SDDC Regulation 380-5

Security:

Military Surface Deployment and Distribution Command (SDDC) Information Security Program

Headquarters, Military Surface Deployment and Distribution Command
709 Ward Drive
Scott AFB IL 62225-1604
26 March 2010

UNCLASSIFIED

SUMMARY of CHANGE

SDDCR 380-5
Military Surface Deployment and Distribution Command (SDDC) Information Security Program

This is a new issuance that must be reviewed in its entirety.

DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
709 WARD DRIVE, SCOTT AIR FORCE BASE IL 62225-1604

SDDC REGULATION NO. 380-5 — 26 March 2010

Security

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND (SDDC) INFORMATION SECURITY PROGRAM

1. Purpose. This regulation provides policy and prescribes procedures for implementation of AR 380-5, Department of the Army Information Security Program.

2. Applicability. This regulation is applicable to all Military Surface Deployment and Distribution Command (SDDC) staff elements and subordinate commands/activities to include Army Reserve units under the operational control of SDDC during mobilization or contingencies, and provides supplemental guidance to referenced regulations.

3. Policy.

a. The SDDC Information Security Program will follow the intent as well as the letter of AR 380-5, Department of the Army Information Security Program. Security is a primary

responsibility of this command. Commanders and supervisors at all levels are responsible for the security practices of assigned personnel.

b. Original classification of information may only be exercised by a designated Original Classification Authority (OCA). The Commanding General (CG), SDDC, is authorized to originally classify information up to and including Secret. All other personnel with access to classified information are only authorized to perform derivative classification actions.

c. Centralized storage will be maintained in the Classified Document Repository (CDR) over all classified documents. *Exception*: Top Secret documents will be stored in approved security containers with all necessary supplemental controls. Top Secret documents will be maintained in the Command Operations Center by a designated Top Secret Control Officer. Classified documents up to Secret may be maintained within the respective staff element or office of primary responsibility when mission requirements necessitate it and storage capability is in accordance with AR 380-5, Chapter 7. All classified material will be stored as required in approved security containers. The holder of the document/material will provide G-2 the following information:

(1) Staff/office

(2) Location (Building/room numbers)

(3) Container type and number

(4) Container lock type and number

(5) Classified document/safe custodian and alternate appointment orders

d. Commanders of subordinate activities are authorized to further specify classified storage at their respective locations consistent with requirements of AR 380-5, Chapter 7, the AMC Supplement to AR 380-5 and this regulation. Open storage is not authorized within SDDC except in those instances where facilities meet or exceed SCIF or vault regulatory standards.

e. Information proposed for posting on SDDC web sites or disclosure to open sources will be reviewed for information security sensitivity and operations security implications prior to such posting or release. The information must also be cleared for release by the Command Affairs Office in accordance with requirements of AR 360-1, The Army Public Affairs Program.

e. All SDDC activities that maintain classified information will implement a system of Information Security Program management controls. AR 380-5, Appendix F, provides a baseline Management Control Evaluation Checklist. You may obtain a current G-2 Command Inspection Checklist upon request. Commands and activities may include other applicable requirements of AR 380-5 to evaluate the effectiveness of their information security programs. Checklists will be completed annually and a copy of the report will be provided to the Deputy Chief of Staff, G-2. Additionally, each subordinate command/activity that maintains classified

information will undergo an annual Information Security Program inspection by G-2/S-2. Group Commanders will inspect their subordinates IAW SDDC HQ inspection checklists.

4. Responsibilities.

a. The Deputy Chief of Staff, G-2, will exercise staff supervision over the provisions of this regulation and will designate the following personnel in writing:

(1) SDDC Security Manager/Alternate.

(2) Alternate Top Secret Control Officer.

(3)..Classified Document Reproduction Control Officer.

(4) SDDC Foreign Disclosure Officer/Alternate.

b. The Deputy Chief of Staff, G-3, will designate in writing the following personnel:

(1) Alternate Top Secret Control Officer.

(2) In addition, G-3 will establish and activate a Classified Document Control Activity for all command post exercises.

c. The Deputy Chief of Staff, G-6, will designate in writing (when required) the following personnel:

(1) Top Secret Control Officer.

(2) Top Secret Reproduction Control Officer/Alternate.

(3) CDR Custodian/Alternate.

d. Staff principals and commanders of subordinate units will:

(1) In addition to the relevant designations above, appoint in writing the following personnel and forward a copy of all written appointments and subsequent changes to G-2 and a copy of the Top Secret Control Officer/Alternate to the Top Secret Control Officer, G-6, within 30 days of designation:

(a) Activity/Command Security Manager/Alternate.

(b) Classified Document/Safe Custodian/Alternate.

(2) Designate positions which are identified as "non-critical sensitive" or "critical sensitive" as required, and submit a request for personnel action through servicing civilian personnel office channels.

(3) Report credible derogatory information on all unit personnel, regardless of whether or not they possess a security clearance, to G-2 in accordance with AR 380-67.

5. Procedures.

a. SDDC Security Manager will:

(1) Administer provisions and requirements of regulations governing the safeguarding, classifying, reproducing, transmitting, re-grading, declassifying, destruction and emergency planning of classified information.

(2) Administer a security education and training program in accordance with the following minimum standards:

(a) All SDDC commands and activities will establish information security training programs. These programs will be aimed at promoting quality execution of security protocols by command personnel.

(b) All personnel assigned or attached to SDDC will be provided initial security instruction on information security, operations security and facility security fundamentals within 30 days of arrival, or prior to access of classified or sensitive unclassified information. Personnel will complete refresher training at least annually thereafter. Persons with access to classified information must also receive a personnel security briefing prior to being granted access and before departing on foreign travel.

(c) Cleared personnel must report all foreign travel to or through countries designated in AR 380-67, Appendix H, Table H-1 to the security office in advance of the travel being performed. In addition to the reporting data listed in AR 380-67, paragraph 9-203, individuals will also report mode of travel, contact persons at destination(s), and foreign addresses and telephone numbers if available.

(d) Security managers/officers are encouraged to use, in whole or in part, G-2 web-based security education information to facilitate these minimum training requirements available on the SDDC Portal at https://portal.sddc.army.mil/g2/default.aspx.

(3) Review and process challenges to classification decisions in accordance with the provisions of AR 380-5, paragraph 2-22.

(4) Conduct annual inspections of each organizational element authorized to maintain classified material and participate as a subject matter expert in the Organizational Inspection Program in accordance with AR 1-201 and requirements of this regulation to examine, assess and evaluate information security program compliance.

(5) Periodically conduct unannounced Information Security Program inspections of organizational elements maintaining classified, For Official Use Only and Privacy Act

information for compliance with material safeguards and custodial requirements. Reports of discrepancies will be reviewed with responsible officials and maintained in unit/activity files until the next inspection is performed.

b. G-2 Security Division will:

(1) Validate clearances and/or security eligibility for the CG, SDDC during in-processing of all military, civilian and contractor personnel.

(2) Provide a security access roster to each SDDC director or staff principal and subordinate commander upon request.

