Department of the Army
Headquarters, U.S. Army Garrison
462 Hamilton Road, Suite 120
Fort Sill, Oklahoma 73503
1 November 2013

***Fort Sill Supplement 1 to AR 380-5**

Security

DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

Summary. This publication prescribes policies, responsibilities, and procedures set forth in Executive Order (E.O.) 13526, "Classified National Security Information", December 29, 2009, with amendments, and DOD 5200.1–R, "Information Security Program" Army Regulation 380-5. It establishes the policy for classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security.

Applicability. This publication applies to all military and civilian members to include contractors employed by, assigned or attached to units and activities on Fort Sill.

Suggested Improvements. The proponent of this publication is the DPTMS, Security and Intelligence Division. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to DPTMS, Security and Intelligence Division.

Distribution. This publication is distributed solely through the DHR, ASD Homepage at http://sill-www.army.mil/usag/publications.html.

---

*This publication supersedes USAFCOEFS Supplement 1 to AR 380-5, 28 October 2009.

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

Paragraph 1-6. The Commander. Add the following after the second sentence in paragraph e:

Each commander or activity head will develop information security policies and procedures consistent with the mission of that activity and the requirements of AR 380-5, as supplemented. This supplement promulgates information security policy for Fort Sill, and constitutes the Information Security Program for this installation. Incorporate these policies and procedures into a written security SOP, and update to reflect current command information security policy. Each USAFCOEFS activity down to battalion, department, and directorate level will appoint in writing a security manager and one alternate. Large directorates and departments may appoint assistant security managers at lower levels (e.g., division or branch). Commanders will provide the name and contact information for their Command Security Manager to the Security and Intelligence Division.

Paragraph 1-7. Command Security Manager. Add the following after the first sentence in the introductory paragraph:

The Chief of Security & Intelligence Division, Directorate of Plans, Training, Mobilization, and Security (DPTMS) is the Command Security Manager for USAFCOEFS. Security managers will attend the Security and Intelligence Division's Security Managers Conference as soon as possible after assuming such duties. Assistant security managers may attend.

Paragraph 1-7. Command Security Manager. Add the following subparagraph after subparagraph q:

r. The Security and Intelligence Division will conduct Staff Assistance Visits (SAV) to all USAFCOEFS special staffs, directorates, and organizations that store or process classified information.

Paragraph 1-10. Applicability. Add the following after the last sentence:

This supplement applies to all military and civilian personnel assigned to Fort Sill, Oklahoma, or units over whom Fort Sill exercises staff cognizance.

Paragraph 1-19. Waivers and Exceptions to Policy. Add the following after the last sentence of subparagraph b:

Forward all requests for exemptions or waivers through Security & Intelligence Division.

Paragraph 1-22. Reporting of Incidents. Add the following after the last sentence:

Report all incidents involving classified information to the Security and Intelligence Division.

Paragraph 1-23. Reporting Requirements. Add the following after the last sentence:

Security Managers will report the number of classified documents created under this section to the Security and Intelligence Division at the end of each fiscal year quarter. This report is exempt from AR 335-15 requirements.

Paragraph 1-24. Command Security Inspections. Add subparagraphs a and b:

a. Commanders will conduct annual security inspections of subordinate units. Retain results of visits IAW AR 25-400-2 The Army Records Information Management System (ARIMS).

b. The Security & Intelligence Division will conduct courtesy Staff Assistance Visits to all USAFCOEFS activities. Upon request, Security & Intelligence Division can schedule this courtesy visit for any classified document custodian or security manager. Security & Intelligence Division will conduct unannounced and follow-up security visits when requested or when required to evaluate the current security posture of a

USAFCOEFS activity. Maintain the results of all staff assistance visits in unit or activity files IAW AR 25-400-2.

Paragraph 2-2. Policy (Original Classification). Add the following after the last sentence:

No one on Fort Sill has the authority to classify information at any level.

Paragraph 2-22. Classification Challenges. Add the following after the first sentence of subparagraph a:

Within USAFCOEFS, the holder of the information will contact the proponent of the information in order to resolve differences. Activities may conduct challenges that involve upgrading a document (e.g., CONFIDENTIAL to SECRET) via secured means. Challenges involving unclassified information considered to be classified will be discussed over secure voice for OPSEC purposes. When activities cannot resolve differences through an informal method, request Security and Intelligence Division to make a formal challenge.

Paragraph 3-2. Special Program Manager. Add subparagraph d. after subparagraph c:

d. USAFCOEFS annual review of all classified material to be downgraded, declassified, or destroyed will be the first working day after Labor Day. Each unit and activity security manager must send an informal memorandum to the Security and Intelligence Division reporting that the review occurred.

Paragraph 3-6. Exemption from Automatic Declassification. Add the following after the last sentence of paragraph a:

Forward requests for continued classification to Security & Intelligence Division to arrive not later than 160 days before the scheduled review date.

Paragraph 3-9. Mandatory Review for Declassification. Add the following after the last sentence of subparagraph a:

Forward proposals for retention of classification to Cdr, USAG, ATTN: IMSI-PLS.

Paragraph 3-18. Clearing, Purging, Declassifying, and Destroying Media: Add the following after last sentence in subparagraph d.

Security and Intelligence Division has a HD-1T Degausser available. Personnel can schedule appointments for degaussing classified media through the Information Security Branch at 442-1816.

