DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
1401 DESHLER STREET SW
FORT MCPHERSON, GEORGIA 30330-2000
1 January 1999

*** USARC Regulation 380-5**

Security

INFORMATION SECURITY

History. This is the second printing of USARC Regulation 380-5. It was originally published 1 Apr 97.

Summary. This regulation provides information security procedures and policies as set forth in Executive Order 12958, Classified National Security Information, 17 April 1995, and AR 380-5, Department of the Army Information Security Program.

Applicability. This regulation applies to the Headquarters, U.S. Army Reserve Command (USARC), all units, organizations, and installations assigned to the USARC and USARC security teams. Provisions of this regulation have a direct impact on unit readiness and mobilization. Local reproduction is authorized.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, Intelligence (DCSINT). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the Commander, USARC, ATTN: AFRC-INS, 1401 Deshler Street SW, Fort McPherson, GA 30330-2000.

Interim changes. Interim changes to this regulation are not official unless authenticated by the Director, Army Reserve Information Systems Services. Users will destroy interim changes on their expiration date unless superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvement on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Commander, USARC, ATTN: AFRC-INS, 1401 Deshler Street SW, Fort McPherson, GA 30330-2000.

FOR THE COMMANDER:

MITCHELL M. ZAIS
Brigadier General, U.S. Army
Chief of Staff

OFFICIAL:

SIGNED
MELVIN T. LEONARD, JR.
Director, Army Reserve
Information Systems Services

DISTRIBUTION: A

CONTENTS *(Listed by paragraph number)*

*** This regulation supersedes USARC Regulation 380-5, 1 April 1997**

Chapter 1
General

1-1. Purpose
This regulation prescribes USAR policy, assigns responsibility and establishes procedures for all USAR personnel to safeguard Department of Defense (DOD) information relating to national security. Use this regulation in conjunction with AR 380-5, Information Security, and all other required references listed in appendix A.

1-2. References
a. Required and related publications and forms are listed in appendix A.

b. Recordkeeping requirements. This regulation requires the creation, maintenance, and use of File Number 380.

1-3. Explanation of abbreviations and terms
Abbreviations and terms used in this regulation are explained in the glossary.

1-4. Responsibilities
a. **Commander, USARC** will--

(1) Implement and ensure USAR compliance with the Army information security program and requirements of AR 380-5 with its U.S. Army Forces Command (FORSCOM) Supplement.

(2) Commit necessary resources to implementing an effective Information Security Program.

b. **Deputy Chief of Staff for Intelligence (DCSINT)** will--

(1) Develop, assist, and provide guidance with implementing an information security policy.

(2) Designate a USARC Command Security Manager in writing.

(3) Ensure the Command Security Manager receives appropriate training.

(4) Issue written command security procedures.

(5) Establish and maintain a security education program.

(6) Establish and maintain a command security inspection program.

(7) Review and inspect the effectiveness of USAR security programs.

c. **The USARC Command Security Manager** will--

(1) Serve as the Command's adviser and direct representative for classified information matters.

(2) Issue written information security policy and procedures are issued.

(3) Establish and maintain a command security education program.

(4) Establish procedures to limit access of classified information to appropriately cleared personnel with a demonstrated need-to-know.

(5) Establish command procedures to safeguard, control, and destroy classified information.

(6) Advise derivative classifiers of classification, declassification, and marking requirements.

(7) Ensure investigation and reporting of security violations.

(8) Recommend appropriate administrative sanction or corrective action for security violations.

(9) Ensure proposed public releases do not contain classified information.

(10) Establish and maintain visit control procedures.

(11) Implement information security policy to USAR unit level.

(12) Ensure USAR unit security managers receive information security policy training.

(13) Continuously evaluate subordinate units with announced, unannounced, and after-hour security inspection and assistance visit programs.

d**. Commanders, USARC Major Subordinate Command (MSCs)** will--

(1) Appoint, in writing, a full-time employee, civilian or AGR, to serve as Command Security Manager. Appoint, in writing, full-time employees or drilling Reservists, to serve as alternate security managers to assist the primary security manager (as needed).

(2) Ensure **ALL** primary security managers attend a 40-hour security manager course approved by the USARC DCSINT. Security managers must receive training before or concurrent with, but not later than 6 months following, appointment and assumption of duties.

(3) Commit to the successful implementation of the Information Security Program.

(4) Commit necessary resources to implementing an effective Information Security Program

e. **All USAR security managers** will--

(1) Serve as their commander's adviser and direct representative for classified information matters.

(2) Issue written information security policies and procedures.

(3) Post their name and telephone number (use FORSCOM Form 102-R) in each organization.

(4) Establish and maintain a unit security education program.

(5) Ensure all military and civilian personnel receive the following briefings in accordance with AR 380-5: an initial security briefing, annual security briefings, foreign travel and force protection briefings, biennial SAEDA briefings, and termination briefings. Record all briefings on USARC Form 60-R (a blank copy is at the back of this regulation for reproduction purposes). In conjunction with USARC Form 60-R, use the initial and annual security briefing at appendix B, section I.

(6) Ensure all individuals with access to classified information complete a Classified Information Nondisclosure Agreement (SF 312) ***(see app B, sec II)***. Maintain a signed copy on file.

(7) Establish unit procedures to limit access of classified information to appropriately cleared personnel with a demonstrated need-to-know.

(8) Establish procedures to implement this regulation's requirements to safeguard, control, and destroy classified information.

(9) Advise unit personnel of all Army information security requirements.

(10) Report security violations, including compromises or other threats to safeguarding classified information to the USARC Command Security Manager.

(11) Establish and maintain procedures to control authorized visitor access to classified information, in accordance with this regulation ***(see chap 10)***.

(12) Issue local contingency plans for the emergency destruction or safeguarding of classified information.

(13) Conduct announced, unannounced, and after-hour security inspections of subordinate units.

(14) Properly issue and account for DD Forms 2501, Courier Authorization Cards, in accordance with AR 380-5.

(15) Prepare courier orders for personnel hand-carrying classified information aboard commercial aircraft or beyond the local 50-mile radius. ***(See para 6-3 and app D.)***

(16) Ensure that personnel hand-carrying classified information OCONUS receive authorization from USARC DCSINT ***(see para 6-4)***.

(17) Strictly adhere to all requirements of this regulation and required regulations listed in appendix A.

f. **All USAR civilian and military personnel** will-

(1) Safeguard all classified information.

(2) Comply with all requirements of this regulation and required references listed in appendix A.

1-5. Reporting requirements

Units will submit data in support of reporting requirements of (Executive Order) EO 12958 and other publications in

appendix A through the USARC DCSINT for further submission to higher headquarters.

Chapter 2
Classification

2-1. Classification
Use DOD 5200.1-R as the basis for classifying information. Assign the lowest level classification to information when the need or level of classification is in doubt.

2-2. Safeguarding classified information
All individuals must adequately protect classified information from compromise. Custodians will not apply in-house codes to make classified information available to a wider audience without first getting permission from the USARC DCSINT.

2-3. Original classification authority

a. The Secretary of the Army has authority for original classification of information. The Secretary of the Army has further delegated Original Classification Authority (OCA) to the Commander, U.S. Army Forces Command (FORSCOM). No original classification authority exists within the USARC.

b. Submit information developed within the USAR that may need classification, and has not been previously classified by an OCA, through HQ, USARC, ATTN: AFRC-INS to Commander, FORSCOM, ATTN: FCJ2-CIC. Include the entire document and an explanation of possible damage to national security if compromised.

c. Pending final classification, protect the material at the highest proposed classification level. Mark the information with the intended classification.

d. When the OCA reaches a decision, replace the temporary markings with appropriate classification markings .

2-4. Derivative classification
Any properly cleared individual who uses information that is already classified or requires classification based on guidance from an OCA has derivative classification authority. This authority does not require delegation or appointment in writing. All USAR personnel who generate information derived from original classification authorities must comply with the following:

a. Use derivative classification markings made by the OCA.

b. Verify the information's current level of classification before applying markings.

c. Ensure that information on the "Derived from" line is appropriate. If original information does not show a classification authority, request that information from the originator.

2-5. Compiled or associated information

a. Compiled unclassified items of information will normally not be classified. However, their compilation could provide an added factor that may warrant a higher classification than the component parts.

b. Classification by association occurs when the relationship between two or more unclassified items of information is, in itself, classified. For example, both the name of a weapon system and a randomly generated code word may be unclassified. However, the fact that the randomly generated code word relates to or stands for that weapon system may indeed be classified information.

c. An exception is Unit Status Reports (USRs). Base the classification of a USR on the number and size of units reporting. *(Additional classification guidance pertaining to USRs can be found in AR 220-1, para 2-8.)* For USAR units, classify the overall C-level, the level of any measured resource area, or any portion of the USR will be classified as follows:

(1) SECRET for a total of 10 or more Battalions, company-sized or separate companies or detachments (AA Level UIC's).

(2) CONFIDENTIAL for any combination of between two and nine Battalions, company-sized or separate companies or detachments (AA Level UICs).

(3) CONFIDENTIAL for a single unit (AA Level UICs).