(3) Administer actions identified in AR 380-l3, Acquisition and Storage of Information Concerning Non-affiliated Persons and Organizations.

c. Subordinate Activity/Command Security Managers will:

(1) Maintain a copy of AR 380-5, AR 380-67, AMC Supplement to AR 380-5 and this regulation with all changes for ready reference.

(2) Assist each supervisor in training personnel in the specific security requirements of their position and administer refresher training at least annually.

(3) Ensure each newly assigned member is scheduled for initial security and annual refresher training regardless of their level of access to classified information.

(4) Verify that all new employees have signed Standard Form (SF) 312, Classified Information Nondisclosure Agreement, prior to access of classified information.

(5) Develop and implement a system for validating proper marking in accordance with the Authorized Classification and Control Markings Register and AR 380-5, Chapter 4 on incoming and outgoing classified documents/messages and all working papers. (See Appendix C of this regulation for additional guidance).

(6) When required, submit requests for the designation of SDDC staff element classified material escorts and couriers to G-2. Commanders/supervisors of subordinate commands/activities will appoint escorts and couriers, as required. Approved escorts and couriers will be designated via DD Form 2501, Courier Authorization.

(7) Ensure appropriate action officers conduct a semiannual review of all classified documents during the first week of April and October of all classified documents for which they are responsible. The reverse side of each document retained in classified files will be annotated with the date of the review, initials of the reviewer and the word "Retain." Verify re-grading or declassification actions. If destruction is indicated, documents will be immediately pulled and safeguarded until properly destroyed in accordance with existing regulations. Discrepancies that cannot be reconciled immediately will be promptly reported to the G-2 in writing. A report in

accordance with Appendix G will be submitted to G-2 depicting the number of retained and destroyed documents by classification level.

(8) Ensure security container custodians and all alternates are listed on SF 700 (Security Container Information); SF 702 (Security Container Check Sheet) is properly completed in accordance with AR 380-5, paragraph 6-10 each time the safe is opened, closed and checked; an entry must be annotated for each day of the month - "Not Opened" will be used for inactive days; safe combinations are changed in accordance with AR 380-5, paragraph 7-8; emergency destruction and evacuation instructions are posted on the side of the security container and G-2 is notified whenever a security container is moved into, or out of, a command/activity location.

(9) Establish procedures to ensure all sensitive materials, classified and unclassified, are properly stored when not in use.

(10) Ensure all outgoing documents to be mailed are prepared and marked in accordance with current regulations and hand-carried to the CDR for processing and dispatch. Documents will not be sealed prior to delivery to the CDR.

(11) Ensure all Top Secret documents received are hand-carried to the CDR for entry in the register and safeguarded as necessary.

(12) Ensure personnel assigned to open first class mail are cleared for access to Secret or higher classification.

(13) Establish procedures for a daily security check at the close of business. Individuals performing the check will initial SF 70l which will be posted by each activity on the outside of primary exits/entrances, to include required individual office and cubicle areas. Whether or not the activity stores or handles classified information shall not preclude the posting and use of SF 701. (See Appendix I for sample SF 701.)

(14) Ensure all equipment and peripherals such as copiers, facsimile machines, typewriters and printer ribbons, drafts, carbon sheets, computers, notebooks, portable data managers, flash pen drives or any other medium used to transcribe classified information are protected consistent with the intent of AR 380-5.

(15) Provide and document leisure and official duty foreign travel security briefings for military, civilian and contractor personnel.

(16) Immediately report all known or suspected security violations.

(17) Ensure each classified document/safe custodian, prior to relief from such duty conducts a joint inventory of all classified documents on hand with their successor. The results will be recorded and certified by the signatures of both individuals. Report to G-2 any discrepancies that are not satisfactorily reconciled.

(18) Maintain a copy of AR 380-l3 and ensure that each individual, whose duties include or may logically extend to the acquisition, reporting, processing or storage of information concerning non-DOD affiliated persons and organizations, is familiar with this regulation.

(19) When tasked by G-2, review unit tables of distribution and allowance to ensure accurate position sensitivity coding for civilian/military position descriptions and forward validated status to the Deputy Chiefs of Staff, G-1/4 and G-2. Notify G-2 when a military or civilian member occupying a sensitive position is reassigned to another SDDC staff element or leaves the command/activity.

(20) Verify the change of security container combinations in accordance with paragraph 22 below.

(21) Request written secure room certification to operate/store classified systems/information from G-2 for all locations. Group Commanders will inspect subordinate unit locations and provide written reports of local findings to the Deputy Chief of Staff, G-2 for review and CG approval.

(22) Inspect security equipment (vaults and security containers) when taken out of service for turn-in or repair to ensure classified material is not left in the containers. This will include removal of drawers and visual inspection of the interior. A written, signed record certifying that this inspection has been accomplished and that no classified material remains will be furnished to G-2 and maintained on file for 2 years. Verify that combinations have been reset to the standard combination of 50-25-50 for safes and doors and 10-20-30 for combination padlocks. Post a deactivated sign on the exterior of the container/door as appropriate.

(23) Thoroughly inspect data processing equipment used for classified information prior to turn-in for any residual classified information. G-6 personnel will oversee the erasure of all memory banks and inspect software (discs, tapes, portable drives, etc.) to ensure they contain no classified material. Notify G-2 prior to removing equipment that was used for classified processing.

(24) Ensure emergency evacuation/destruction plans are current, include procedures for prioritizing destruction, and are tested on an annual basis.

(25) Coordinate classified conferences or presentations with designated sponsors.

(26) Establish procedures to ensure that individuals who are permanently departing SDDC return office and building keys to the appropriate key control custodian, and that if they had access to security containers, the classified document/safe custodian is notified of their departure.

(27) Inspect subordinate commands annually.

d. Supervisors will:

(1) Ensure personnel are properly cleared and have a legitimate need to know.

(2) Review annually with the organization security officer, all positions to determine the correctness of the position sensitivity assigned and certify in writing to G-2 that current designations are accurate as listed or advise of necessary changes.

(3) Ensure all persons under their supervision are thoroughly familiar with their security responsibilities and are knowledgeable of the portions of AR 380-5 and this regulation as required by their specific duties.

(4) Verify that new employees have signed SF 312, Classified Information Nondisclosure Agreement, before they are given access to classified information.

(5) Continually evaluate employees who maintain a security clearance. Report all suspected or known derogatory information on individuals to G-2 or the local security office.

(6) Review and submit appropriate challenges to classifications in accordance with AR 380-5, paragraph 2-22.

(7) Include the management of classified and sensitive information as a critical element/item/objective in personnel performance evaluations, where deemed appropriate, in accordance with paragraphs 1-8 and 1-5c of AR 380-5.

(8) Ensure cleared personnel receive a termination briefing in accordance with AR 380-5, paragraph 9-15, (back side of SF 312) when access is terminated or prior to leaving the command.

e. The Top Secret Control Officer (TSCO) will:

(1) Comply with AR 380-5, paragraph 6-21, and all relevant provisions and requirements.

(2) Operate a CDR for materials that are not maintained by other staff principals and where appropriate, a NATO Sub-Registry.

