authority. AR 380-5, Chapter 8, and Fort Knox Reg 380-5, Chapter 8.

2. All security violations are to be immediately reported to one of the following:

   a. Security Division, DPTMS, 4-1655/6170.

   b. Installation Operation Center, 4-5151.

3. Point of contact is the undersigned at (security manager's phone number).

SECURITY MANAGER
Signature Block

Appendix F
Instructions for the Completion of Standard Form 311

BLOCK #

1. Period Covered. (i.e., 1st Qtr, FY07).

2. Your Unit or Directorate.

3. Security Manager or Preparer's Information.

4. and 5. N/A.

6. This section pertains to documents your unit or directorate created at all levels of classification. It includes SAPs and SCI. It does not include any copies made. In order to fully understand how to fill this area out, you must understand what ORIGINAL CLASSIFICATION and DERIVATIVE CLASSIFICATION is and the difference between them.

7. This section refers to written requests that your activity review classified information for the purpose of declassifying such data. Complete the area under "Declassification Decisions," reporting the amount of pages only. Additionally, this area must be broken out into material created prior to 1976 and information created from 1976 to present. If fully or partially granted, the total should appear in Block #8.

8. Automatic declassification refers to the program established under section 3.4 or Executive Order 12958 and amended by EO 13142, which requires that all files of permanent historical value, that will reach 25 years old by October 2001 be declassified or exempted from automatic declassification prior to 17 October 2001. We must report statistics on the amount of material reviewed, declassified, or exempted from automatic declassification by page count. Systematic review refers to the program under which classified, permanently valuable records exempted from automatic declassification are reviewed for declassification. The figures reported should indicate the combined total of pages under BOTH the systematic and automatic declassification programs. However, in Block #10, indicate the amount of material that was created after 1 January 1976. (This figure will be counted under the Systematic Declassification Program.)

9. The amount of formal inspections, surveys, or program reviews you conducted on yourself or on subordinate units.

10. Include information noted above and any other information you feel is needed to elaborate or explain any information provided.

(This page intentionally left blank)

Appendix G
Secret Internet Protocol Router Network (SIPRNET)

G-1. Requirements.

- Establish a SIPRNET site security SOP.

- Follow the requirements and procedures in AR 25-2, AR 380-5, and applicable Army and DOD Regulations.

- Maintain an access roster of all authorized users.

- Ensure all authorized users possess individual accounts (no generic/group accounts).

- Use the Knox SIPRNET for official government business only.

- Unauthorized changes to an approved SIPRNET connection may result in the loss of network connection.

- Authorized users must have the proper security clearance (SECRET) and an authorization based on an established need-to-know.

- SIPRNET passwords are considered classified SECRET.

- Use of another's user ID and password is prohibited and will be considered a security violation.

- All information system components must be labeled IAW published security directives.

- All SIPRNET equipment will be protected at the SECRET level IAW AR 380-5.

- Cell phones should not be allowed in the area when the SIPRNET is operational.

- All data on the SIPRNET should be marked. When using information that is not properly marked, it is your responsibility to determine appropriate classification prior to incorporating information in a document you create. You cannot assume it is unclassified just because it is not marked.

Magnetic Media, storage media including removable hard drives, diskettes, zip/jaz disks, and CD ROMS (recordable and non-recordable) introduced into SIPRNET systems will be labeled and protected as SECRET information. Storage media will be labeled with an SF 707 (SECRET) label and will be secured in a GSA-approved storage container.

- SIPRNET drop lock boxes will be secured with an approved combination lock. Combinations will be changed once a year or when an individual no longer has a need to know the combination or leaves the organization. Complete an SF 700. Post the SF 700 at each drop box.

- Removable media (e.g. hard drives, diskettes) must be degaussed and destroyed when no longer needed. The media will not be introduced into any unclassified system.

- All classification markings must be removed prior to equipment being transferred or turned in.

G-2. Users.

- Prior to operating the SIPRNET, ensure everyone in the room is cleared to view classified information and has a valid need to know.

- Close all blinds and lock doors.

- Retrieve the classified laptop or removable hard drive and SIPRNET key from the safe if your SIPRNET is not already keyed and in an open storage room.

- When the SIPRNET is keyed or the NSA-approved lock box is unlocked and the Esthernet cable is connected to the personal computer, the system is live and classified.

- This is a SECRET system and cannot be left unattended. Locking the office door does not meet security standards. A cleared individual must be with the system at all times while the system is active.

- Mark the media with the appropriate classification.

- Only create media or documents when it is really necessary to preclude the additional administration involved.

- Return the hard drive, laptop, media, SIPRNET key, and documents to the GSA-approved safe after completion.

G-3. SIPRNET Incidents.

- All real or suspected security incidents will be reported to the Information Assurance Security Officer, DOIM. Investigation procedures outlined in AR 380-5, Chapter 10, will be followed for SIPRNET security incidents. The SIPRNET network connection will be disabled during an incident.