Paragraph 3-18. Clearing, Purging, Declassifying, and Destroying Media: Add the following after last sentence in subparagraph e.

Security and Intelligence Division has a CD-101 Datastroyer CD Shredder available. Personnel can schedule appointments for shredding classified media only, through the Information Security Branch at 442-1816.

Paragraph 4-28. Slides and Transparencies. Add after last sentence in subparagraph b:

Keep slides in containers (trays, carousels, envelopes, boxes, etc.) bearing conspicuous classification marking of the highest-level classification contained therein.

Paragraph 5-5. Protection of FOUO information. Add the following after the last sentence of subparagraph a:

Personnel will ensure their electronic media is encrypted in accordance with AR 25-2.

Paragraph 6-1. Responsibilities. Add the following after the last sentence:

Organizations will verify clearances through the Joint Personnel Adjudication System (JPAS) before access is granted to classified material.

Paragraph 6-10. Care During Working Hours. Add subparagraph f after subparagraph e:

f. Locate security containers in areas where personnel can deny inadvertent or easy access to unauthorized personnel. However, do not treat such areas as a restricted area as defined in AR 190-13. Commanders may submit requests for designation of restricted areas, in accordance with AR 190-13.

Paragraph 6-12. Emergency Planning. Add the following after the last sentence of opening paragraph:

Post emergency plans for evacuation and destruction of classified material in a conspicuous location near security containers in all organizations where personnel retain or store classified information.

Paragraph 6-18. Classified Meetings and Conferences. Add the following after the last sentence in the introductory paragraph:

Inform Security & Intelligence Division of conferences or large meetings wherein personnel will discuss classified material. Security & Intelligence Division will provide staff assistance as appropriate. Address questions concerning necessary safeguards for classified discussion areas to Security & Intelligence Division. The use of cellular phones, pagers, and other unauthorized electronic devices is prohibited while attending classified meetings, sessions, and conferences. Personnel will not bring their cellular phones, pagers, and other electronic devices into areas where classified discussions are held. Military clubs or other public facilities are not authorized areas for classified presentations.

Paragraph 6-18. Classified Meetings and Conferences. Add the following after the last sentence of paragraph c:

Send requests through Cdr, USAG ATTN: IMSI-PLS, to arrive not later than 120 days before the meeting date.

Paragraph 6-18. Classified Meetings and Conferences. Add the following subparagraph (8) after subparagraph d(7):

(8) Security & Intelligence Division is the main point of contact for all foreign nationals visiting Fort Sill. Prior to inviting a foreign national to attend a meeting or conference, the sponsoring activity will coordinate with Security and Intelligence Division Foreign Disclosure Officer. Commanders and heads of USAFCOEFS activities will ensure compliance with all applicable provisions of subparagraphs f and g of this paragraph, and of the National Disclosure Policy AR 380-10 and TRADOC Regulation 380-1.

Paragraph 6-20. Receipt of Classified Material. Add the following subparagraphs after the first paragraph:

a. Protect incoming official First Class and accountable mail as classified until a determination is made whether classified information is contained therein. Personnel who work in mail rooms, or other screening points, where incoming official First Class mail, accountable mail, bulk shipments or other potentially classified items are processed, will possess a SECRET security clearance. It would be possible; however, to have some uncleared support personnel assigned to these areas provided--

(1) They are under constant control and supervision of appropriately cleared personnel.

(2) They do not open mail or have visual access to classified information.

(3) Written standard operating instructions are in place to protect classified information from unauthorized disclosure or physical removal from the areas.

(4) These areas are inspected during command security inspections.

b. Protect all incoming official First Class and accountable mail as classified from the time it leaves U.S. Postal Office control and comes under the control of U.S. Army civilian or military personnel. This protection continues until it is opened and the contents are verified as being unclassified.

c. Secure a SECRET security clearance and access for all U.S. Army military or civilian personnel who have unescorted access to unopened official First Class mail, accountable mail, bulk shipments or other potentially classified shipments. This requirement includes all personnel who have access to these items from the time they are received from the U.S. Postal Service until they are opened, regardless of how many distribution points these items pass through.

Paragraph 6-22. SECRET and CONFIDENTIAL Information. Add the following after the last sentence:

All organizations will maintain a log of all SECRET and CONFIDENTIAL material. This log must reflect the date and disposition.

Paragraph 6-25. Policy. Add the following after the last sentence of subparagraph a:

Use administrative procedures as outlined in appendix A to this supplement for handling TOP SECRET information. Date marking will be permanent.

Paragraph 6-25. Policy. Add subparagraphs (1), (2), and (3) after the last sentence of subparagraph c:

(1) Submit requests for designation of reproduction machines authorized to reproduce SECRET or CONFIDENTIAL information to Security & Intelligence Division. Written justification will address the extent of classified information and frequency reproduction is required. Identify the machine to be authorized by manufacturer, model number, and serial number. Cite procedures to be implemented for the safeguarding of classified information during reproduction. Post letter authority to reproduce classified information in the immediate vicinity of the approved reproduction machine. Do not use replacement or additional machines for classified reproduction without prior approval for such use.

(2) Machines used to produce classified training aids, to print classified material, or to process classified material in any way will similarly be approved for such use by this headquarters. Inform Security & Intelligence Division when personnel procure new or replacement machines.