(3) Maintain sealed combinations to security containers in use in SDDC staff elements and to doors of offices secured with a three-position combination lock. Alternate TSCOs will establish similar controls within their respective organizations.

(4) Ensure all Top Secret documents received are recorded, accounted for, and properly distributed or stored in the CDR.

(5) Establish operating procedures to ensure two-person integrity when handling Top Secret information.

(6) Perform Top Secret inventories semiannually in accordance with the provisions of AR 380-5, Chapter 6, Section III. Inventories will be conducted by the TSCO or alternate with a disinterested party, designated in writing, who is neither a TSCO, alternate, or subordinate to either official. Discrepancies that cannot be promptly reconciled will be reported immediately to

the G-2. A report in accordance with Appendix F of this regulation will be submitted to G-2 depicting the number of retained and destroyed documents by classification level.

f. Top Secret Reproduction Control Officer will:

(1) Obtain approval from the originator or higher authority before granting written permission to reproduce Top Secret documents and materials. This record will be maintained for the life of the copy and filed with the destruction certificate when the copy is destroyed.

(2) Verify compliance with reproduction limitations and special controls. Ensure copies are numbered serially and marked to indicate its copy number.

(3) Notify the TSCO when Top Secret material is reproduced and provide the TSCO the copies so they can be taken under control, and include a copy of the reproduction authorization.

g. Classified Document Reproduction Control Officer will:

(1) Establish procedures for the reproduction of classified material up to and including Secret. Procedures must limit the reproduction to that which is mission essential. Measures will be taken to negate or minimize any risk.

(2) Require that all reproduced classified documents, including those incorporated in working papers, be safeguarded and controlled as the original document.

h. The Classified Document/Safe Custodian will:

(1) Be properly cleared in accordance with AR 380-67 and maintain familiarity with custodial responsibilities specified in AR 380-5.

(2) Receive and dispatch classified and sensitive unclassified mail and check each incoming/outgoing classified document for proper markings (see Appendix C of this regulation). Protect registered mail as Secret material and certified mail as Confidential material until opened by appropriately cleared personnel. Secret working papers will be converted to permanent documents after 180 days, when filed permanently, or prior to release outside of the command (see AR 380-5, paragraph 6-24, for further guidance). Top Secret documents will be brought under control immediately after creation.

(3) Initiate Optional Form 23 (Chargeout Record) for each document removed from files. Transfer of Top Secret documents out of the activity must be accomplished on DA Form 3964 through the CDR.

(4) When locking a security container, spin the combination lock dial at least three times in each direction and attempt to operate the lock drawer handle to ensure the container is locked. A second individual will immediately check that the container is locked by also spinning the dial three times in each direction and attempting to operate the lock drawer handle. Complete SF 702 as appropriate.

(5) Ensure SF 702 is initialed each time the safe is opened/closed and checked. If the security container has not been opened, SF 702 will be annotated "NOT OPENED" for that particular day.

(6) Ensure reversible "Open/Secured" or "Open/Locked" signs are prominently displayed on all security containers.

(7) Change security container combinations when the container is placed into or removed from service, whenever an individual knowing the combination no longer requires access, when the combination has been subject to possible compromise, or at least annually. If assistance is required, contact the local security office. After a combination change, complete SF 700 and post Part 1 on the inside of the lock drawer of the security container. SF 700, Parts 2 and 2A, must be marked with the highest classification of material stored in the container. The custodian's name will be the first name listed on SF 700. Alternate custodians will be shown in descending order. Assistance rendered to make security container combination changes must not result in non-custodial personnel knowing the combination lock codes.

(8) Hand-carry all new security container combinations, properly recorded on SF 700, to the TSCO for safekeeping. Combinations classified Top Secret will be delivered with a completed DA Form 3964 for receipt purposes.

(9) Assist in the semiannual review of classified documents.

(10) Ensure that prior to relief from appointment as a classified document custodian, a joint inventory of all classified material in their possession is conducted with the successor custodian. The inventory will be in writing and certified by the signatures of the outgoing and incoming custodians.

(11) Post emergency evacuation/destruction plans conspicuously on the outside of security containers and provide a sufficient number of corrugated boxes specified in Appendix E of this regulation to hold materials for evacuation.

i. The individual will:

(1) Regardless of rank, grade, title, or position, be responsible for safeguarding defense information related to the national security to which they have access. Individuals will take personal possession of classified materials that they observe out of control, or otherwise in danger of unauthorized disclosure, and protect it until it can be turned over to a responsible official (e.g., the security manager/officer or the commander/director of the activity).

(2) Report to the proper authority (supervisor, security manager, G-2, or commander) security violations that could lead to unauthorized disclosure of classified and sensitive information. This responsibility cannot be waived, delegated, or in any other respect, excused.

(3) Fully comply with all security protocols outlined in AR 380-5.

j. Access, Control, Safeguard and Transmission of Classified Material.

(1) All personnel in possession of classified material are responsible to ensure that only appropriately cleared persons with a legitimate need-to-know are permitted access to such information. Classified information will be protected at all times, either by storage in an approved security container or having it under the direct personal observation and physical control of an authorized individual.

(2) Command activities at every level that access, process, or store classified information will establish a positive system of controls to ensure classified information is not inadvertently disclosed to unauthorized personnel, lost, or otherwise mishandled.

(3) All classified documents, files, folders, or groups of documents containing classified information will be conspicuously marked with the highest classification contained therein. Classified document cover sheets, SFs 703 (Top Secret), 704 (Secret), and 705 (Confidential), will be used for this purpose whenever classified material is not securely stored in approved security containers and/or equipment. Approved removable classified storage media such as compact discs, flash/pen drives, diskettes or other such devices will be affixed with SFs 706 (Top Secret), 707 (Secret) or 708 (Confidential), as appropriate.

(4) For the reproduction of classified material, see AR 380-5, paragraph 6-25. Within HQ SDDC, G-2 will approve the reproduction of classified material up to Secret and G-6 will designate reproduction machines to be used for that purpose. Commanders or directors of subordinate activities will establish similar controls.

(5) Top Secret material will not be reproduced except as provided for in AR 380-5, paragraph 6-25. In every case, the authority to reproduce Top Secret information must be designated in writing by the Top Secret Reproduction Control Officer, G-6, or other command official specifically appointed in writing to perform this function. Top Secret reproductions will be immediately taken under control by the TSCO.

(6) Classified materials will be stored in GSA-approved security containers adequate to prevent access by unauthorized persons and meeting the minimum standards specified in AR 380-5, Chapter 7.

(7) Personnel who process classified information on computers or other information processing systems will safeguard the information from inadvertent disclosure. Computer operators will log off prior to leaving their work station and computer-generated documents will be marked, controlled and safeguarded like other classified documents.

(8) For document marking, to include removable computer media, drives, etc., see Appendix B of this regulation, Authorized Classification and Control Markings Register and AR 380-5, Chapter 4.

(9) Working papers will be marked and protected in accordance with AR 380-5, paragraph 6-24. Top Secret working papers will be brought under control immediately.

(10) Preparation for transmission and transportation guidelines will follow AR 380-5, Chapter 8. All classified and accountable mail will be delivered unsealed to the CDR for dispatch.