(4) Unclassified for a single company-sized or separate company or detachment (AA level UICs).

d. When referencing the entire ARNG, USAR, or any other large groupings of units, classify the C-level, percentages, the level of any measured resource area, or references to deployability as SECRET. However, treat overall depictions of small slices of the USAR, or 50% of reserves when referring to an MSC, as FOUO vice SECRET, as long as C-levels are not associated with units. If several subordinate units C-ratings are listed, but only the higher headquarters is identified, treat the document as FOUO.

e. **Do not** omit or disguise information to make USR information unclassified. If in doubt, label and treat it as SECRET until the RSC or USARC DCSOPS can make a determination as to its classification. ***Do not transmit FOUO or classified information, to include USR data and unit COMPUSERVE accounts, via e-mail under any circumstances.*** Only transmit classified information in accordance with chapter 6 of this regulation.

f. Add - WARTRACE information extracted from the Global Command and Control System (GCCS) requires a subjective review as to the classification guidance in FORSCOM Regulation 11-30, paragraphs 2-23 through 2-26. The user must determine the classification of extracted data on a case-by-case basis. However, the originator has final responsibility for classification.

2-6. Duration of classification

a. Information is declassified as soon as it no longer meets the standards for classification. It remains classified only as long as it is in the interest of national security and meets the criteria stated in AR 380-5. When OCA originally classifies information, they decide the length of time for classification and select a declassification date or event. There are only two options: 10 years or less, or more than 10 years. If unable to determine a

declassification date that is 10 years or less, the OCA assigns an exemption designation per AR 380-5.

b. When OCA selects an exemption designation as the reason for classification beyond 10 years, they will indicate that on the material and on the classification guide, if any. Marking policy is contained in AR 380-5, chapter 4. An exemption category means that there is no requirement to select a specific date or event for declassification at that time.

c. Commanders will notify the USARC DCSINT, in writing, of any classified information they feel should be kept beyond 10 years or beyond the declassification date.

2-7. Sensitive But Unclassified (SBU) and Limited Official Use (LOU) information

a. Department of State-originated information is SBU if it warrants protection and administrative control, and is exempt from mandatory public disclosure under the Freedom of Information Act. Before 26 May 1995, the designator for this type of information was LOU. The LOU marking is now obsolete.

b. The Department of State does not require specific marking of SBU information, but does require holders to be aware of the need for controls. When including SBU information in DOD documents, mark them as FOUO. There is no requirement to re-mark existing material containing SBU information. Protect and limit access to SBU and FOUO information in the same manner.

Chapter 3
Declassification and Regrading

3-1. Declassification

a. Declassification is the complete removal of classification from an item of information. Regrading changes a document to a lower or higher classification. Authorization for downgrading or regrading is not designated below HQ, FORSCOM. Custodians of classified documents and information will process requests for declassification or regrading as follows:

(1) Identify the information and explain the basis for the request. Include a copy of the information when possible.

(2) Forward the request through HQ, USARC, ATTN: AFRC-INS, to the FORSCOM directorate having the functional area of interest.

b. Army Regulation 380-5, chapter 3, explains in detail declassification and regrading procedures.

3-2. Automatic declassification

The EO 12958 requires the automatic declassification of all classified information contained in records that--

a. Will be more than 25 years old on 17 April 2000.

b. Have been determined to have permanent historical value under Title 44, United States Code (U.S.C.) unless that information has been exempted from automatic declassification. After 2000, the same requirement exists for all material as it reaches its 25th year.

Chapter 4
Marking

4-1. Marking purpose and policy

Marking indicates the classification level and protection requirements of classified information. The term "marking" includes all methods of classification notification. Classification markings must be conspicuous. Custodians of classified information will comply with the requirements of this chapter.

4-2. Marking requirements

a. Appendix G of this regulation contains samples of classified markings and instructions. More detailed requirements are in AR 380-5.

b. All classified material must bear the following markings:

(1) The overall (highest) classification.

(2) The command, office of origin, date and, if not evident by the name of the command, the fact that the document was generated by the Army.

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

(4) Identification of the classification source(s) ("Classified by" or "Derived from" line) and, for originally classified information, concise reason(s) for classification.

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

(6) Most recent source date (on "Date of Source" line).

(7) Applicable warning notices, if any, and other markings, if any.

4-3. Overall classification marking

Mark classified documents with the highest classification of information within the document. Conspicuously mark, stamp, or affix (using sticker, tape, etc.) the overall classification on the document in the following locations:

a. Front and back covers (if any).

b. Title page (if any).

c. First page and back of the last page.

4-4. Command, office of origin, and date

Clearly mark the face of a classified document with the date of the document, and the originating command and office. This allows users to contact the originating command if questions or problems arise about the classification.

4-5. Page and portion marking

Each classified document will clearly show the information that is classified and at what level.

a. Each interior page, except blank pages. Conspicuously mark the top and bottom with the highest classification of the information on the page. Mark pages that have only unclassified information as "Unclassified."

b. Each portion of text. Mark with the appropriate abbreviation (TS for TOP SECRET, S for SECRET, C for CONFIDENTIAL, or U for UNCLASSIFIED) in

parentheses **immediately before the beginning** of the portion, but **after the letter or number** at the start of the text (e.g., 1. (S) This is a sample...).

c. The subject line or title of classified documents. Mark at the end of the subject or title with the appropriate abbreviation (TS, S, C, or U) to show the classification of information in the subject or title.

d. Charts, graphs, photographs, illustrations, figures, tables, drawings, etc. Mark with the unabbreviated (e.g., CONFIDENTIAL) classification of the information level revealed. Mark the captions and titles at the beginning, just as text portions would be marked.

e. Complied information.

(1) When a document is classified by compilation, but portions standing alone are unclassified, mark those portions (U). Mark the document and pages with the classification of the compilation.

(2) When the classification of individual portions is a lower level than the classification of the compilation, mark each portion accordingly. Then, mark the overall document and pages with the higher classification of the compilation.

(3) The cover or title page will contain an explanation of the classification by compilation in either of the above situations.

4-6. Sources of classification

The face of a classified document will contain the following markings:

a. "Classified by" line. Place on originally classified documents preceding the source of classification (the OCA), along with the reason for classification. Very few documents are originally classified.

b. "Derived from" line. Use on all derivatively classified documents preceding the source of classification. The majority of the documents classified within the USAR are derivatively classified. Complete the "Derived from" line as follows:

(1) If all the information was derivatively classified using a single security classification guide or only one source document, identify the guide or source and its date.

(2) If more than one security classification guide or source document was used, use the term "Multiple Sources." Maintain a record with the document file copy and include a list of sources with all document copies, if possible. If the derivatively marked source document states "Multiple Sources, cite the source document itself. Do not use "Multiple Sources" on the new derivatively marked document.

c. "Date of Source" line. Reflects the most recent source date.

4-7. Reason for original classification

This requirement applies only to originally classified documents. Do not use the "Reason" line on derivatively classified documents. The reasons are in AR 380-5.

4-8. Declassification instructions

Declassification instructions apply to both originally and derivatively classified documents. Mark declassification instructions, or the "Declassify on" line, on the face of the document as follows.

a. The instructions will—

(1) Specify either a date or event for declassification; ***or***

(2) Indicate the information is exempt from declassification within 10 years by using an "X" followed by a number (or numbers) showing the applicable exemption category (or categories) in AR 380-5.

b. If the OCA selects a date or event for declassification more than 10 years in the future, the date or event will follow the exemption category number. If more than one exemption applies, the original classified document will list each exemption.

c. To ensure all information in the document is protected for as long as necessary, use the most restrictive applicable declassification instructions (or the date or event furthest in the future).

d. If all information was from a document marked "Originating Agency Determination Required" (or "OADR") created before 14 October 1995, place "Source marked OADR" followed by the date of the document after the words "Date of Source". When using several sources of information marked "OADR," the "Date of Source" line will show the most recent date or the date of the latest document.

e. If a document is classified by "Multiple Sources" and different declassification instructions apply, the derivative classifier will use the most restrictive declassification instructions.

4-9. Downgrading

Downgrading instructions are not required for every document but, if required, the instructions will be on the face of each document. If the OCA determines to downgrade a document on a date or event, the marking will say, "Downgrade to CONFIDENTIAL on...," followed by the date or event. This will be immediately before the "Declassify on" line. The downgrade marking is used in addition to, and not as a substitute for, declassification instructions.

4-10. Marking special types of documents

a. Documents with component parts.

(1) If a classified document has components, such as annexes, appendices, or reference charts. Mark each component as a separate document.

(2) If a transmittal document contains information with the same or higher classification of the documents it is transmitting, mark it the same as any other classified document. If information on a transmittal is unclassified has a lower classification than one or more of the documents it is transmitting, mark it as follows:

(a) Conspicuously mark the face, top and bottom, with the highest classification of any of the documents being transmitted.

(b) On the face of the transmittal, show its classification status when separated from material being transmitted; e.g., "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES."

(3) Do not portion mark unclassified transmittals and their interior pages do not require markings.

b. Mark printed electronic messages transmitted on automated systems, the same as any other classified document. The first item in the text will be the overall classification. Include a properly completed "Classified by" or "Derived from" line, declassification instructions, and downgrading instructions (if any), in the last lines of the message.

4-11. Documents marked for training

Documents marked as classified for training purposes that contain no classified information will have clear markings to show they are actually unclassified; e.g., "CLASSIFIED FOR TRAINING ONLY."

4-12. Files, folders, and groups of documents

a. Clearly mark files, folders, and groups of documents with the highest classification of information they contain. Mark the classification on the outside of the file or folder (front and back). Attaching a document cover sheet to the front and back of the file or folder is acceptable.

b. When placed in secure storage, cover sheets may be removed. Mark any file or folder with no cover sheet in secure storage with the highest level of classified information in the file.

4-13. Automation information system (AIS) equipment-produced documents

Mark any AIS equipment-produced documents, including fan-folded printouts like any other classified document. Mark pages or other portions of AIS printouts removed for separate use or maintenance as standard individual documents. For specific marking of AIS media, refer to USARC Regulation 380-2.