(3) Do not use Automated Information Systems (AIS) or Word Processing Equipment (WPE) for the processing of classified military information without accreditation from appropriate headquarters, in accordance with AR 25-2.

Paragraph 6-25. Policy. Add the following subparagraphs d and e after subparagraph c:

d. This headquarters will issue the following Fort Sill poster indicating level of authorized reproduction with the letter of approval. Activities/units will need to display it on or in the immediate vicinity of the authorized copier or reproduction machine: (These posters are located on the following website:)

http://sill-ww.army.mil/usag/forms_rev.html.

WARNING: This machine is authorized to reproduce TOP SECRET material or below (Fort Sill Suppl 1 to AR 380-5, paragraph 6-25) FS Poster 380-5d (TS) (DPTMS) 12 Mar 08.

WARNING: This machine is authorized to reproduce SECRET material or below (Fort Sill Suppl 1 to AR 380-5, paragraph 6-25) FS Poster 380-5c (S) (DPTMS) 12 Mar 08.

WARNING: This machine is authorized to reproduce CONFIDENTIAL material or below. (Fort Sill Suppl 1 to AR 380-5, paragraph 6-25) FS Poster 380-5b (C) (DPTMS) 12 Mar 08.

e. Post Fort Sill Poster 380-5a on or near all machines which are **not authorized** for the reproduction of classified material.

WARNING: THIS MACHINE IS NOT AUTHORZIZED TO REPRODUCE CLASSIFIED MATERIAL (Fort Sill Suppl 1 to AR 380-5, Para 6-25) FS Poster 380-5a (UNCLAS) (DPTMS) 12 Mar 08

Paragraph 6-26. Approval for Reproduction. Add the following after the first sentence of subparagraph a:

All USAFCOEFS reproduction authorities will honor production of dissemination restrictions stated by classified document originators.

Paragraph 6-26. Approval for Reproduction. Add subparagraphs (1) through (5) after subparagraph b:

(1) Reproduction of TOP SECRET Information. Commander, USAFCOEFS, retains the authority for the reproduction of TOP SECRET information. Forward requests for the reproduction of TOP SECRET documents or other material to ATTN: Cdr, USAG, IMSI-PLS, with written justification.

(2) Reproduction of SECRET Material. The Assistant Commandant, USAFAS, may delegate approval authority, in writing, to his/her deputies, department directors, principal staff, and deputy department directors.

(3) Reproduction of CONFIDENTIAL Information. Commanders and heads of activities will establish written procedures to maintain reproduction at a level consistent with substantiated need.

(4) Reproduction Request. Use one of the following forms to request reproduction or fabrication of SECRET classified material. Authorized signatures of officials designated in (1) and (2) above will appear in the appropriate section of each form. Heads of activities, with authorized reproduction and fabrication capability, will implement procedures to verify that only authorized reproduction authorities approve these requests.

(a) DD Form 843 (Requisition for Printing and Binding Service).

(b) DD Form 844 (Requisition for Local Duplicating Service).

(c) DA Form 3964 (Classified Document Accountability Record), section D.

(d) DA Form 3903 (Training-Audiovisual Work Order).

(e) Training Aids and Printing Facilities. Heads of these activities will establish written security procedures consistent with AR 380-5 and this supplement to preclude inadvertent disclosure of classified material that has been improperly marked, handled, or safeguarded. Report compromise or possible compromise in accordance with AR 380-5, paragraph 10-3, as supplemented.

Paragraph 6-27. Policy. Add the following after the last sentence in paragraph a:

Continuous destruction of unneeded classified material is encouraged, however, the first working day after Labor Day each year is designated as Fort Sill's Annual Clean-out Day.

Paragraph 6-28. Methods and Standards for Destruction. Add the following as the last sentence in subparagraph c:

Personnel may temporarily store classified waste in the same container as other classified material, but keep it in a separate drawer.

Paragraph 7-5. Procurement of New Storage Equipment. Add the following after the last sentence of subparagraph b:

Forward requests for exception to Cdr, USAG ATTN: IMSI-PLS.

Paragraph 7-8. Equipment Designations and Combinations. Add the following after the first sentence of subparagraph b:

Change combinations with the container drawer open. Security Managers are authorized to change combinations as needed. GSA certified safe and vault technicians will change vault door combinations equipped with non-electro-mechanical locks, however, security managers are authorized to change vault door combinations if the door is equipped with an X-07, X-08 or X-09 electro-mechanical lock.

Paragraph 7-8. Equipment Designations and Combinations. Add the following after the last sentence of subparagraph d:

Designate one container as the master container. Use it to store part 2 SF 700 to the remaining containers. Use paper tape to seal part 2. Store the master container combination at the next higher command or directorate. If next higher command or directorate is located off of Fort Sill, then store the combination for the master container at the Security and Intelligence Divisions Information Security Office’s master container.