(11) Classified recordings of voice or sounds on magnetic tapes will abide by the following:

(a) Have subject, date, time, recorder, classification and declassification instructions dubbed at the head of the recording and classification repeated at the end with identification of the original classifier (source document). Label affixed to reel and carton will also reflect above data.

(b) Bear the additional "Working Paper" marking if to be transcribed within 180 days. Upon completion of transcription, tape(s) will be degaussed. Arrangements for degaussing will be made with G-6.

(c) Be safeguarded and stored as classified documents.

(12) Classified slides, transparencies and other graphic materials will be marked in accordance with AR 380-5, Chapter 4, Section III.

(13) USB Flash/Pen drives and other similar portable/removable media are not authorized for use on government network systems.

(14) Documents and material received from outside SDDC.

(a) All registered and certified mail, and material delivered by courier/messenger or marked “To Be Opened by Addressee only” will be delivered unopened to the CDR so it may be handled under proper control.

(b) All certified mail will be stored and protected as Confidential material until opened by appropriately cleared personnel.

(c) All registered mail will be stored and protected as Secret material until opened by appropriately cleared personnel.

(d) If an addressee receives classified material that requires a receipt, the addressee will take it to the CDR so it may be handled under control.

k. Classified documents or materials removed for official business:

(1) Classified material will not be physically removed from SDDC facilities except when specifically authorized by G-2 or SDDC commanders/directors of subordinate activities.

Commanders/directors may assign administrative control functions prescribed in AR 380-5, Chapter 8, Section IV, to unit security managers/officers.

(2) Supervisors requiring personnel to perform classified escort or courier duty will request authorization in writing from their respective cognizant security offices. The use of a courier is strongly discouraged and will be authorized only as a last resort when material cannot be sent via mail or electronically. Requests must include name, grade, social security number of the candidate courier, classification of material, type of material (document, slides, computer cards, flash/pen drives, etc.) number and size of package(s), itinerary, and specific justification. Requests must be received by the security office at least 1 week prior to the courier mission.

(3) Appropriately cleared personnel may only be authorized to escort or hand carry classified material when the information is not available at the destination and other means of transmission or transportation, such as secure facsimile or authorized express mail carrier, do not satisfy operational requirements. See Appendix E for a listing of authorized overnight carriers. The listing is subject to change and should be verified with the local security office/G-2 when use is anticipated.

(4) Couriers/escorts will be designated on DD Form 2501, Courier Authorization, and briefed regarding additional requirements, such as material inventories, special authorization letters for OCONUS travel and security custodial responsibilities.

(5) Classified material may be carried aboard commercial passenger aircraft only in exceptional circumstances and when specifically authorized in writing. Use of non-U.S. flag carriers will not be approved as a mode of travel.

(6) All classified information will have the appropriate classification coversheet on top of the document when transporting from the printer to storage container to desks or meetings.

(7) For preparation of material for escort, hand carry, or other form of transmission, see AR 380-5, Chapter 8.

l. COMSEC Material. COMSEC handling and accountability will be in accordance with the provisions of AR 380-40 (Policy for Safeguarding and Controlling COMSEC Information) and TB 380-41 (Procedures for Safeguarding, Accounting and Supply control of COMSEC Material). All COMSEC matters will be coordinated with the Command COMSEC Custodian in G-6.

m. Classified Conferences or Presentations.

(1) Top Secret presentations are only authorized in approved locations. These areas will be designated in writing by G-2.

(2) Within HQ SDDC, all classified meetings or conferences will be held in classified conference rooms. Only those personnel with appropriate clearances will be authorized access. For other than in-house meetings, the G-2 will be promptly notified.

(3) Conference sponsors will ensure that:

(a) A roster of attendees showing the organization and security clearance of each is furnished to the cognizant security office for verification 3 working days, or as early as practical, prior to commencement of conferences or presentations. G-2 will assist with Joint Personnel Adjudication System (JPAS) visit requests for classified meetings/conferences.

(b) Cleared individuals are posted as required to provide positive access control during classified proceedings.

(c) An inspection is made of the conference room and adjacent spaces immediately prior to the start of the conference to confirm no unauthorized personnel or listening devices are present. Subject inspections will be conducted by a qualified physical security inspector. Contact G-2 or the local security office for assistance.

(d) The conference room door is closed at all times during on-going presentations. A sign will be posted on the external side of the door to alert personnel that a classified meeting is taking place. When utilizing conference rooms that do not have a structural sound attenuation equivalent to a Sound Transmission Coefficient (STC) of at least STC 45, and the meeting room is bordered by uncontrolled areas, a guard must be posted for the duration of the meeting to monitor hallways and adjacent areas while classified presentations are in progress to ensure no loitering/listening occurs.

(e) Conference speakers or presenters give the classification level of the information to be disseminated before and after each presentation.

(f) When audio equipment is utilized, it must be set at a volume that cannot be heard outside of the conference room.

(g) Information systems technicians and/or other assistants possess an appropriate level security clearance.

(h) Housekeeping of the area is performed after the meeting to ensure that no sensitive materials have been left behind.

n. Destruction of Classified Material.

(1) Classified material will be destroyed to preclude recognition or reconstruction of the classified information contained in or on the material. Destruction methods include burning, crosscut shredding, wet pulping, melting, mutilation, chemical decomposition, and pulverizing. Within SDDC, the preferred method of destruction for classified paper products is crosscut shredding. The crosscut shredding machine must reduce the material to shreds no greater than 1/32 of an inch (plus 1/64-inch tolerance) by 1/2-inch crosscut. Contact G-2 for a list of approved destruction equipment prior to any contemplated purchase.

(2) All Top Secret material will be accounted for and destroyed by the TSCO, CDR. Section C, DA Form 3964 will be used to record the destruction of Top Secret material. Destruction records are not required for waste materials (scratch notes, typewriter and printer ribbons, carbon paper, etc.) containing Top Secret information, unless that material has been placed on an accountability record. Destruction certificates need not be completed for Secret and Confidential material, except for NATO and foreign government documents, if destroyed in the presence of a witnessing official. For NATO or foreign government Secret material, two signatures are required on the record of destruction. NATO Confidential material does not require destruction records unless specified by the originator.

(3) Witnessing official for destruction of Top Secret material will have neither personal nor supervisory responsibility for the documents, and will not supervise or be supervised by the destruction official.

(4) All classified waste such as typewriter and printer ribbons, CDs, diskettes, carbons, drafts and other materials used in preparation of classified documents will be protected as classified material and handled and destroyed appropriately.

(5) Document destruction records shall be maintained on file for 2 years.

(6) For emergency destruction of classified material, see Appendix E of this regulation.

o. Visitor Control.

(1) When visitors require access to classified information, the SDDC sponsor will request the security office of the visitor's organization furnish the SDDC security office the visitor's security clearance data and purpose of visit through JPAS or via facsimile in advance of arrival.

(2) Foreign visitations will be coordinated and processed in accordance with AR 380-10 and paragraph 5p of this regulation.