4-14. Marking special types of material

Refer to marking provisions of AR 380-5, chapter 4-300, when marking special types of material that contain classified material. Examples of some special materials are: equipment, hardware, AIS media, film, tape, audiovisual media, or other materials not commonly thought of as documents. The main concern is to warn holders and users that materials contain classified information and require protection. Use common sense.

4-15. Standard Form (SF) labels

a. If not marked otherwise, items covered by this chapter may be marked with the appropriate SF 706 through SF 711 labels ***(see app A, sec III).***

b. Do not use the SF 709 (Classified Label for ADP Media) if the appropriate classification label is available and feasible for use.

c. There is no requirement to use SF 710 (Unclassified Label for ADP Media) in totally unclassified environments. However, if creating and using both classified and unclassified information in the same location, use SF 710 to distinguish the unclassified from the classified AIS removable storage media.

d. Using commercially pre-printed, color-coded floppy diskettes with classification markings of SECRET (red), CONFIDENTIAL (blue), UNCLASSIFIED (green), and SCI(yellow) is acceptable. However, if using the SF 710 labels on these diskettes, the classification markings on the label must show on the diskette top edge.

4-16. Re-marking

There is no requirement to re-mark material marked "IAW previous Executive Orders." Do not re-mark this material without specific instructions from the OCA. If the material is marked for automatic downgrading or declassification on a specific date or event, re-mark it as specified in AR 380-5. If the document does not specify a specific date or event for downgrading or declassification (e.g., "Declassify on: OADR"), do not re-mark the item until it reaches 25 years.

Chapter 5
Access, Control and Safeguarding

5-1. Responsibilities

All Army personnel with access to classified information are both personally and officially responsible for safeguarding that information. Access requires both an appropriate clearance and a need-to-know. The custodian of the information, not the recipient, will verify the appropriate clearance. Responsibilities to safeguard classified information extends to all means of access, to include keeping classified conversations out of hearing distance of unauthorized personnel. **NEVER** collect, obtain, record or remove classified information for personal use.

5-2. Nondisclosure Agreement (NDA), SF 312

All Federal employees in positions requiring access to classified information must sign a Classified Information Nondisclosure Agreement (NDA), SF 312. The NDA is a contract between the U.S. Government and the cleared employee in which the employee agrees never to disclose classified information to an unauthorized person. Refusal to sign is grounds for withdrawal of security clearance and access. All persons who have a security clearance must have a copy of the signed SF 312 on file with the security manager. *(See app C for more specific guidance.)*

5-3. Retirement or resignation

Security managers or designated command officials will ensure compliance with the following regarding retiring or resigning personnel:

a. Ensure all DOD personnel who are retiring, resigning, or being discharged out-process through their office. During out-processing, inform the individuals that their security clearance and access to classified information has been terminated, but that they still have an obligation to protect classified information. Have military personnel sign a debriefing statement. Encourage civilian employees to also sign a debriefing statement, although it is not required.

b. When a person resigns or retires from government service, use either a DA Form 2962 (Security Termination Statement), or the debriefing portion of the security manager's file copy of the SF 312. If using a DA Form 2962, the copy of the NDA can be destroyed. If using the copy of the SF 312, the debriefing itself will be the original. In either case, retain the debriefing on file for 2 years.

5-4. Control measures

a. The custodian will protect classified information at all times either by storage in a GSA-approved container or having it under the personal observation and control of an authorized individual.

b. During working hours, the custodian will keep classified materials removed from storage under constant surveillance by authorized personnel. Place classified cover sheets (SFs 703, 704, and 705) on classified documents or files not in a GSA-approved container.

c. Personnel at all commands that access, process, or store classified information conduct end-of-day security checks using SF 701 (Activity Security Checklist).

d. To minimize the risk of compromise, the security manager will develop a plan for emergency safeguarding of classified materials. The plan must cover the protection, removal, or destruction of classified materials in case of fire, flood, earthquake, other natural disasters, civil disturbances, terrorist activities, or enemy action. A sample emergency plan is at appendix E.

e. Personnel will only discuss classified information over secure communication equipment and circuits approved for transmission of information at the level of classification being discussed.

f. Security managers will ensure no classified information remains within any GSA-approved storage containers or information processing equipment before removal. These items of equipment include safes, reproduction equipment, facsimile machines, micrographics readers and printers, AIS equipment and components, and shredders. Security managers will have cleared personnel inspect such equipment before removal from protected areas or before unauthorized persons can access the equipment without escort.

g. Visit requests.

(1) Except when a continuing working relationship is established, through which current security clearance and need-to-know are determined, USARC personnel visiting other Army commands will provide--

(a) Advance notification.

(b) Request to visit.

(c) Verification of security clearance signed by the respective security manager (if visit involves access to classified information).

(2) Consider visit requests approved unless receiving notification to the contrary. They may remain valid for not more than 1 year. Each agency outside of the Army has its own criteria for a visit request. Exercise care with non-relevant personal information outside the USARC.

5-5. Classified meetings and conferences

a. All meetings, conferences, classes, seminars, symposia, or other similar activities are classified if presentation or discussion of classified information takes place. Without exception, all security requirements in this regulation and other applicable security regulations apply.

b. Individuals coordinating classified activities will—

(1) Limit attendees to persons possessing an appropriate clearance and the need-to-know.

(2) Conduct classified meetings only at military installations or reserve centers. If concerns arise regarding a classified meeting (e.g., location, facility, attendees, foreign visitors, etc.), contact the USARC DCSINT for guidance.

(3) Keep announcements of classified meetings unclassified by limiting information to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

c. The security manager will ensure adherence to the actions in appendix F.

5-6. Receipt of classified materials

a. All mailroom managers of USARC subordinate units will develop standing operating procedures (SOP) to protect and limit access to incoming mail and bulk shipments. The SOP will specify how to protect items delivered to a unit (e.g., locked in a GSA-approved container for up to and including SECRET information) until determining whether it contains classified information.

b. All mailroom personnel will have at least a SECRET clearance.

5-7. Residential storage and classified discussions

All personnel will comply with the following:

a. Do not store classified information in a personal residence or outside an approved location for any reason.

b. Do not conduct classified discussions in personal residences, in public areas or transportation conveyances, or in any area outside approved spaces on a government or cleared contractor facility.

c. To the extent that FORSCOM policy permits, installation of secure telephones may be authorized in certain situations where immediate contact and discussion of classified information during off-duty hours is necessary. Notify the USARC DCSINT if a situation arises requiring installation of a secure telephone unit in a private residence.

5-8. Storage and safeguarding

a. Secure classified information adequately to prevent access by unauthorized persons and to meet the minimum standards in AR 380-5. Do not store items having only monetary value (e.g., cash, negotiable checks or securities, precious metals, jewelry, narcotics, and unclassified hand weapons) in any security container, vault, or other area designated for classified material storage.

b. Use only GSA-approved storage equipment to store and protect classified information. In accordance with AR 380-5, guard or store classified information not under the personal control and observation of an authorized person in a locked security container, vault, room, or area.

c. There is no mandatory cutoff date for the Congressional mandate to install electronic locks on classified information storage containers. However, units will install electronic locks as soon as feasible to ensure maximum coverage of the warranty period.

5-9. Entry and exit inspections

Do not conduct entry and exit inspections without prior approval of the USARC DCSINT.

5-10. Equipment designations and combinations

a. Do not externally mark containers or vaults with the level of classified information authorized for storage. Do not post emergency evacuation and destruction priorities on the exterior of storage containers, vaults, or secure rooms. Affix a number to the outside for identification purposes only.

b. Change combinations under the following conditions: when initially placed in use; whenever an individual no longer has access; when the combination has been subject to possible compromise; at least once ***every*** year; or when taken out of service. Only authorized individuals with appropriate security clearances will change combinations.

c. Reset the combination for locks being taken out of service to 50-25-50.

d. Treat combinations, including ***any*** pertinent written record, as having a classification equal to the highest category of information it protects. Store combinations in containers approved for the appropriate level of classified information.

e. Use an SF 700 (Security Container Information) as a record for each container, vault, or secure room that stores classified information.

f. Release combinations only to those individuals authorized access to the protected information.

g. Control entrances to secure rooms or areas in accordance with AR 380-5, appendix G.

5-11. Repair of damaged security containers

Repair, turn-in, or transfer security containers in accordance with AR 380-5, chapter 5.

5-12. Accountability of TOP SECRET information

a. In accordance with AR 380-5, commands that handle or maintain TOP SECRET materials will appoint a TOP SECRET Control Officer (TSCO) . The TSCO will establish procedures for the control and management of TOP SECRET information.

b. Use AR 380-5, paragraph 5-400, as a guide for the control and management of all TOP SECRET documents.

5-13. Accountability of SECRET and CONFIDENTIAL information

In accordance with AR 380-5, commands will establish procedures for the control of SECRET and CONFIDENTIAL information .

5-14. Classified working papers

a. Working papers are any documents and materials accumulated or created while preparing finished classified documents and material.

b. Users will control and manage classified working papers as follows:

(1) Date them when created.

(2) Mark them with the highest classification of any information they contain.

(3) Protect them in accordance with the level of classification.

(4) Destroy them when no longer needed.

(5) Account for, control, and mark them in the manner prescribed for a finished document of the same classification when they--

(a) Are released by the originator outside the command, or transmitted electronically or through message center channels within the activity.

(b) Are retained more than 90 days from the date of origin.

(c) Are filed permanently.

(d) Contain TOP SECRET information.