Paragraph 7-9. Repair of Damaged Security Containers. Add the following after the last sentence of the introductory paragraph:

Process requests for service on security containers that personnel cannot open for whatever reason through the organization's security manager, through normal supply channels, to DOL Maintenance Division. Only authorized civilian contractor personnel will drill or repair security containers. The unit will ensure that a properly cleared individual is present when the container is opened. This requirement applies even if the container is believed not to contain classified information. Notify Security & Intelligence Division (442-1816) when a lockout has occurred and repair or drilling is required. Before the container can be utilized for classified material, a representative from Security & Intelligence Division will physically verify that the security container has been restored to its original state of security integrity. It is not required to notify Security & Intelligence Division when the lockout involves non-GSA approved safes used in orderly rooms for unclassified storage. When the lockout involves a security container used for storage of classified material, conduct an informal inquiry to determine the cause of the lockout and make a determination if there was unauthorized tampering.

Paragraph 7-13. Vault and Secure Room (Open Storage Area) Construction Standards. Add the following subparagraphs c and d after subparagraph b:

c. Refer plans for the construction or modification of vaults or secure rooms for the purpose of open storage of classified material to Security & Intelligence Division for coordination. Commanders or activity heads will request, in writing, necessary inspection and approval of the facility prior to use. Technical specifications for vaults are contained in AR 380-5. Commander, USAFCOEFS, retains the authority for open storage approval. Forward requests for same to Cdr, USAG, ATTN: IMSI-PLS.

d. Requests for open storage will be in writing, and will be submitted with appendix A (Open Storage Checklist). The checklist is designed to assist Security Managers on Fort Sill to identify and assess security requirements for areas within their organization which are being considered for use as Open Storage Area. The completed checklist is a required attachment to any request for open storage authorization. This checklist is applicable to all activities physically located or assigned to Fort Sill.

Paragraph 8-2. TOP SECRET Information. Add the following after the last sentence of subparagraph a:

Material containing collateral TOP SECRET information will be accounted for in a manner greater then that for SECRET information. Continue to control and account for collateral TOP SECRET information based on current standards as prescribed in AR 380-5

Paragraph 8-3. SECRET Information. Add subparagraphs (1) and (2) after subparagraph a:

(1) Fort Sill, including USAFCOEFS activities and tenants, is considered a single activity for SECRET information receipting purposes. Do not transmit SECRET information between Fort Sill activities through DHR, Administrative Services Division, Official Mail and Distribution Center. Use of DA Form 3964 is required for transmittal of CLASSIFIED material between contractor activities and government personnel. File and retain DA Form 3964, used as a receipt, IAW AR 25-400-2.

(2) When SECRET information is transmitted outside USAFCOEFS, the sending activity will prepare DA Form 3964 in triplicate. Send a receipt copy (copy 1) and a courtesy copy (copy 2) with the SECRET information. Retain the third copy as a suspense copy until copy 1 is returned. DHR, Administrative Services Division, Official Mail and Distribution Center personnel will annotate United States Post Office registered mail stamp and number on the suspense copy at the time of mailing.

Paragraph 8-9. Envelope or Containers. Add the following after the first sentence in paragraph a:

Seal all seams using paper tape to detect tampering.

Paragraph 8-9. Envelopes or Containers. Add the following subparagraphs (1) and (2) after subparagraph b:

(1) When personnel hand carry classified information from one installation to another installation, double wrap, mark, and address as required by AR 380-5, paragraphs 8-9 and 8-10.

(2) When personnel hand carry classified information between buildings or units located on Fort Sill, double wrap; or single wrap it, with the envelope marked as required in AR 380-5, paragraphs 8-9 & 8-10, and carry it in a briefcase or similar container.

Paragraph 8-13. Documentation. Add subparagraphs (6), (7) and (8) after subparagraph b(5):

(6) Brief personnel issued DD Form 2501 (Courier Authorization Card) on the responsibilities as a courier. See figure 8-1 of this supplement for a sample briefing certification.

(7) DD Form 2501 is required for all personnel who on a daily basis hand carry classified information from any place on Fort Sill.

(8) Hand carrying classified information while in possession of DD Form 2501 only, is restricted to Fort Sill and a 25 mile radius within the local area. Travel beyond those boundaries requires courier orders and the DD Form 2501.

Paragraph 8-15. Hand carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. Add the following after the last sentence of subparagraph b:

Seal the envelopes in accordance with AR 380-5, paragraphs 8-9 and 8-10.

Paragraph 8-15. Hand carrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. Add the following after the last sentence of subparagraph a(1):

See figure 8-2 and figure 8-3 of this supplement for a sample of the memorandum for hand carrying classified documents aboard commercial aircraft. Chief, Security & Intelligence Division is the approving authority for outside continental United States (OCONUS) courier orders. Lieutenant Colonel or higher may approve continental United States (CONUS) courier orders.

Paragraph 9-2. Methodology. Add the following after the last sentence of introductory subparagraph:

All Fort Sill units and activities will maintain records of attendance at training and security education briefings IAW AR 25-400-2.

Paragraph 9-3. Initial Orientation. Add the following after the last sentence of subparagraph a:

All personnel who are granted access to classified military information while assigned to this command will receive initial indoctrination emphasizing the provisions of this paragraph.

Paragraph 9-8. Foreign Travel Briefing. Add as an introductory paragraph before subparagraph a:

All foreign travel briefings are scheduled through the AT/FP office (442-5973 or 442-2537) for the last Tuesday of each month.

Paragraph 9-8. Foreign Travel Briefing. Add subparagraph e after subparagraph d:

e. Unit or activity security managers must ensure that all personnel who have Special Compartmented Information (SCI) access are debriefed and receive a travel brief by the Fort Sill Special Security Office prior to overseas travel either in TDY or leave status.