(3) Sponsors must advise visitors regarding restrictions on personal electronic devices, such as cellular telephones, cameras, recorders, two-way pagers, and other devices capable of collecting or transmitting information while in designated controlled areas within SDDC. Sponsors will remind visitors that they are about to enter a controlled/restricted area and are subject to search. Sponsors must point out to visitors the posted signs warning of these restrictions and conditions.

(4) Visitors to HQ SDDC must sign in/out on DA Form 1999, Restricted Area Visitor Register, or a locally produced form. They will be issued a badge which they must display conspicuously on their front upper chest area in a manner that permits easy recognition. An escort will be provided full time for non-cleared visitors that require access within controlled/restricted areas.

(5) When non-cleared visitors are granted access to controlled areas, the sponsor will announce their presence in a clear and firm voice. If mechanical or electronic means of

announcing visitors is available (red light), it will be activated when the visitor arrives and turned off upon visitor's departure from the controlled area. Mechanical or electronic methods of announcing non-cleared visitors will not be used in place of the verbal announcement.

(6) Sponsors will ensure visitors return badges to the issuing point and retrieve personal restricted items that may have been temporarily secured prior to departing SDDC.

(7) SDDC personnel visiting other agencies where classified information is expected to be disclosed will request their local security office forward clearance verification to the sponsoring organization and will comply with local visitor procedures.

p. Foreign Disclosure. Foreign visits will be coordinated and processed in accordance with AR 380-10. All approved visits to SDDC must be vetted through G-2 (Foreign Disclosure and Personnel Security POCs) at least 30 days in advance or as early as practical.

q. Security Violations. Known or suspected violations will be immediately reported to the command/activity security manager/officer. The security manager/officer will immediately notify the head of the staff element and G-2, who will monitor the incident or take appropriate action in accordance with the requirements of AR 380-5, Chapter 10.

r. Controlled Unclassified Information. All material designated "For Official Use Only," "Sensitive But Unclassified," "DEA Sensitive Information," "DOD Controlled Unclassified Nuclear Information," or "Sensitive Information" as defined in the Computer Security Act of 1987 will be handled and safeguarded in accordance with AR 380-5, Chapter 5.

s. Privacy Act Information. All material containing personal information restricted by AR 340-21, The Army Privacy Program, will be afforded at least the protection required for information designated "For Official Use Only."

t. Emergency Planning.

(1) Commands and activities authorized to store classified material will ensure that emergency procedures are developed for its protection, removal or destruction in case of fire, natural disaster, civil disturbance, terrorist activities or enemy action.

(2) A sample evacuation/destruction plan is provided in Appendix D. Commands and activities will structure this plan to meet local security requirements and will update annually, or when necessary. The emergency plan will be briefed to all personnel involved, exercised at least annually, and placed in a sealed envelope affixed to the outside of security containers in a manner by which it is readily accessible.

(3) An emergency destruction plan for classified material is considered controlled unclassified information. To protect sensitive specifics of internal operating procedures, such as prioritization for destruction indicated in Appendix D, paragraph 4b, each activity will devise a coding system to enable personnel responsible for carrying out destruction procedures to readily identify materials according to their priority for destruction. The prioritizing of materials for the

purpose of emergency destruction should not be based solely on the classification level of the materials; equal consideration must be given to the potential effect loss of the materials would have on the national security.

(4) These emergency planning procedures do not apply to material related to COMSEC. COMSEC related questions should be addressed to the Command COMSEC Custodian in G-6.

u. Classified Material Entry/Exit Inspection. Inspections will be conducted in accordance with Appendix G.

Supplementation of this regulation is prohibited. The proponent of this regulation is the DCS for Intelligence and Security. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to HQ SDDC G-2, Attn: AMSSD-IS, 709 Ward Drive, Scott AFB IL 62225-1604.

FOR THE COMMANDER:

//Signed//
STANLEY H. WOLOSZ
COL, GS
Chief of Staff

Appendix A
References

Section I
Required Publications

AR 380-5
Department of the Army Information Security Program

AR 380-13
Acquisition and Storage of Information concerning Non-Affiliated Persons and Organizations

Section II
Related Publications

Executive Order 12958
Classified National Security Information

DoD 5200.1-R
Information Security Program

AR 1-201
Army Inspection Program

AR 25-2
Information Assurance

AR 25-55
The Department of the Army Freedom of Information Act (FOIA) Program

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

AR 340-21
The Army Privacy Program

AR 360-1
The Army Public Affairs Program

AR 380-10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380-13
Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations

AR 380-40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Materiel

AR 380-67
The Department of the Army Personnel Security Program

AR 381-12
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

TB 380-41
Security: Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material (FOUO)

Authorized Classification and Control Markings Register, Volume 2, Edition 1, Version 2.1

Army Materiel Command Regulation 380-14
Security Classification Guide

Army Materiel Command Supplement to AR 380-5
Department of the Army Information Security Program

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms

DD Form 2501
Courier Authorization

DA Form 1999
Restricted Area Visitor Register

DA Form 3964
Classified document Accountability Record

SF 312
Classified Information Nondisclosure Agreement

SF 700
Security Container Information

SF 701
Activity Security Checklist

SF 702
Security Container Checksheet

SF 703
Top Secret (Cover Sheet)

SF 704
Secret (Cover Sheet)

SF 705
Confidential (Cover Sheet)

SF 706
Top Secret (Label)

SF 707
Secret (Label)

SF 708
Confidential (Label)

OF 23
Chargeout Record

Appendix B
Classification Guidance

1. Original Classification.

a. Original classification is the initial determination that information requires protection against unauthorized disclosure. Only select senior officials are delegated the responsibility as an "Original Classification Authority" (OCA).

b. It is important to remember who has OCA and who does not. Sometimes individuals are persuaded to place classification markings on information which they "think" should be classified when it is not. One should never mark material as classified unless they have clear guidance to do so.

c. The SDDC CG is the only OCA for our command. He or she has been delegated up to Secret Classification Authority by the Secretary of the Army.

2. Derivative Classification.

a. The majority of employees in SDDC are derivative classifiers. This means that one incorporates, paraphrases, restates or generates in new form information that is already classified by an OCA. As a derivative classifier, one must refer to the classification of the source information and mark the newly developed materials accordingly.

b. When preparing a new document by copying, restating or paraphrasing information from a single classified document, observe and respect original classification decisions. Individuals are to carry forward the pertinent classification markings consistent with those found on the source documents.

c. When derivatively classifying from more than one classified source, use "Multiple Sources" as the Derived From value, and use the longest classification duration from among the sources as the Declassify On value. A list of the sources must be kept with the record copy of the document and, if practical, included with all copies of the derivative document.

3. Duration of Classification.

a. At the time of original classification, the OCA will establish a specific date or event for declassification based upon the duration of the national security sensitivity of that information. Upon reaching the date or event, the information will automatically be declassified.

b. If the OCA cannot determine an earlier specific date or event for declassification, that information shall be marked for declassification 10 years from the date of the original decision, unless the OCA otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision.

c. Declassification decision options for an OCA are:

(1) A date or event less than 10 years.

(2) A date 10 years from the date of the document.

(3) A date greater than 10 years but less than 25 years from the date of the document.

(4) A date 25 years from the date of the document.