5-15. Reproduction of classified information

a. Individuals will only reproduce classified information as necessary to accomplish the command's mission. Commanders will establish and enforce procedures for reproduction of classified information.

b. Custodians of classified materials may reproduce classified materials only when approved by a command or unit-designated official. Security managers will designate an individual within each unit, in writing, to oversee reproduction of classified material, up to and including SECRET. Identify the appointed individual on FORSCOM Form 138-R (Equipment is Designated for Reproduction of Classified Material). Preferably, the designated official will be the command or unit security manager, or the alternate security manager.

c. All reproduced copies of classified documents, including working papers, require the same safeguards and controls as the original document.

d. Security managers must designate specific equipment that does not leave latent images for reproduction of classified information. They must post FORSCOM Form 138-R on or near the designated equipment.

e. Security managers will post a FORSCOM Form 93-R (Warning Reproduction of Classified Material with this Equipment is Prohibited) on or near equipment only authorized for unclassified reproduction.

f. No one will reproduce TOP SECRET materials without the originator's approval.

5-16. Disposition and destruction of classified materials

a. Custodians will only retain classified documents if they required for effective and efficient command operation, or if required by law or regulation.

b. All custodians will dispose of classified documents no longer required for operational reasons, in accordance with AR 25-400-2.

c. In accordance with DOD Directive 5200.1-R, all DOD activities will have a cleanout day each year to destroy unneeded classified holdings. The USARC annual cleanout day is 1 July. All USARC MSC and installation security managers will ensure that all subordinate units, down to and including companies and detachments, destroy unnecessary classified documents prior to that date.

5-17. Destruction methods and standards

a. Custodians will destroy classified documents and materials sufficiently to preclude recognition or reconstruction of the classified information. Some methods of destruction are: burning, melting, chemical decomposition, pulping, pulverizing, cross-cut shredding, or mutilation.

b. USARC Regulation 380-2, chapter 6, establishes procedures for destruction and degaussing of magnetic media.

c. The unit security manager will approve all newly purchased shredders. Shredders will meet required specifications for destruction of TOP SECRET materials, in accordance with AR 380-5.

d. Custodians will ensure collection of classified material for later destruction (e.g., burn bags, burn drawers) includes provisions to minimize risk of compromise of the material while it awaits destruction.

5-18. Destruction records

a. Records of destruction are required for TOP SECRET documents. The custodian and a witness will observe the destruction and sign the DA Form 3964 (Classified Document Accountability Record) that accompanies the document. Notes, ribbons, carbons, etc., that contain TOP SECRET information do not require destruction records. The security manager will file the document transmittal receipt for 2 years.

b. Records of destruction are not required for SECRET or CONFIDENTIAL documents; but, the security manager will file any document transmittal receipts for 2 years.

Chapter 6
Transmission and Transportation

[Requirements of this chapter apply to all custodians of classified material.]

6-1. Transmission and transportation policy

a. Transmit or transport classified information only as specified in AR 380-5. Never use street side mail collection boxes for the dispatch of classified information. All unit mailroom managers will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger until determining whether it contains classified information.. They will establish screening points to limit access of classified information to cleared personnel.

b. The U.S. Postal Service registered mail and U.S. Postal Service Express Mail may be used for transmission of classified information (SECRET and below) within and between the 50 states, the District of Columbia, and the Commonwealth of Puerto Rico. Do not use U.S. Postal Service Express Mail Label 11-B under any circumstances.

c. Urgent situations may warrant use of the current GSA contract holder (e.g., FEDEX) for overnight or next-day delivery of classified material (up to SECRET). The following conditions must apply for this authorization:

(1) It must be the most cost effective way to meet a program requirement, given time, security and accountability restraints.

(2) Provisions of DOD regulation 5200.1-R concerning wrapping, addressing and receipting remain in effect. However, the contract holder's envelope may be considered as the second envelope for purpose of double wrapping.

(3) Use only within CONUS.

(4) To ensure direct delivery to the addressee, do not complete the release signature block on the airbill label under any circumstances;

(5) SECRET and CONFIDENTIAL material must meet the carrier's size and weight limitations.

(6) Only ship packages via the contract holder on Mondays through Thursdays, to ensure the carrier does not have possession over a weekend.

6-2. Preparation of material for transmission

a. Classified information will be enclosed in two durable opaque, sealed envelopes, wrappings, or containers for transmission. If the classified material is an internal component of equipment, the outside shell may serve as the inner enclosure if it does not reveal classified information.

b. When classified material is hand-carried outside an activity, a locked briefcase may serve as the outer wrapper. There are no addressing requirements when using a locked briefcase.

c. Address the outer envelope or container to an official government activity and show the complete return

address of the sender. Never address the outer envelope to an individual; however office codes are acceptable. The outer envelope will not bear any classification markings or any special instructions.

d. The inner envelope will show the address of the receiving activity, the address of the sender, the highest classification of the contents and may have an attention line.

e. The security manager, supervisor, or someone in authority must know of the classified material being transported, the reason, and the anticipated time and date the courier is expected to return.

6-3. Hand-carrying classified materials

a. When other methods are not feasible, security managers may authorize appropriately cleared personnel to escort or hand-carry classified material between locations…but only when absolutely necessary. Give first consideration to secure facsimile or U.S. Postal Service Express Mail.

b. Security managers will issue and control DD Form 2501 (Courier Authorization Card) as required by AR 380-5 and FORSCOM Suppl 1. Security managers will only issue cards to appropriately cleared individuals. Cards are only for hand-carrying- classified information locally within a 50-mile radius of the individual's command. Courier cards will be on the individual's person when transporting classified information between buildings on all Reserve facilities. If an individual is hand-carrying classified information on a one-time basis, authorization may be documented by the use of a courier authorization letter in lieu of the DD Form 2501.

c. Commanders will include guidance and restrictions on the use of DD Form 2501 in their security SOP. The completed courier card will identify the individual and will have an expiration date not to exceed 1 year. No indication of special access will be on the card. Security managers will maintain a record of each card's control number. If the courier card is lost or stolen, the courier will immediately report it to the security manager. When designated couriers permanently depart the duty station or no longer require courier cards, they will surrender the cards to the security manager.

d. See appendix D for courier briefings, detailed courier card issuance instructions, and a sample courier memorandum for carrying classified material beyond a 50-mile radius. USARC Form 90-R (USARC Courier Briefing Acknowledgement) is at the back of this regulation for local reproduction.

6-4. Security requirements for TDY travel OCONUS

a. Hand-carrying classified material OCONUS subjects the information to increased risk. Strictly follow the requirements of AR 380-5 and AR 380-10.

b. The USARC DCSINT, the USARC Command Security Manager, or their designees must provide a written original authorization to carry classified material OCONUS. This memorandum will serve as the courier's authorization to hand-carry classified materials aboard commercial aircraft between CONUS and OCONUS. Additionally, block 16 of DD Form 1610 (Request and Authorization for TDY Travel for DOD Personnel) will state, "Traveler is authorized to carry classified material."

c. When requesting authorization to hand-carry classified information OCONUS, submit a copy of the courier's travel orders and USARC Form 81-R (USARC OCONUS Handcarry Classified Information Request) to the USARC DCSINT. A blank copy of USARC Form 81-R is at the back of this regulation for reproduction purposes. Upon receipt, the USARC DCSINT will review the request, and if justified, issue an OCONUS Courier Orders memorandum within 5 working days. When the unit receives the memorandum, the security manager will give the courier a security briefing and forward it along with a signed USARC Form 90-R to USARC DCSINT for retention ***(see sample briefing at app D)***.

Chapter 7
Security Education

7-1. Policy

a. Commanders will establish security education programs to promote security compliance by command personnel. Programs will—

(1) Provide necessary knowledge and information for quality performance of security functions.

(2) Promote understanding of information security program policies and requirements and their importance to the national security.

(3) Instill and maintain continuing awareness of security requirements.

(4) Assist in promoting motivation to support program goals.

b. Security education should be continuous. Supplement annual briefings and periodic training sessions with other informational and promotional efforts. Use job aids whenever possible to achieve program goals.

7-2. Initial and refresher briefings

a. Security managers will—

(1) Ensure all newly assigned military and civilian personnel will receive an initial security briefing (within 3 working days for full-time employees and during the first drill weekend for reservists).

(2) Ensure all personnel receive an annual refresher briefing.

(3) As a minimum, use the USARC Security Briefing (app B, sec I) for the initial and refresher briefings.

(4) Annotate briefings on USARC Form 60-R.

b. Prior to receiving access to classified information, employees must sign an NDA, SF 312 ***(see para 5-2 and app B, sec II)***. Advise individuals refusing to sign the form that it is mandatory before they may have access to classified information. Immediately notify the command's security team and request further guidance in these cases. Reluctance to sign an NDA demonstrates a lack of personal commitment to protect classified information and that person's clearance will be denied or revoked.

7-3. Derivative classifiers
Security managers will ensure all personnel responsible for derivative classification receive training in requirements and procedures appropriate to the information and materials they will be classifying. Training will include the use of classification guides and source documents.

7-4. Security manager training
All unit security managers, from company level up, will attend a Security Manager Course approved by the USARC DCSINT. Training must be sufficient to permit quality performance of security manager duties. It must take place before or concurrent with, but not later than 6 months following, the assumption or appointment of security manager duties.