Paragraph 10-2. Reaction to Discovery of Incident. Add the following after the last sentence in subparagraph a:

Security containers found unsecured are to be secured prior to notifying individuals listed on SF Form 700. Security Manager will do a 100% inventory upon arrival of all material with in the security container.

Paragraph 10-2. Reaction to Discovery of Incident. Add the following after the last sentence in subparagraph b:

The security manager will telephonically notify Security & Intelligence Division as soon as possible in the event of a possible or actual compromise of classified information (442-1816).

Paragraph 10-3. The Preliminary Inquiry. Add the following after the last sentence of the introductory paragraph:

(See paragraph 10-3g for Fort Sill guidance.)

Paragraph 10-3. The Preliminary Inquiry. Add the following subparagraph g after subparagraph f:

g. Upon notification of an actual or possible compromise of classified material,--

(1) The concerned agency or unit will notify the next higher headquarters of the circumstances surrounding the incident.

(2) The security manager will advise the commander of the appropriate actions to be taken, and will notify Security & Intelligence Division by the fastest means available (442-1816) consistent with sound security and report the circumstances surrounding the incident. At this time Security & Intelligence Division will issue the Preliminary Inquiry (PI) Number.

(3) Security and Intelligence Division will have a tasking request submitted through G3 Taskings for a disinterested commissioned officer, warrant officer, noncommissioned officer (SFC or above) or a DA Civilian (GS7 or above) outside the concerned agency or units chain of command to conduct a preliminary inquiry (PI) in accordance with the guidance in this supplement (see figure 6-1, this supplement, for appointment order format). The individual appointed to conduct the PI (i.e., "Inquiry Officer") will report to Security & Intelligence Division with a copy of his or her appointment orders for instructions prior to starting inquiry action. The PIO (Preliminary Inquiry Officer) will have no other duties assigned during the time of appointment as the PIO.

(4) The PIO will prepare a Report of Preliminary Inquiry and forward it to the appointing authority and Chief, Security & Intelligence Division, DPTMS within 10 working days. An extension may be granted if factors within the inquiry require to extend past the 10 days through Security and Intelligence Division from the date of appointment (see figure 6-2, this supplement, for sample report of preliminary inquiry).

(5) The Appointing Authority will review then endorse the preliminary inquiry to Security & Intelligence Division within 3 working days of receipt. The endorsement will indicate whether a compromise or an administrative security violation has occurred. If an administrative security violation is determined to have occurred involving information

classified CONFIDENTIAL, final action taken should be indicated. If an administrative security violation is determined to have occurred involving information classified SECRET or higher, recommended action should be indicated. Commander, USAFCOEFS, retains authority to impose administrative or nonjudicial punishment in those instances involving the compromise or possible compromise of SECRET information.

(6) The Director and the Chief of Security & Intelligence Division, will review the preliminary inquiry and will recommend final disposition or further investigation to the Commander, USAFCOEFS.

Paragraph 10-9. Unauthorized Absences, Suicides, or Incapacitation. Add the following after the last sentence:

Commanders or activity heads, G2s, S2s and security managers are responsible for monitoring military members declared AWOL or unexplained failure to report for work by DA civilians, who have had access to national defense information classified SECRET and higher or communications security (COMSEC) information. Commanders or activity heads must make a determination as to the degree of sensitivity of the classified information involved and must report the absence immediately through S2s or security manager channels to Security & Intelligence Division (442-1816) in the following format:

(1) Name, rank, SSN.

(2) Date and place of birth.

(3) Organization and station.

(4) Date of absence.

(5) Last known location.

(6) Home of record.

(7) Next of kin with address.

(8) Level of clearance.

(9) Type of access (current and past).

(10) Reason for, circumstances of AWOL, and indications of defection or intent to defect.

(11) Other pertinent information.

Paragraph 10-9. Unauthorized Absences, Suicides, or Incapacitation. Add the following after the last sentence:

Commanders and activity heads will ensure individual personnel records are immediately screened to determine if the individual committing or attempting suicide has been granted a clearance and authorized access to classified military information. Telephonically report the results of this check and known reasons for suicide or attempted suicide to Security & Intelligence Division (442-1816) as soon as possible.

(Appropriate Letterhead of Issuing Agency)

S: (10 Working Days)

(Office Symbol) Date

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Duty Appointment or Assignment

1. Effective 25 Dec 89, CPT Security, Violate C., USAFCOEFS, 442-XXXX is appointed the following duty:

Preliminary Inquiry Officer

2. Authority.

a. AR 380-5, paragraph 10-3.

b. Fort Sill Supplement 1 to AR 380-5.

3. Purpose. To conduct a Preliminary Inquiry on the possible compromise of classified information.

4. Period. From DD MMM YY until officially released.

5. Special Instructions.

a. Report to Security & Intelligence Division with appointment order (Information Security Program Manager), Bldg 1651, NLT (*The following day after appointment has been made).*

b. This investigation is your primary duty until released by Security and Intelligence Division.