4. Compilation of Information. Security classification must be determined by thoughtful consideration of all applicable elements. When partial information relative to those subjects is presented, the lowest classification consistent with adequate protection of the information concerned will be assigned. Similarly, a higher classification may be assigned to compilations of information if the compilation provides an added factor, which warrant higher classification than that of its component parts. Classification on this basis shall be fully supported by a written explanation that will be provided with the material so classified.

5. Security Classification Guides.

a. A security classification guide (SCG) is issued for each system, plan, program, or project in which classified information is involved. Refer to the United States Transportation Command SCG as the process owner for transportation information systems and to combatant commander SCGs for operational and planning information in their respective area of operation. SDDC cannot downgrade or declassify another command's information without permission from their security manager or OCA.

b. SDDC has no current Security Classification Guides internal to the command.

Appendix C
Guidelines for Checking classified Material for Proper Markings

(This list is not all inclusive; refer to the Authorized Classification and Control Markings Register, AR 380-5, Chapter 4)

1. General Documents/Correspondence.

a. Mark the overall classification on the top and bottom of the front cover, on the title page, on the first page, and on the outside of the back cover.

b. Mark each interior page at the top and bottom with the overall classification of its content, to include "UNCLASSIFIED" when no classified information is contained on the page.

c. If the document was originated after 1 August 1982, mark each section, part, paragraph, lead-in paragraph, or similar portion to show the level of classification it contains, or that it is “UNCLASSIFIED.”

d. Apply "CLASSIFIED BY" or “DERIVED FROM” markings, as the case may be, on the face of the document.

e. Apply re-grading or declassification dates or events on the face of the document.

f. Mark classified subjects and titles with the appropriate classification immediately following and to the right.

g. Mark each annex, attachment or major component likely to be used separately as a separate document.

h. Ensure record (file) copies show all markings on the face of the document.

i. If the "DERIVED FROM" marking shows "multiple sources" and the document was generated in SDDC, ensure the record copy completely identifies each source.

j. Ensure each document clearly shows an audit trail to the source document/original classifier, so if questions concerning classification, re-grading, and declassification arise at a later date, they can be promptly resolved.

k. Mark working papers as "WORKING PAPERS," date when created, mark with the overall classification and at each portion and apply declassification/re-grading instructions. Confidential and Secret working papers will be destroyed or converted to permanent documents within 180 days of creation, and Top Secret working papers will be controlled immediately.

m. When applicable, mark warning notices on the outside front cover, or first page if there is no cover, on transmittal documents, in portion markings and on interior pages. Warning notices

could be required in numerous circumstances. Refer to AR 380-5, Chapter 4, Section I for specific applications.

n. The following authorized control markings will be applied to documents when appropriate:

- ORCON means "Dissemination and Extraction of Information is Originator Controlled"
- PROPIN means "Caution-Proprietary Information Involved" – usually intelligence or vendor related
- NOFORN means "Not Releasable to Foreign Nationals"
- RELEASE TO means "Authorized for Release to" a specific country or entity

2. Special Types of Documents. Mark documents with component parts, letters of transmittal, classified by compilation, classified translations, marked for training, and files, folders and groups of documents in accordance with AR 380-5, Chapter 4, and Section II.

3. Electronically Transmitted Message. Mark the same as any other classified document with the following special provisions:

a. The overall classification/sensitivity of the message is the first item in the text of the message.

b. If the message is processed by an automated system that applies the overall and page markings, the markings must stand out conspicuously from the text. In older systems, this may be achieved by surrounding the markings with asterisks, stars, or other symbols.

c. A properly completed "Classified By" or "Derived From" line, reason, declassification instruction, and re-grading instruction (when applicable) must be included in the last lines of the message. This is a new requirement and will not apply to messages containing Restricted Data or Formerly Restricted Data.

4. Special Types of Material. Special marking instructions apply when classified/sensitive information is contained in some form not commonly thought of as a document. Included among this type of material are blueprints, schematics, maps, charts, photographs, negatives, slides, transparencies, video/sound recordings, and removable storage media. Marking provisions of AR 380-5, Chapter 4, and Section III, or other applicable regulations, will be met in a way that is compatible with the type of material involved.

Appendix D
Security Procedures for Secure Terminal Equipment (STE)

1. General:

a. This appendix provides guidance relative to the security considerations for placement and utilization of STE telephones in use throughout SDDC. For further information or assistance, contact the Deputy Chief of Staff, G-2 (physical/information security issues) or the Deputy Chief of Staff, G-6 (COMSEC Manager).

b. In order to understand how the STE works, an understanding of certain terminology is necessary. Below are listed some of the more frequently used terms:

(1) Classification Level. The highest classification level of information authorized to be transmitted over the unit. During a secure call the classification level displayed on each unit is the highest common level of classified information authorized to be transmitted by both units, and represents the authorized classification level for the call. It does not, however, establish "need-to-know" or the actual clearance level of the user.

(2) Fortezza Card (KSV-21). A storage device that holds information used to lock and unlock the secure capability of the unit. The secure capability is unlocked (enabled) when the Fortezza card is inserted into the unit, and locked (disabled) when it is removed. The Fortezza card, by itself, is unclassified as long as it is not left unattended within the vicinity of the associated unit. The basic intent of controlling the Fortezza card is to prevent unauthorized access to it and its accompanying unit.

(3) Key. Information used to initially set up and periodically change the operations performed in cryptographic equipment for purposes of encrypting or decrypting electronic signals.

(4) Keyed Unit. A STE loaded with a.key and in which a Fortezza card has been inserted. Note: Access to a unit that has been loaded and access to the Fortezza card associated with that unit constitutes access to a keyed unit.

(5) Unkeyed Unit. A STE which does not contain a key or a unit which has been loaded with a key but has the Fortezza card removed and stored separately for protection.

(6) Authorized Person/User. An individual granted access to an unkeyed unit for use as a standard telephone. Person(s) granted access to keyed units must possess the appropriate level of security clearance commensurate with the individual unit (see paragraph 4b(4) below).

2. Description: The STE is a dual-function telephone. It is an ordinary office telephone and functions over common telephone lines. It is also capable of securing voice conversations and data transmissions over those same lines. The unit is intended to replace the current office telephone as well as existing secure telephones. When used as a standard telephone the unit interfaces with any other telephone. When used in the secure mode the unit interfaces with

secure telephones. The secure capability of each unit is enabled and disabled by use of a removable Fortezza card (KSV-21). The STE is considered a Controlled Cryptographic Item (CCI) and is approved for securing voice and data transmissions at all levels of security classification. As the quantity of installed units increases, the capability to secure even unclassified (sensitive) voice/data will become available.