7-5. Other security education briefings and programs

a. Personnel who use automated information systems to store, process, or transmit classified information will receive special training in accordance with AR 380-19.

b. All U.S. Army civilian and military personnel must receive an antiterrorism and force protection briefing prior to traveling OCONUS, either in an official or unofficial capacity. Additionally, DA recommends that family members traveling OCONUS receive the briefing. Security managers will maintain a log of such briefings for a minimum of 2 years. Use USARC Form 91-R (Foreign Travel Briefing Statement) to record the briefing (app D, sec III).

c. Personnel will receive appropriate briefings if traveling to foreign countries where special concerns about possible exploitation exist, or if attending meetings or conferences where foreign attendance is possible . Foreign travel briefings are a defensive measure to alert the traveler to possible risks and to furnish guidance that may help to overcome those risks. Individuals who travel frequently do not need briefings for each occasion, but require a thorough briefing at least once every 6 months, as well as a general reminder of security responsibilities prior to each such activity. Security managers will obtain travel advisories from the Department of State for countries to which personnel plan to travel.

d. Personnel escorting, hand-carrying, or serving as a courier for classified information will receive an appropriate briefing ***(see app D)***.

e. Personnel authorized access to special compartmented information (SCI) or any classified information requiring special controls or safeguarding measures will receive a briefing from an SSO.

f. Subversion and Espionage Directed Against the U.S. Army (SAEDA) training will be given biennially. The SAEDA training may be combined with other security training in order to conserve resources. Commanders with highly sensitive missions, or whose missions are priority targets for foreign intelligence collection, may conduct SAEDA or other awareness training more than biennially. The SAEDA training may be on a continual basis, but each employee must receive SAEDA training at least once every 2 years.

g. Establish procedures to issue termination briefings to cleared employees who leave the command or whose clearance is terminated. The Security Debriefing Acknowledgment portion of the SF 312 or DA Form 2962 (Security Termination Statement) may serve as the termination briefing documentation.

Chapter 8
Unauthorized Disclosure and Other Security Incidents

8-1. Unauthorized disclosure policy

a. The loss or compromise of classified information or materials can cause damage to our national security. Notify the USARC DCSINT within 24 hours if loss or compromise of classified information occurs. Additionally, the commander will take immediate action to minimize the damage and eliminate any further compromises.

b. Prompt and effective investigation of the situation and prompt reporting of results are critical. Each incident of possible loss or compromise of classified information or material must be the subject of an inquiry, in accordance with AR 380-5. A preliminary inquiry will determine whether classified information was compromised and, if so, whether damage to national security may result. Additionally, it will determine what persons, situations, and conditions were responsible for, or contributed to, the incident.

c. Provisions of other Army regulations that require the investigation and reporting of counterintelligence, criminal, or other serious incidents may also apply; i.e., AR 381-10, AR 195-2, AR 380-40, AR 380-381 and AR 190-40. Follow all pertinent Army regulations in reporting and investigating the loss or compromise of classified information or materials.

8-2. Discovery of incident

a. Anyone finding classified materials out of proper control will safeguard the materials and immediately notify the commander, the security manager or other command-designated official.

b. Anyone who becomes aware of the possible loss or compromise of classified information will immediately report it to the commander, the security manager, or other command-designated official.

c. If the individual making the discovery believes that the commander, security manager, or other official designated to receive such reports may be involved in the incident, that person may report it to security authorities at the next higher level of command or supervision, or directly to the USARC DCSINT.

d. If classified information appears in the public media, or if a representative of the media wishing to discuss information approaches personnel, they will not make any statement or comment to confirm the accuracy or the classification of the information. Additionally, they will report the fact to the appropriate command security and public affairs authorities.

8-3. Inquiry

a. The commander will immediately initiate an inquiry into any report of possible loss or compromise of classified information.

b. Except in unusual circumstances, the Command Security Manager will not conduct the preliminary inquiry, but will ensure appointment of an inquiry official and that the inquiry is done in accordance with this regulation. The appointed individual will—

(1) Have an appropriate security clearance.

(2) Have the ability and available resources to conduct an effective inquiry.

(3) Be senior to the individual(s) involved.

(4) NOT be involved in the incident.

c. The preliminary inquiry will follow the format in FORSCOM Suppl 1 to AR 380-5, figure R-1. The official will forwarded it through command channels to the USARC DCSINT within 10 working days following the incident or discovery.

d. In cases of apparent loss of classified material, the official conducting the inquiry will initiate a thorough search for the material.

e. The inquiry will focus on answering the following:

(1) When, where, and how did the incident occur?

(2) What specific information and material was involved and what level of classification was it?

(3) What situations, conditions, or persons caused or contributed to the incident?

(4) Did compromise occur?

(5) If compromise occurred, can damage to national security be expected?

f. In cases of apparent unauthorized disclosure of classified information to the public media, the inquiry will include—

(1) Identification of the article or program in which the classified information appeared.

(2) To what extent the information was disseminated.

(3) If the information was properly classified.

(4) If the information was officially released previously.

(5) If there are any investigative leads or suspects.

(6) If an investigation will increase the damage caused by the disclosure.

g. The inquiry official will forward a DA Form 5248-R to the USARC personnel security team on each individual known to have been responsible for the security violation.

8-4. Unauthorized absences, suicide, and attempted suicide

Notify the USARC DCSINT, through command channels, when an individual with access to classified information is absent without authorization, or attempts or commits suicide. Additionally, inquire into the situation for indications of activities, behavior, or associations that may indicate classified information is at risk. If so, notify the supporting 902nd Military Intelligence unit.

Chapter 9
Security Inspections

9-1. Biennial security inspections

a. Travel funds and personnel permitting, the USARC DCSINT staff will conduct biennial security inspections of USARC RSCs, DRUs, and installations in accordance with AR 380-5. The RSCs, DRUs, and installations will conduct biennial security inspections of their subordinates, and as feasible, unannounced and after-hour inspections. Units will conduct self-inspections during any off year that an official inspection is not conducted.

b. Use USARC Form 68-R (Security Inspection Checklist) for both official and self-inspections. Forward a written record to higher headquarters and maintain it on file until the next official inspection by the higher headquarters. The only exception to policy for conducting an inspection earlier than the biennial inspection schedule allows is if a command security manager is transferring and the unit has not had an inspection during that individual's tenure.

9-2. Security Inspection Checklist (USARC Form 68-R)

a. Use the USARC Form 68-R to evaluate and assess the implementation and management effectiveness the security program. (A blank copy of USARC Form 68-R is at the back of this regulation for reproduction purposes.) The Security Inspection Checklist is divided into six parts:

(1) Program Management.

(2) Personnel Security Program.

(3) Information Security Program.

(4) Information Systems Security Program.

(5) Controlled Cryptographic Items (CCI) and Secure Telephone Unit, Third Generation (STU III).

(6) Intelligence Oversight Program.

b. Questions focus on compliance with DOD, DA, and FORSCOM security policies and USARC guidance, when applicable. Specifically identify, any area of non-compliance, security weaknesses, and recommendations for improvement in the remarks section.

c. Forward written findings of all security inspections to the next higher headquarters. The security manager will maintain results on file until completion of the next 'Fully Met' inspection.

d. Inspection ratings are at the beginning of each program on the form. These ratings are: 'Fully Met,' 'Partially Met,' or 'Not Met.' To receive an overall rating of 'Fully Met,' all programs must be 'Fully Met.' Give an overall rating of 'Partially Met' for anything less than 'Fully Met,' but not if any programs are 'Not Met.' Assign an overall rating of 'Not Met' if any program is 'Not Met.'

Chapter 10
Foreign Visitors and Foreign Disclosures

10-1. General

a. An appropriate Delegation of Disclosure Authority must specifically authorize any disclosure of classified military information. Foreign disclosures of classified

military information and technical data must be in support of U.S. national security interests.

b. Specific foreign visitor and foreign disclosure is in AR 380-10. Any interactions between units and foreign visitors, including informally coordinated visits, must comply with the requirements of AR 380-10 to avoid mutual confusion and embarrassment.

c. The foreign visitor request process must begin with the requester's Washington, D.C.-based diplomatically accredited military attaché or embassy. Attachés know the appropriate DA channels of communication and are familiar with the policies and procedures in AR 380-10. The military attaché submits the visit authorization to the ODCSINT, DA, who will staff the request through FORSCOM to the USARC DCSINT.

10-2. Foreign visitor and disclosure guidance

a. In accordance with AR 12-15, permit foreign participants in unit training exchanges access to only unclassified information, except as specifically authorized by AR 380-10, or as approved by DA ODCSINT on a case-by-case basis.

b. Immediately notify the USARC DCSINT (Command Security Manager) if a foreign visitor notification arrives through functional channels rather than from DA or the USARC DCSINT. Inform the foreign national's embassy to submit a visit request to HQDA, DAMI-CHS.

c. Restrict foreign visitors to the minimum amount of information necessary to accomplish the mission of their visit. Make every effort to conduct the visit at the unclassified level. If the purpose of the visit requires disclosure of classified information, provide the USARC DCSINT a brief narrative of the information proposed for release, justification, and a statement of the "net benefit" to the U.S. from the disclosure. Mail any classified narrative in accordance with AR 380-5.

d. In order to protect the interests of individuals, DOD, and the U.S. Army, it is absolutely critical that commanders ensure all unit members are aware of the requirements of AR 380-10 concerning contact with foreign representatives.

Appendix A
References

Section I
Required Publications

EO 12958 (Classified National Security Information). Cited in paras 1-5, 3-2, fig B-1, glossary.

AR 25-400-2 (The Modern Army Recordkeeping System (MARKS)). Cited in para 5-16b.