FOR THE COMMANDER:

Signature Block

DISTRIBUTION:
1-Individual
1-IMSI-PLS
1-Unit S2

Figure 6-1. Sample Letter Appointing Preliminary Inquiry Officer

(Appropriate Letterhead of Report Agency)

OFFICE SYMBOL Date

MEMORANDUM FOR Appointing Authority

SUBJECT: Report of Preliminary Inquiry Officer

1. In compliance with the appointing letter, the following is my report of preliminary inquiry (*PI Issued Number*).

2. Facts and Circumstances. The investigating officer must be completely objective and consider all facts and circumstances to answer the following questions. When the facts are lengthy or complicated, separate the paragraph containing the narrative of the summary of events in chronological order.

a. WHEN? Date and time the incident occurred, date and time the situation was discovered and reported.

b. WHERE? Complete identification of unit, section, activity, office, building and room number or geographic location.

c. WHO? Complete identity of everyone involved, including responsible officials, and how they are involved.

d. WHAT? Exact description of the information or material involved and what happened to it.

e. HOW? Circumstances of the incident related to how the information or material was lost or compromised. Summarize the evidence supporting your conclusion, and attach supporting enclosures when appropriate.

f. WHY? What are applicable policies, regulations, etc., for controlling the material or information involved? Were they complied with? Was anyone negligent or derelict in his duties? Was unit SOP adequate to ensure compliance with applicable directives of higher headquarters and for ensuring the proper protection of the information or material?

Figure 6-2. Sample of Investigating Officers Memorandum

(Office Symbol)
SUBJECT: Report of Preliminary Inquiry Officer

3. Findings. When you have answered all of the above questions, you should review the facts to reach findings on the following matters.

a. Did a loss of classified information or material occur? (AR 380-5, para 10-3.)

b. Did a compromise occur? Or, under the circumstances, what is the probability of compromise? Or, state that a compromise did not occur, or that there is a minimal risk of damage to the national security (AR 380-5, para 10-3).

c. Is there any indication of significant security weaknesses in the activity or unit (i.e., were there any deficiencies in procedures for safeguarding classified information or material, or were there any violations of established procedures)? If so, were they significant or contributory to the loss or compromise?

d. Is disciplinary action appropriate? If so, against whom? (Administrative sanctions are outlined in AR 380-5, paragraph 10-10).

4. Recommendations. Based on the findings, the investigating officer must make specific recommendations. The recommendations may include any relevant corrective or disciplinary action consistent with the findings, but, as a minimum, must address the following:

a. If the findings are that a loss occurred, what actions should be taken to prevent recurrence?

b. If a compromise occurred and the probability of identifiable damage to the national security cannot be discounted, or it is determined that further investigation is likely to be productive, a recommendation that an investigation under AR 15-6 be conducted may be included.

c. If there were significant security weaknesses, the recommendation must include specific changes that should be made to correct the deficiency. In addition, further investigation under AR 15-6 may be appropriate if the weaknesses resulted from conscience noncompliance with applicable directives.

d. If disciplinary action is considered appropriate, the recommendation should include the specific action recommended, against whom and for what specific conduct, and who should take the action.

Figure 6-2. Sample of Investigating Officers Memorandum (cont)

(Office Symbol)
SUBJECT: Report of Preliminary Inquiry Officer

e. If further investigation under AR 15-6 is recommended, the recommendation should identify any person who should be designated as a respondent (see AR 15-6, paragraph 5-4) and make a recommendation as to whether formal or informal investigation should be conducted (see AR 15-6, paragraph 1-2b).

5. Point of contact is …

(Signature block of inquiry officer)

Figure 6-2. Sample of Investigating Officers Memorandum (cont)

COURIER CERTIFICATION OF BRIEFING

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

(Designated Courier)
(Date)
(Security Manager)

Figure 8-1. Courier Certification of Briefing

(Appropriate Letterhead of Report Agency)

Office Symbol Date

MEMORANDUM FOR Addressee (Name of Airline(s))

SUBJECT: Authority to Hand-carry United States Military Classified Information

Designated Courier:

Name: Doe, John Joseph, Major, (*UNIT*) United States Army

SSN: **DOB:** **POB:**
Sex: **Height:** **Weight:** **Hair Color:** **Eye Color:**

HQ or Agency: Headquarters, United States Army Field Artillery Center, Fort Sill, Directorate of Plans, Training, Mobilization, and , Security & Intelligence Division, Fort Sill, OK 73503-5100

Type of Identification: DD Form 2A (Armed Forces Identification Card) and DD Form 2501 Courier Authorization Card.

Material Carried: 1 sealed envelope, 8'x 10'x 1' or 3 sealed packages, 9'x 8'x 24' overall

Addressee and Addresser: Commander, Cambrai Frisch Kaserne, Darmstadt, Germany
APO AE 09175

Departure Point: Lawton Municipal Airport, Lawton, OK

Departure Date: DDMMYY

Destination: Frankfurt International Airport, Frankfurt, Germany

Transfer Point: Dallas-Fort Worth International Airport, Dallas, TX

Issue Date: DDMMYY

Expiration Date: DDMMYY (not to exceed 7 days from date of issue)

Figure 8-2. Sample memorandum for hand-carrying classified documents aboard commercial aircraft

(Office Symbol)
SUBJECT: Authority to Hand-Carry United States Military Classified Information

Authority: Headquarters, United States Field Artillery Center and Fort Sill, OK 73503-5100. Phone: (580) 442-1816.