3. Security Procedures:

a. Security procedures for CCI are contained in Technical Bulletin 380-41. However, as an item of equipment expected to be located in the office environment at U.S. controlled facilities, security safeguards for STEs will be as specified in AR 190-51, Security of Unclassified Army Property (Sensitive and Non-sensitive), and paragraph 3-24, CCI. In essence, referenced paragraph requires that office doors, windows, etc., be secured when no permanently assigned personnel are physically present in the area.

b. The Fortezza card will be personally retained by individual users or locked in an approved security container. Storage of the Fortezza card within desks, filing cabinets, key depository boxes, etc., is not authorized within SDDC. Also, Fortezza cards should never be marked or labeled in any fashion which would identify the specific unit to which the card is matched (added precaution in the event of loss or misplacement).

c. The unit may be moved from one location to another by authorized persons for official purposes when authorized by the local commander or his/her designated security manager. During the move, the unit and associated Fortezza card may be carried by the same individual; however, the card cannot remain in the unit or be carried in the same case or container as the unit (see paragraph 1b(4) of this appendix).

d. Unkeyed STEs may be stored on desktops at the close of business within SDDC. The large volume of units within the command will make more stringent storage requirements impractical, although local commanders may deem otherwise in evaluating their particular environment.

e. The acquisition of anchor pads for securing STEs against theft and tampering is highly recommended as a proactive and cost effective security measure. Information on these and other security devices may be obtained by contacting G-6 or G-2.

4. Access Controls:

a. Unkeyed Units. Access will be limited to authorized individuals for the purpose of official government business. Access to office areas containing STEs may be granted by local commanders to non-authorized persons provided all of the following conditions are met:

(1) Access to the office area by non-authorized persons is in conjunction with maintenance, custodial duties, or other functions normally performed by such personnel in the area while unescorted.

(2) The office area is located in a U.S. controlled facility.

(3) All Fortezza cards are protected by being in the personal possession or custody of an authorized person or appropriately secured.

(4) Provided all conditions cited in paragraphs (1) through (3) above are met, there is no restriction on a non-authorized person using the un-keyed unit as a standard telephone.

b. Keyed Units:

(1) A keyed unit must be protected to the same classification level as the information authorized to be transmitted by the unit. At least one properly cleared individual (security clearance equal to or higher than that of the keyed unit) must be present to maintain positive control over the unit at all times when it is keyed.

(2) Users of the unit must possess a security clearance equal to or greater than that of the keyed unit (see paragraph 1b(1) of this appendix).

(3) Whenever a keyed unit is to be left unattended the unit must be disabled (unkeyed) by removing the Fortezza card and properly protecting it.

(4) In the event that an authorized user possesses a lower level of security clearance than that of the keyed unit, an alternate authorized individual possessing the appropriate clearance must be present to initiate the call, and will advise the party at the receiving end of the call of the security clearance level of the user to follow. The individual with the higher security clearance must remain with the unit through the entire call and disable the unit upon termination, by removing the Fortezza card.

Appendix E
Sample Classified Document Evacuation/Destruction Plan

(OFFICE SYMBOL) Date:

1. Reference. AR 380-5, Chapters 6 and 8.

2. Emergency conditions may warrant the evacuation or destruction of classified material stored in this activity. Upon order to execute from the Commanding General, Deputy Commanding General, Deputy Chief of Staff for Intelligence and Security, G-2, or other designated authority, the following procedures will be implemented by the custodians of classified material with assistance from persons designated below.

3. EVACUATION PROCEDURES.

a. Phase I – Planning Phase:

Activity Custodian:
(P) _____
Name/Grade/Office/Phone/e-mail
(A)_____
Name/Grade/Office/ Phone/e-mail

Emergency Evacuation/Destruction Team:
Team Ldr _____
Name/Grade/Office/ Phone/e-mail
Team Mbr _____
Name/Grade/Office/ Phone/e-mail
Team Mbr _____
Name/Grade/Office/ Phone/e-mail

Storage Locations and Volume:
_____
Bldg/Room/Container Number Linear Feet
_____
Bldg/Room/Container Number Linear Feet

Quantity and Location of (15" x 12" x 10") Boxes Required for Evacuation:
_____
Quantity/Location

Special Containers/Boxes required for Evacuation: _____

b. Phase II – Execution Phase:

Evacuation: Prepare classified material for transport utilizing corrugated boxes or other authorized means. Custodians and evacuation teams will transport the classified material to a specified location, and ensure compliance with all security considerations and requirements per AR 380-5, Chapter 6 and 8.

Destruction: Upon receipt of a valid order to destroy in-place implement Emergency Destruction Procedures. Designated, cleared personnel, will utilize any method available, i.e., burning outside in trash cans (for reasons of safety, consider using two people if this method is chosen), shredding or any other form of destruction sufficient to preclude reconstruction of classified information. If applicable, DA Form 3964, Classified Document Accountability Records, will be completed and retained by custodians. Time permitting, coordinate the use of available heavy duty shredders with staff elements that possess them. The heavy duty shredders for classified documents are located throughout building 1990. They are all clearly marked with classified labels and destruction signs.

c. Priorities for destruction are:

- Priority One: Top Secret Material
- Priority Two: Secret Material
- Priority Three: Confidential Material

_____
Commander/Staff Principal

_____
Unit Activity

Appendix F
Overnight Carriers

1. The following are General Services Administration approved overnight carriers (as of 1 February 2010) and may be utilized for the overnight transport of sensitive materials up to and including Secret:

- U.S. Postal Service Express Mail
- United Parcel Service
- D.C. Dyna, Inc
- Air Freight Plus, Inc.
- FEDEX Corporation
- AirNet Systems, Inc.
- Astar Air Cargo, Inc.
- CorTrans Logistics, LLC

2. The designated overnight carrier listing is subject to change and should be verified with local security officials whenever their use is anticipated.

Appendix G
Sample Report for Review of Classified Material/Top Secret Inventory

1. References:

a. AR 380-5, Department of the Army Information Security Program.

b. SDDCR 380-5, SDDC Information Security Program.

2. IAW requirements of referenced regulations, a semiannual review of classified documents on hand and a 100% inventory of Top Secret documents was completed on 21 April 2009 as indicated below:

Unit	Top Secret		Secret		Confidential	
	Destroyed	Retained	Destroyed	Retained	Destroyed	Retained
596th Trans Bde	0	0	15	67	6	10
834th	0	0	34	24	2	34
Total	0	0	49	91	8	40

(SAMPLE REPORT)

Appendix H
Classified Material Entry and Exit Inspection Procedures

1. Purpose. This appendix assigns responsibility and prescribes policy and procedure for planning and conducting classified material entry and exit inspections. SDDC staff principals and commanders/directors of subordinate activities are responsible to establish and maintain measures to deter and detect the unauthorized transfer of classified material from/to SDDC owned or leased installations and facilities.

2. Policy.

a. Classified material entry and exit inspections will be performed at a frequency sufficient to provide a credible deterrent. Facilities with activities that handle or store classified material will be targeted at entry/exit inspection points. In leased buildings, only those areas under SDDC control will be used as inspection sites. Inspections will be conducted in a manner that does not unnecessarily disrupt the entry and exit of persons employed by or visiting the activity/facility. Records of inspections will be maintained on file in accordance with AR 25-400-2, The Army Records Information Management System (ARIMS). Such records will be an item of interest during higher headquarters security inspections.

b. All SDDC activities will ensure the entry/exit inspection policy and procedure are made available to the entire workforce. Periodic reminders should be provided during training sessions or security briefings, and in bulletins and notices.

c. Entry/exit inspections will be conducted by trained security personnel.