AR 380-5 w/FORSCOM Suppl 1 (Information Security). Cited in paras 1-1, 1-4a(1), 1-4e(5),1-4e(14), 2-6, 3-1b, 4-2a, 4-7, 4-8a, 4-14, 4-16, 5-8, 5-10g, 5-11, 5-12, 5-13, 5-17c, 6-1a, 6-3b, 6-4a, 8-1b, 8-3b, 9-1, 10-2c, fig C-1, fig C-2, fig C-3, app F.

AR 380-10 (Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives). Cited in paras 6-4a, 10-1, 10-2.

AR 380-15(C) (Safeguarding Classified NATO Information (U)). Cited in fig C-2.

AR 380-19 (Information Systems Security). Cited in para 7-5a.

AR 380-40 (Policy for Safeguarding and Controlling Communications Security (COMSEC) Material). Cited in para 8-1c.

AR 380-381(C) (Special Access Programs (U)). Cited in para 8-1c.

DOD Dir 5200.1-R (DOD Information Security Program Regulation). Cited in para 2-1.

USARC Reg 380-2 (Information Systems Security) . Cited in paras 4-13, 5-17b, and fig B-1.

Section II
Related Publications

EO 12972 (Amendment to Executive Order No. 12958)

AR 12-15 (Joint Security Assistance Training (JSAT) Regulation)

AR 340-17 (Release of Information and Records from Army Files (Freedom of Information Act Program))

AR 360-5 (Public Information (DOD Directive 5230.9, Clearance of DOD Information for Public Release))

AR 380-28 (Sensitive Compartmented Information (SCI))

AR 380-49 (Industrial Security)

AR 380-67 (Personnel Security Program)

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

DCID No. 1/7 (Directive of Central Intelligence Directive No. 1/7)

Section III
Prescribed Forms

USARC Form 60-R (Personnel Initial/Annual Security Briefing Record). Cited in paras 1-4e(5), 7-2a, app B.

USARC Form 68-R (Security Inspection Checklist). Cited in paras 9-1, 9-2.

USARC Form 81-R (USARC OCONUS Handcarry Classified Information Request Form). Cited in paras 6-4c, C-7.

USARC Form 90-R (USARC Courier Briefing Acknowledgement). Cited in paras 6-3d, 6-4c, C-4.

USARC Form 91-R (Foreign Travel Briefing). Cited in paras 7-5b, C-9.

Section IV
Related Forms

DA Form 455 (Mail and Document Register)

DA Form 2962 (Security Termination Statement)

DA Form 3964 (Classified Document Accountability Record)

DA Form 5248-R (Report of Derogatory Information)

DA Label 87 (For Official Use Only) cover sheet

DD Form 1610 (Request and Authorization for TDY Travel for DOD Personnel)

DD Form 2501 (Courier Authorization Card)

SF 312 (Classified Information Nondisclosure Agreement)

SF 700 (Security Container Information)

SF 701 (Activity Security Checklist)

SF 702 (Security Container Check Sheet)

SF 706 (TOP SECRET Label for ADP Media)

SF 707 (SECRET Label for ADP Media)

SF 708 (CONFIDENTIAL Label for ADP Media)

SF 709 (Classified Label for ADP Media)

SF 710 (Unclassified Label for ADP Media)

SF 711 (Data Descriptor Label for SCI Media)

SF 712 (Classified SCI Label for ADP Media)

FORSCOM Form 93-R (Warning Reproduction of Classified Material with this Equipment is Prohibited)

FORSCOM Form 102-R (Security Manager Poster)

FORSCOM Form 138-R (Equipment is Designated for Reproduction of Classified Material)

FORSCOM Label 236-R (This Equipment will not be Used to Process Classified Information)

Appendix B
Security and Classified Information Requirements

Section I
Security Briefing

[Recommend security managers use this briefing at figure B-1 in conjunction with USARC Form 60-R, Personnel Initial/Annual Security Briefing Record.]

Security Briefing

1. Introduction

a. As a DOD employee who occupies a position that requires access to classified information, you have been the subject of a personnel security investigation. A personnel security investigation is an inquiry into the loyalty, integrity, discretion, morals and character of an individual employed by or under contract to the U.S. Government. The purpose of that investigation was to determine your trustworthiness for access to classified information. When the investigation was completed, the Central Clearance Facility (CCF) granted you a security clearance based upon a favorable adjudication of the investigative results. Once the security clearance was granted, you met the first of three requirements necessary to have access to classified information.

b. The second requirement that you must fulfill is to sign an SF 312, Classified Information Nondisclosure Agreement. This requirement was established in a presidential directive that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." The SF 312 is a contractual agreement between the U.S. government and you, a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of--

(1) The trust that is placed in you by providing you access to classified information.
(2) Your responsibilities to protect that information from unauthorized disclosure.
(3) The consequences that may result from your failure to meet those responsibilities.

c. The third requirement is a "need-to-know." The holder of classified information, to which you seek access, is responsible for confirming your identity, your clearance, and your "need-to-know." As a holder (custodian) of classified information, you are responsible for making these same determinations with respect to any individual to whom you may disclose it.

2. What is classified information?

Classified information is information that requires protection against unauthorized disclosure in the interest of national security, and is classified under one of three designations: TOP SECRET, SECRET, or CONFIDENTIAL.

a. *TOP SECRET* is applied only to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security. ALL control and accountability of TOP SECRET documents will be handled by the TSCO.

b. *SECRET* is applied only to information whose unauthorized disclosure could reasonably be expected to cause serious damage to national security.

c. *CONFIDENTIAL* is applied only to information whose unauthorized disclosure could reasonably be expected to cause damage to national security.

3. Classification of information

a. Security classification is not used to conceal violations of law, inefficiency, administrative error, prevent embarrassment, nor to restrain competition. Information may be classified either originally or derivatively.

(1) *Original Classification* is an initial determination by an Original Classification Authority (OCA), who has been designated in writing, that information requires protection against unauthorized disclosure in the interest of national security.

Figure B-1. Security Briefing

(Continuation of Security Briefing)

(2) *Derivative Classification* is classification derived from another source. It is the act of incorporating or restating information already classified, and marking that material consistent with the security markings of your source document and information. Over 95% of all classification decisions in the Army are derivative.

b. Information is classified derivatively, either through the use of a reference document, such as a security classification guide, or another source document, such as an Army regulation, OPLAN, message, report or memorandum. Information taken from a classified report or memorandum, and incorporated into a new document is derivatively classified in accordance with the classification markings shown in the source document. Of course, if the information taken from the classified source is unclassified, then the new document is also unclassified. If the source document does not provide enough guidance for you to determine what the derivative classification should be, contact your security manager for assistance.

4. Access

a. No person may have access to classified information unless that person has the appropriate security clearance and a demonstrated need-to-know. If you have authorized possession, knowledge, and control of information, YOU are the person responsible to determine if another person's official duties require access to that classified information and if that person has been granted the appropriate security clearance by CCF.

b. No one, regardless of rank or position or mere possession of a badge, has a right to have access to classified information. DON'T ASSUME ANYTHING. Check identity, clearance, need-to-know, and ability to protect (or store) the information before passing classified information to anyone. You must strictly limit distribution of papers and other media containing classified information. When in doubt, do not route. Avoid routine dissemination of classified material.

5. Accountability of classified information

TOP SECRET information is accounted for by a continuous chain of receipts. SECRET information is controlled through administrative procedures (i.e., receipt) in the absence of hand-to-hand transfer. Appropriate administrative controls are also required to ensure that CONFIDENTIAL information is protected.

6. Protecting classified information.

a. All security procedures that we follow have two goals in mind: to PREVENT those who have NO NEED TO KNOW from being exposed to the information; and secondly, to PREVENT deliberate compromise.

b. As a custodian of classified information, you have a personal, moral, and legal responsibility, at all times, to protect classified information, whether oral or written, within your knowledge, possession, or control. You are further responsible for locking classified information in a GSA approved security container, whenever it is not in use, under the direct supervision of authorized persons, or in an area approved for open storage of classified information. Further, you must follow procedures that ensure that unauthorized persons do not gain access to classified information.

(1) Classified information must not be discussed on a non-secure telephone, read, or discussed in public places. "*Talking around*" classified information or using private codes doesn't really fool anyone and must be avoided. Many leaks of classified information result from conversations or interviews.

(2) Never leave documents uncovered or unattended.

(3) Always use cover sheets.

(4) Never "drop off" classified.

(5) Only use in authorized areas.

(6) Be very cautious in dealings with persons not authorized to have access to classified information. Remember, leaks may be just as damaging to our national security as outright espionage.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

c. Classified documents removed from storage must be kept under constant surveillance. Cover sheets used shall be SFs 703, 704, 705 for TOP SECRET, SECRET, and CONFIDENTIAL documents, respectively. Drafts, carbons, notes, working papers, ribbons, disks, or any items containing classified information must be destroyed when no longer needed, or must be classified and handled just as the classified information they contain.

7. Marking classified information

a. When you mark (or stamp) a classified document, you communicate a decision. You alert people that the information is classified, and at what level. At a minimum, classified documents must indicate:

(1) The highest level of classification at the top and bottom of the first page, title and cover pages, and back page and cover, if any.

(2) Portion markings for each section, part, paragraph, subparagraph, or similar portion. The subject and title also contain a portion marking.

(3) Interior pages are marked top and bottom with the OVERALL classification of information contained on that page; Remember, always conspicuously mark folders and files, on the outside front and back.

(4) The source document, the office of origin and the date of the source or classification guide.

(5) The "Derived From" (previously "Classified By") line must identify the original classification authority or source document; or state "Multiple Sources," and the derivative classifier shall keep a list of the sources with the file.

(6) The "Declassify On" line must state a specific date or event for declassification and is determined by the appropriate OCA.

(7) The "Date of Service" line will reflect the date of the latest source.