Typed Name
Chief, Security and Intelligence Division

NOTE: Approving authority for OCONUS is Security & Intelligence Division

Figure 8-2. Sample memorandum for hand-carrying classified documents aboard commercial aircraft (cont)
(Appropriate Agency Letterhead)

Date

(Agency/Unit Identification)
Directorate of Plans, Training, and
Mobilization, Security Division

Addressee (Name of Airline(s))

Dear Sir:

Authority to Hand-Carry United States Military Classified Information

Designated Courier:

Name: Doe, John Joseph, Major (*Unit*) United States Army

SSN: **DOB:** **POB:**
Sex: **Height:** **Weight:** **Hair Color:** **Eye Color:**

HQ or Agency: Headquarters, United States Army Field Artillery Center, Fort Sill, Directorate of Plans, Training, Mobilization, and , Security & Intelligence Division, Fort Sill, OK 73503-5100

Type of Identification: DD Form 2A (Armed Forces Identification Card) and DD Form 2501 Courier Authorization Card.

Material Carried: 1 sealed envelope, 8'x 10'x 1' or 3 sealed packages, 9'x 8'x 24' overall

Addressee and Addresser: Commander, Fort Bragg - Headquarters, 18th Airborne Corp Artillery, Fort Bragg, North Carolina 28307

Departure Point: Lawton Municipal Airport, Lawton, OK

Departure Date: DDMMYY

Destination: Fayetteville Regional Airport, Fayetteville, NC

Figure 8-3. Sample letter for hand-carrying classified documents aboard commercial aircraft

Transfer Point: Dallas-Fort Worth International Airport, Dallas, TX

Issue Date: DDMMYY

Expiration Date: DDMMYY (not to exceed 7 days from date of issue)

Authority: Complete Unit Address, POC, and Telephone.

Letter Style Signature Block

NOTE: Commander (05 and above) and directors or heads of departments can sign authorization letters for CONUS.

Figure 8-3. Sample letter for hand-carrying classified documents aboard commercial aircraft (cont)

Appendix A to USAFCOEFS Supplement 1 to AR 380-5 Open Storage Area Checklist	Classification UNCLASSIFIED FOR OFFICIAL USE ONLY	Date OCT 13
		Page 24 of 31

1. Purpose. The following checklist is designed to assist Security Managers on Fort Sill to identify and assess security requirements for areas within their organization which are being considered for use as an Open Storage Area. The completed checklist is a required attachment to any request for open storage authorization.

2. Applicability. This checklist is applicable to all activities physically located or assigned to Fort Sill.

3. References.

a. AR 380-5, Information Security Program, 29 September 2000.

b. Fort Sill Supplement 1 to AR 380-5.

4. Section A – General Information.

a. Organization Name:

b. Location: Building #: Floor(s): Room(s) #:

c. Security Representative(s):

(1) Primary Security Manager:

Name: Rank/Grade: Date Appointed: (dd mmm yy)

Office Telephone (Comm): Office Email:

(2) Assistant Security Manager:

Name: Rank/Grade: Date Appointed: (dd mmm yy)

Office Telephone (Comm): Office Email:

d. Requested Authorization Data:

(1) Classification Level Requested: (check one)

☐ SECRET ☐ CONFIDENTIAL

e. Indicate type storage requirement: (check all that apply)

☐ Large volumes exceeding GSA approved security container capabilities.

☐ Large and/or bulky items unable to fit into GSA approved security container.

☐ SIPRnet terminals and associated network equipment.

☐ Other (Describe):

_____

f. Indicate regularity of storage requirement:

☐ Continuous (24/7)

☐ During duty hours only: _____ - _____ (hours), _____ - _____ (days).

☐ During exercise periods only

☐ Other (Describe):

_____

g. Is a graphic floor plan of the Open Storage Area attached, showing all walls, doors, windows, vents, other openings, and indicating adjacent areas and their functions?

☐ YES ☐ NO.

If No, explain;

5. Section B – Justification for Open Storage Requirement.

a. Purpose:

b. Positive impact on operations if request is approved:

c. Negative impact on operations if request is denied:

6. Section C – Open Storage Area Security.

a. Floor, Walls, and Roof. The walls, floor, and roof construction of secure rooms must be of permanent construction materials (i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials) offering resistance to, and evidence of, unauthorized entry into the area. Walls will be extended to the true ceiling and attached with permanent construction materials, with mesh or 18 gauge expanded steel screen. The ceiling will be constructed of plaster, gypsum, wallboard material, hardware, or other similar material that the command security manager judges to be of equivalent strength.

(1) Do the floors meet the standards in paragraph C-1?

☐ YES ☐ NO.

If No, explain;

(2) Do the walls meet the standards in paragraph C-1?

☐ YES ☐ NO.

If No, explain;

(3) Do the roof/ceiling meet the standards in paragraph C-1?

☐ YES ☐ NO.

If No, explain;

b. Doors. The access door to the secure room will be substantially constructed of wood or metal. The hinge pins of out–swing doors will be pinned, brazed, or spot–welded to prevent removal. The access door will be equipped with a built–in GSA–approved combination lock meeting Federal Specification FF–L–2740A. Doors, other than the access door, will be secured from the inside. For example, by using a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door, or by any other means that will prevent entry from the outside. Key operated or cipher locks are not permitted on any door that provides access from the exterior of the open storage area.