3. Responsibility.

a. The Deputy Chief of Staff, G-2, will exercise staff supervision over the requirements of this policy and provide guidance and interpretation.

b. Commanders/directors of subordinate commands/activities may designate individuals to assist assigned/local security personnel in performing this function. However, non-security personnel must be in military grade O-3 and above, or civilian grade GS-11 or above and thoroughly trained to perform the required inspection.

4. Procedures.

a. Upon approval of the commander or designated representative, an entry/exit inspection will commence with the posting of conspicuously displayed inspection signs (figures H-1 and H-2) at the entry/exit point. Signs will state the purpose and scope of the inspection.

b. Individuals will be asked to open their briefcases, shoulder or handbags, luggage, athletic bags or other packages to check for classified material. A table should be available to expedite the inspection.

c. Inspections should be cursory in nature and should not extend to checking items such as wallets, change purses, clothing, cosmetic cases, or other items of an unusually personal nature.

d. Personnel conducting inspections will work in two-person teams for added security.

e. The duration of an inspection should be limited to a specific period of time such as 1 hour, 2 hours, or 1 day at the discretion of the implementing authority.

f. Inspections may be done on a random basis using any appropriate standard. For example, every third person or every tenth person seeking to pass the inspection point. The standard should remain consistent during the course of a particular inspection.

g. Entrances and exits used as inspection points should be rotated, if possible, to preclude familiarity with inspection sites.

h. All activities will provide employees who have a legitimate need to remove classified material from the facility or installation with written authorization to pass through designated entry/exit points. Requests to hand carry classified material out of SDDC facilities will be submitted with full justification to the security manager/officer for approval. Approved couriers will be designated on DD Form 2501, Courier Authorization.

i. If an individual does not possess appropriate authorization, inspectors will attempt to contact the individual's supervisor in order to verify his/her authority to remove classified material from the facility or installation. If attempts to verify authority are not successful, the security manager/officer or the commander will be notified. In any case, individuals will not be allowed to depart the inspection area with classified material in their possession without proper authorization.

j. All incidents of suspected compromise of classified material will be immediately brought to the attention of the security manager/officer and G-2.

WARNING NOTICE

ALL PERSONS WITHIN THESE PREMISES ARE SUBJECT TO INSPECTION TO PREVENT AND DETECT THE UNAUTHORIZED REMOVAL OF CLASSIFIED MATERIAL

Figure H-1. Classified material entry/exit inspection program warning notice

ATTENTION EMPLOYEES AND VISITORS

1. THE FOLLOWING ITEMS ARE SUBJECT TO INSPECTION:

- **FOLDERS**
- **BRIEFCASES**
- **ATHLETIC BAGS**
- **SHOULDER/HANDBAGS**
- **OTHER PACKAGES**

2. THE FOLLOWING ITEMS ARE NOT SUBJECT TO INSPECTION:

- **WALLETS**
- **CLOTHING**
- **CHANGE PURSES**
- **COSMETIC CASES**
- **OTHER ITEMS OF AN UNUSUALLY PERSONAL NATURE**

Figure H-2. Classified material entry/exit inspection sign

Appendix I
Activity Security Checklist

ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	BLDG/ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO (*If required*)	FROM *(If required)*	THROUGH *(If required)*
SDDC G2		

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Workstations are free of classified material																															
2. Trash receptacles are free of classified material																															
3. Logged off SIPRNET Computer Systems																															
4. Logged off NIPRNET Computer Systems																															
5. ID Card Secured																															
6. KSV-21, Fortezza Card(s) Secured																															
7. Security container locked and SF 702 documented																															
8. Doors and windows locked																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

Form designed using PerForm Pro Software

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Glossary

Section I
Abbreviations

AMC
Army Materiel Command

ATO
Army Technology Objective

CASCOM
Army Combined Arms Support Command

CBA
capabilities-based assessment

CG
commanding general

CJCSI
Chairman of the Joint Chiefs of Staff instruction

COCOM
combatant command

COTS
commercial off-the-shelf

CTIO
Command Transformation and Integration Office

DARPA
Defense Advanced Research Projects Agency

DOD
Department of Defense

DOTMLPF
doctrine, organization, training, materiel, leadership and education, personnel, and facilities

DPO
Distribution Process Owner

DTS
Defense Transportation System

FAST
Field Assistance in Science and Technology Program

GOTS
government off-the-shelf

IPPD
Integrated Product and Process Development

IT
Information Technology

JCIDS
Joint Capabilities Integration and Development System

JCTD
Joint Capability Technology Demonstration

OSD
Office of the Secretary of Defense

RDECOM
U.S. Army Research, Development Engineering Command

RDT&E
research, development, test and evaluation

RFI
request for information

SDDC
Military Surface Deployment and Distribution Command

S&T
science and technology

STC
SDDC Science and Technology Council

STWG
Science and Technology Working Group

TEA
Transportation Engineering Agency

TRADOC
United States Army Training and Doctrine Command

TRL
Technology Readiness Level

USTRANSCOM
United States Transportation Command

Section II
Terms

SDDC Security Manager
An individual designated in writing by the Deputy Chief of Staff for Intelligence and Security (G-2) responsible for management of the information security program. Generally, the SDDC Security Manager will be a commissioned officer (O-3 or above), warrant officer, or civilian in the grade of GS-12 or above.

Subordinate Activity/Unit Security Manager
Member of an organizational element designated in writing to perform information security responsibilities. Subject to higher headquarters approval, subordinate commands may designate a security manager at a lower rank or grade than that which is stipulated for the SDDC Security Manger when the individual selected has been formally schooled trained to effectively discharge assigned responsibilities.

Top Secret Control Officer/Alternate
An individual assigned to maintain accountability and control of Top Secret material and is designated in writing by the staff principal or commander/director.

Top Secret Reproduction Control Officer/Alternate
An individual designated in writing to control reproduction of classified material.

Classified Document Reproduction Control Officer
An individual designated in writing to control reproduction of classified material.

Classified document Custodian
An individual designated by staff principals or subordinate commanders, or who has possession of, or is otherwise charged with the responsibility for, safeguard or accounting for, classified material. The custodian is designated to protect and account for classified material located within a specified safe.

Foreign Disclosure Officer
An individual designated in writing to be responsible for foreign liaison/disclosure matters as stated in AR 380-10.

Classified Document Repository (CDR)
The element under G-6 designated as the SDDC central control point for all classified mail and message traffic.

Derivative Classification
A determination that information is in substance the same as information that is currently classified and a designation of the level of classification.

Sensitive Position
A position so designated with the DOD, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on national security. As used in this regulation, this definition applies to positions so designated because frequent/recurring access to classified information is required by the incumbent to perform duties outlined in the official job description. Sensitive positions are "non-critical sensitive" (Secret or Confidential access) or "critical sensitive" (Top Secret access) as defined in AR 380-67. No person is entitled solely by virtue of grade, position or security clearance to be furnished classified information. Such information will be entrusted only to persons whose official duties require such information (need-to-know) and who have a valid security clearance.

Section III
Special Terms and Abbreviations
This section contains no entries