*[**NOTE**: In accordance with EO 12958, many current source documents and classification guides indicate the "OADR" as declassification instruction. Until guides are rewritten, the derivative classifier shall carry the fact that the source was marked as "OADR," and the date of the origin of the most recent source document, guide, or specific information being classified.]*

b. Documents created *before* 14 Oct 1995 will not be remarked. Documents created *after* 14 Oct 1995, and not marked in accordance with EO 12958, should be remarked, as stated above, as they are removed from files for working purposes. Care should be taken to ensure that documents sent to other activities or placed in official unit files are marked in accordance with the new EO

c. **Working Papers:** Most, if not all, classified documents originate as "WORKING PAPERS." Working papers are documents and materials accumulated or created in the preparation of finished documents and materials. ***After 90 days, all working papers containing classified information must be dated, marked, protected, accounted for, and destroyed in the same manner as a finished document with the same classification.***

8. Transporting and mailing classified information

a. TOP SECRET documents will not be mailed at any time. SECRET documents may be transported via U.S. Postal Service registered mail or may be hand delivered. The DA Form 3964, Classified Document Accountability Record, must be used and enclosed. Security managers will keep DA Form 3964 on file for 2 years. CONFIDENTIAL documents may be transported via any means approved for SECRET or by U. S. Postal Service First Class mail. The outside envelope must state "*Postmaster: Address Correction Requested. Do Not Forward.*"

b. For both levels, you must double wrap (in an opaque envelope or container), properly seal, and ensure the addressee and return address is typed on both envelopes. Only the inside envelope, both front and back, will be stamped with the highest level of classification of the contents within.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

c. Individuals hand-carrying classified material between buildings or bases within a 50-mile radius of your command must possess a DD Form 2501, *Courier Authorization Card and an Identification card* (DD Form 2 or 2A), and must have received a courier briefing. A locked briefcase may serve as the outside envelope when hand-carrying classified information. Do not store classified material in automobiles, luggage, hotel rooms, trailers, luggage racks, trunks, aircraft travel pods, or drop tanks. If material is to be transported beyond the 50-mile radius, the individual must also have courier orders, and the security manager must maintain a list of all classified material transported. ***Classified material shall be hand-carried ONLY as a last resort.***

d. Only solid opaque envelopes will be used. You **may not** use a shotgun envelope to hand-carry or transmit classified information.

9. Reproducing classified information

Classified information **may not** be reproduced without authorization from an official who has been designated to grant such approval. Avoid routine reproduction of classified information. Classified information that is reproduced is subject to the same controls as the original document. TOP SECRET information must not be reproduced without the consent of the originator or an even higher authority.

10. Destroying classified information

a. You must destroy classified material once its purpose has been served. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding (measuring 1/32"), wet-pulping, mutilation, chemical decomposition or pulverizing. The custodian and a witness will accomplish the destruction of TOP SECRET material. Both individuals will sign the DA Form 3964, Classified Document Accountability Record. When destruction of SECRET documents are witnessed by two cleared individuals, no destruction record is required. CONFIDENTIAL documents can be destroyed by the custodian alone - no destruction certificate is required.

b. USARC Regulation 380-2, chapter 6, establishes procedures for destruction and degaussing of magnetic media.

11. Classified meetings and briefings

Individuals responsible for conducting any classified meeting or briefing must ensure that:

a. The meeting site is appropriate and that it provides proper control, storage, and protection for classified.

b. An access roster is available, and checked, to limit access to properly cleared individuals.

c. The audience is notified of the overall classification.

d. Attendees handle, mark, and control classified notes.

e. Attendees receive assistance in preparing classified notes for mailing.

f. Approval is obtained for meetings with foreign national attendees.

g. Guard(s) shall be posted at doors restricting access and to prevent eavesdropping.

12. Emergency safeguarding of classified information

A local emergency plan will be posted on or near all security containers, and all individuals will be aware of the procedures to follow in an emergency.

13. Safe maintenance

a. Open security containers will NOT be left unattended.

b. Items having only monetary value, like cash, narcotics, weapons, airline tickets, etc., will not be stored in the same container as classified material.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

c. Be alert to signs of trouble, such as the dial being unusually loose, as well as any difficulty in dialing combinations or difficulty with drawers. Call a locksmith if any trouble signs appear.

d. Combinations must be changed anytime anyone having access to the safe combination leaves or no longer has access, and at least every 12 months. New combinations will be randomly selected. Do not use any set pattern, i.e. birth dates, anniversaries, etc. Memorize the combination; do not write numbers down. Be certain a qualified individual changes the security container combination.

14. End-of-day security procedures

a. A system of security checks at the close of each working day ensures that all classified information is secure. An SF 701, Activity Security Checklist, provides a systematic means to make a thorough end-of-day security inspection of a particular work area and shall be used to record such inspection. An integral part of the security inspection system is the security of all GSA-approved vaults and containers used for the storage of classified material. Use of the SF 701 ensures that all classified material is properly stored, waste baskets do not contain classified material, tops of desks are clear of classified material, and computer disks containing classified data are properly secured.

b. In addition, the check may serve to ensure windows and doors are closed and locked, coffee pots are unplugged and computers are turned off. The form is a checklist and any items your office wishes to have checked may be added. An SF 702, Security Container Check Sheet, that provides a record of the names, dates and times that persons have opened, closed and checked a particular container or vault, will be displayed on each security container. A safe can be indicated as opened and closed several times during a given date, but only needs to be checked, and the "Checked By" block initialed, at the end of each working day. Standard Forms 701 and 702 must always be annotated to reflect any after-hour, weekend, and holiday activity regardless of whether or not the security container was opened during that day.

15. Security violations and compromises

a. A *violation* is any unauthorized departure from established procedures for the protection of classified information. Not all violations result in compromise, but each incident must be investigated to determine whether a compromise did occur. A *disclosure* is the release or dissemination of information, either authorized or unauthorized, to a specific individual, group or activity. A *compromise* is a disclosure of classified information to unauthorized individuals that presents a threat to national security and can take several forms:

(1) Dissemination to unauthorized personnel.
(2) Loss of classified material.
(3) Automated information systems insecurities.
(4) Open, unattended security containers.

b. You must immediately report any actual or suspected violation, unauthorized disclosure, or compromise of classified information to your security manager. If any actual or probable disclosure, violation or compromise exists, a properly cleared individual, senior to all individuals known to be involved, will be appointed, in writing, to conduct a preliminary inquiry. USARC Regulation 380-2, para 7-7, establishes procedures for reporting automated information systems (AIS) security incidents, violations, and technical vulnerabilities.

16. Command, section, and unit security standing operating procedures (SOP)

You are required to read and follow local requirements as outlined within your respective command, section or unit security SOP.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

17. Telephone security

a. **Do not discuss classified information on non-secure telephones**. Official DOD telephones are subject to monitoring for communications security purposes at all times. The DOD telephones are provided for transmission of official government information only. Use of official DOD telephones constitutes consent to communications security telephone monitoring.

b. If you must discuss classified information on the telephone, a STU III is the only authorized method you may use. Additionally, a classified facsimile machine should be located in the Emergency Operations Center (EOC), at brigade level and above, for transmitting classified documents.

18. Foreign travel briefings

All U.S. Army personnel, both civilian and military, traveling OCONUS, either in official or unofficial capacity will receive an Anti-terrorism and Force Protection briefing from their security manager prior to travel. Additionally, DA highly recommends that family members traveling OCONUS receive a briefing as well.

19. SAEDA briefings

As an. Army employee, you must receive a Subversion and Espionage Directed Against the U.S. Army (SAEDA) briefing biennially. Your security manager will notify you when you are scheduled to receive the briefing.

20. Information systems security

Before you begin operating an automated information system (AIS), be sure you understand and comply with the security requirements of the system. If you have any questions, ask your Information Systems Security Officer (ISSO), or your Terminal Area Security Officer (TASO). You are responsible for procedural, data communications and physical security.

a. *Procedural security* dictates how you operate and maintain your system. You will:

(1) Ensure AIS equipment is operated in accordance with established procedures and system security requirements.

(2) Safeguard assigned user passwords and report compromised passwords to the ISSO or TASO.

(3) Protect an unattended terminal. Users should log off or turn off a classified computer before leaving it unattended.

(4) Ensure that no additional equipment is attached to an AIS without the knowledge and permission of your ISSO.

(5) Honor software copyright restriction. No unauthorized copies of copyrighted software may be made for office or personal use. Copyrighted software may not be removed from the work place.

(7) Do not load any software without permission of the USARC DCSIM.

(8) Always make backup copies of data files and be sure to update regularly.

(9) Keep food, drink, and electrical appliances away from AIS equipment.

(10) Never introduce diskettes or media onto a government system that are obtained outside the work arena, before having them checked for viruses.

(11) Immediately report any suspected computer misuse or abuse to your ISSO.

b. *Data security*. You must always protect classified and sensitive unclassified information. You will--

(1) Establish a need-to-know and periodically review access privileges for each sensitive file.

(2) Lock up classified removable media in a GSA approved security container.

(3) Do not attempt to access data on an AIS or computer network unless you have specifically been authorized such access.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

(4) Label diskettes with the classified and unclassified contents of the data stored on them and the name of the application program used. Handle diskettes carefully to avoid damage. Do not write on a diskette with pencil or pen. First write data on the label, and then attach the label to the diskette.

(5) Prominently mark removable media, diskettes and printer ribbons with the highest level of classification of information processed or contained on the diskette. The SF 707 (SECRET) and SF 708 (CONFIDENTIAL) should be used to label media. Mark all media that does not contain classified information with SF 710 (Unclassified) label, if it is stored, transmitted, or otherwise intermingled with classified media. Place downgrading and declassification instructions next to the classification marking.