(1) Entry Door Type:

☐ Vault, ☐ Solid Metal, ☐ Solid Wood, ☐ Metal Clad Wood.

(2) Entry Door Hinges: Are hinge pins secured to prevent removal.

☐ YES, ☐ N/A, hinges are inside Open Storage Area

(3) Entry Door Lock: Is a built in combination lock meeting federal specification FF-L-2470A (commonly referred to as X07, X08, or X09) installed on door?

☐ YES, ☐ NO

If No, explain

(4) Emergency Exits and Secondary Doors (if applicable). Do all non-entry doors meet the construction standards identified in paragraph C-2 above?

☐ YES, ☐ NO, ☐ N/A

If No, explain;

(5) Emergency Exits and Secondary Doors (if applicable). Are all non-entry doors secured from the inside as described in paragraph C-2 above?

☐ YES, ☐ NO, ☐ N/A

If No, explain;

(6) Emergency Exits and Secondary Doors (if applicable). Has exterior hardware been removed from the non-entry door(s)?

☐ YES, ☐ NO, ☐ N/A

If No, explain;

c. Windows. Windows which are less than 18 feet above the ground when measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, will be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

(1) Does the Open Storage Area have windows? ☐ YES ☐ NO

(2) Are the windows greater than 18 feet from the ground or any platform that could be used to gain access?

☐ YES ☐ NO ☐ N/A.

If No, are they secured against forced opening? ☐ YES ☐ NO ☐ N/A

Explain.

(3) Are the windows protected against visual surveillance?

☐ YES ☐ NO ☐ N/A

If yes, explain.

d. Openings. Utility openings, such as ducts and vents, will be kept at less than a person–passable, 96 square inches, opening. Openings larger than 96 square inches will be hardened to ensure appropriate physical security.

(1) Are ventilation ducts or similar openings located within the Open Storage Area?

☐ YES ☐ NO

(2) If Yes, are there any of the ducts, vents or openings over 96 square inches?

☐ YES ☐ NO ☐ N/A

(3) If Yes, how are they hardened:

☐ IDS ☐ Bars/Grills/Metal Baffles, ☐ OTHER, please explain:

e. Intrusion Detection Systems (IDS). When deviations to the general open storage area construction standards are approved, IDS must be used to provide complete coverage of the entire open storage area, with a minimum response time of 30 minutes.

(1) Are deviations to the construction standards cited in AR 380-5, Paragraph 7-13 required? ☐ YES ☐ NO

If Yes, explain.

(2) Is the entire Open Storage Area covered by IDS?

☐ YES ☐ NO ☐ N/A

If No, explain.

(3) Where is the IDS monitored?

(4) Does the IDS transmission line between the alarm and monitoring site have 128 bit encryption? ☐ YES ☐ NO

If No, explain.

(5) What is the response time to IDS alarms?

(6) Who is the response force?

7. Section D – Procedural and Peripheral Security Measures.

a. Access Control Procedures.

(1) Access to the Open Storage Area is monitored by:

☐ Properly cleared guard Force personnel.

☐ Properly cleared personnel working within the Open Storage Area.

☐ Properly cleared personnel working outside the Open Storage Area.

☐ Automated access control system (proximity card/cipher locks).

(2) Do access control personnel have visual control of the entrance door?

☐ YES ☐ NO ☐ N/A

If No, explain.

(3) If automated access controls are employed.

(a) Who issues the access card or pin number

(b) Is the individual who issues the access card or pin number cleared and authorized access to Open Storage Area? ☐ YES ☐ NO

If No, explain.

(c) What is the prerequisite for issuance?

(d) How often are the codes changed?

(e) What procedures are in place to prohibit “piggy-backing”?

b. Building Access Controls.

(1) Is your organization the sole occupant of the building in which the Open Storage Area is located? ☐ YES ☐ NO ☐ N/A

If No, explain.

(2) What access controls are applied to visitors during duty-hours?

(3) What access controls are applied after duty-hours?

(4) Is there a presence (guard/Staff Duty) within the building after duty-hours?

☐ YES ☐ NO

If Yes, what is the frequency in which they inspect the Open Storage Area perimeter?

If No, is there any after duty-hours inspections of the Open Storage Area perimeter and/or the building? ☐ YES ☐ NO

Explain.

c. Perimeter Security Controls.

(1) Is the building located on a controlled compound? ☐ YES ☐ NO.

If Yes, describe the perimeter fence (type, height, personnel and vehicle gates).

(2) Is the building exterior and perimeter fence illuminated in hours of darkness?

☐ YES ☐ NO

Explain.

(3) Is the compound/building exterior monitored by closed circuit television (CCTV?) ☐ YES ☐ NO.

If Yes, describe the coverage, monitoring, and the response plan.

8. Section E – Security Inspection

a. An inspection of the Open Storage Area was conducted as indicated below.

(1) Date: (dd/mm/yy)

(2) Inspector's Name:

(3) Inspector's Organization:

(4) Inspector's Phone Number:

(5) Inspector's Email Address.:

b. During the inspection the following deficiencies were noted and corrected.

c. Based upon the review of this checklist and inspection, waivers of security requirements are requested? ☐ YES ☐ NO

If Yes, explain:

d. Additional Remarks:

IMSI-PLS

GLENN A. WATERS
COL, FA
Garrison Commander

JAMES A. MILLER
Director of Human
Resources