(6) Prominently mark the container (sleeves, boxes, etc.) with the highest classification of information contained therein.

(7) Mark all classified computer generated data as you would any other classified document.

(8) Do not process information that exceeds the accreditation sensitivity level of the AIS.

(9) Do not allow unauthorized personnel to access the AIS or the data generated.

(10) Inspect data files for tampering. If you suspect tampering, immediately inform your TASO or ISSO.

(11) Dispose of classified media in such a manner as to preclude reconstruction, i.e., shredding.

c. *Communications Security* (COMSEC) policies apply to a networked AIS, that includes systems with dial-up-modem capability. All users, supervisors, and managers will ensure that:

(1) Their AIS has been accredited to transmit classified or sensitive information.

(2) All individuals log off and secure the removable classified disk when leaving a terminal.

d. *Physical security* limits access to your processing environment and provides security for your AIS.

(1) Recognize, politely challenge, and assist people who do not belong in your area.

(2) Know those who are authorized to use, service, and repair your systems.

(3) Restrict access to areas where classified information is being processed.

(4) Hardware must have an accountability chain back to the Property Book Officer.

(5) Challenge persons carrying AIS components out of an office or building.

(6) Do not allow any AIS hardware to be moved from its accredited location without the knowledge and approval of your ISSO.

(7) Purge and declassify any classified and sensitive data or applications that have resided on storage media prior to allowing the media to leave your office area. Diskettes WILL NOT be purged or downgraded. Consult your ISSO for destruction procedures.

e. *Software Copyright Violations* are punishable under U.S. Code Titles 17 and 18, that provide for civil and criminal penalties for copyright infringement. The civil penalties may include statutory damages up to $10,000. If infringement is proved willful, statutory damages can be as high as $50,000. Criminal penalties may include imprisonment for up to 1 year plus a $25,000 fine.

f. Telecommunications Security Monitoring. The DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for all lawful purposes.

Figure B-1. (continued) Security Briefing

(Continuation of Security Briefing)

21. Personnel security investigations

a. There are three basic types of personnel security investigations: National Agency Checks (NAC), National Agency Checks with Written Inquiries (NACI), and Single Scope Background Investigations (SSBI).

(1) The **NAC** is the investigative basis for a final SECRET clearance. A NAC is requested by submitting an SF 86, Questionnaire for National Security Positions, and a fingerprint card (FD 258 untitled), to Defense Investigative Service (DIS).

(2) An **NACI**, (a NAC with written inquiries), is a suitability investigation required by the Office of Personnel Management (OPM) as a condition for civilian federal employment and is conducted by OPM. The favorably completed NACI is a condition for appointment to nonsensitive and noncritical sensitive positions. A NACI meets the requirements for granting a SECRET clearance. A NACI also requires submission of an SF 86.

(3) An **SSBI** is required for a TOP SECRET clearance and for access to Sensitive Compartmented Information (SCI). An SSBI is requested by submitting a DD Form 1879, Request for Investigation; an SF 86, Request for Personnel Security Investigation, and an FD 258 to DIS. An SSBI consists of all the checks done for a NAC, a subject interview and interviews with information sources. A favorably completed SSBI is a condition for appointment to a critical sensitive position.

b. A *Periodic Reinvestigation (PR)* is for the purpose of reviewing a person's character, morals, maturity, and life-style to ensure that nothing has occurred to affect that person's continued eligibility for a security clearance since their previous investigation. Central Clearance Facility (CCF) will make a determination when a PR is required. Your security manager will notify you if one has been requested by CCF.

c. After the appropriate investigation and adjudication, a DA Form 873, Security Clearance Determination, will be issued by CCF and forwarded to your official personnel folder (OPF) or the Military Personnel Records Jacket (MPRJ) by your security manager. At no time should the DA Form 873 be maintained outside the MPRJ or the OPF. Additionally, you should never maintain a copy of your DA Form 873. The DA Form 873 is not permitted to be used as an access roster. If there is a need to verify your security clearance, your security manager shall do so.

22. Reporting derogatory information

As a DOD employee, it is your responsibility to report to your security manager, all derogatory information of any individuals who possess a security clearance, regardless of rank or grade, as soon as you become aware of that information.

23. Debriefing and outprocessing requirement

You will receive an exit debriefing prior to resignation or retirement from military or civilian service. Ensure out-processing is completed with your respective security managers prior to any transfer, retirement, or resignation.

24. Administrative sanctions and reporting requirements

As a DOD military or civilian employee, you are subject to administrative sanctions. By failing to follow these rules and precautions, you expose yourself to serious penalties if classified information is disclosed or compromised. Such penalties include, but are not limited to, a warning notice, reprimand, termination of classification authority, suspension without pay, removal or discharge, fine and imprisonment.

Figure B-1. (continued) Security Briefing

Appendix C
Classified Information Nondisclosure Agreement (SF 312) Guidance

C-1. Policy

a. All Federal employees requiring access to classified information must sign an SF 312 (NDA). The employee's signature on the NDA shows an agreement to never to disclose classified information to any unauthorized person(s). Refusal to sign is grounds for withdrawal of security clearance and access. The NDA is designed so a new non-disclosure agreement does not need to be signed upon changing jobs. In order to preclude duplicate NDAs, make a reasonable effort to verify if an existing NDA is on record. However, if location and retrieval of a previously signed agreement is impossible, completion of a new NDA is necessary.

b. All personnel who have a security clearance must have a copy of a signed NDA on file with their respective security manager. The security manager will reproduce the original and file the copy until the individual transfers or separates from government service. When a person transfers, it must go to their new command. When a person leaves or retires from government service, it goes to the respective personnel records section for retention in their official personnel file for 50 years from the date of execution.

C-2. Execution

a. ***Witness and Acceptance Blocks:*** The security manager or another individual may witness the NDA by signing the witness block. The security manager will sign the acceptance block of the file copy **only** and retain that copy. For military personnel, leave the acceptance line blank on the original form for completion by records personnel who maintain the MPRJ.

b. ***Debriefing Section:*** Upon retirement, ETS, or resignation from federal employment, this section of the SF 312 may serve as a debriefing statement.

C-3. Retention

Retention of the SF 312 (NDA) is as follows:

a. Civilians. The original NDA for civilians is filed in their Official Personnel File (OPF).

b. Military. The original NDA for military personnel is filed in their official Military Personnel Records Jacket (MPRJ), 201 file, as an adjunct to the DA Form 873.

(1) Active Guard Reserve soldiers' MPRJs are at AR-PERSCOM, St. Louis, MO.

(2) TPU soldiers' MPRJs are at their respective unit.

(3) Active Army officers' MPRJs are at U.S. Total Army Personnel Command, Alexandria, VA.

(4) Active Army enlisted MPRJs are at Army Enlisted Records and Evaluation Center, Fort Benjamin Harrison, IN.

c. The security manager will retain a file copy of the NDA until the individual transfers or separates from service.

C-4. Transfer, separation, and retirement

Upon transfer, mail the copy of the NDA to the gaining organization's security manager. Upon separation, either DA Form 2962 (Security Termination Statement) or the Security Debriefing Acknowledgement portion on the file copy of the SF 312 may serve as acknowledgement of the debriefing. The NDA debriefing is valid since the debriefing itself will have an original signature. If using DA Form 2962 for the debriefing, the copy of the NDA can be destroyed. Retain either the DA Form 2962 or the SF 312 debriefing form in the security office files for 2 years from the date of execution.

Appendix D
Courier Documentation and Briefings

[All USAR security managers will comply with instructions and requirements in this appendix.]

Section I
CONUS and OCONUS Courier Requirements

D-1. Briefing for couriers authorized to hand-carry and escort classified material

a. Have individuals read the courier briefing. A sample CONUS courier briefing is at figure D-1. A sample OCONUS courier briefing is at figure D-2.

b. Ask if they understand or have any questions.

D-2. USARC Form 90-R (USARC Courier Briefing Acknowledgement)

a. The USARC Form 90-R records couriers' receipt of briefings and serves as their acknowledgement of associated responsibilities.

b. Instructions for completion.

(1) Enter the DD Form 2501 Serial Number - *Print pre-serialized number from card.*

(2) Expiration Date - 1 *year minus 1 date from issue date.*

(3) Designated Courier - *Courier's signature.*

(4) Date - *Date signed by courier.*

(5) Security Manager - *Security manager or Alternate's signature.*

D-3. CONUS- and OCONUS-specific requirements

a. CONUS-specific requirements (see sec II).

b. OCONUS-specific requirements (see sec III).

Section II
CONUS-Specific Courier Requirements

[These requirements are in addition to those stated in section I above.]

D-4. DD Form 2501 (Courier Authorization Card)

Issue and control DD Form 2501 to authorized couriers ***(see para 6-3)***. Each card has a pre-printed serial number. Cards are an accountable item and must be safeguarded.

a. Instructions for completing DD Form 2501 are as follows: *[**Type** all data.]*

(1) Block 1. Issue date - S*elf-explanatory.*

(2) Block 2. Expiration date - *1 year from Issue Date minus 1 day.*

(3) Block 3. Name - S*elf-explanatory.*

(4) Block 4. Rank or Grade - S*elf-explanatory.*

(5) Block 5. Social Security Number (SSN) - S*elf-explanatory.*

(6) Block 6. Authorized Level – *Type only the level of clearance authorized for individual.*

(7) Block 7. Geographical Limit(s) - *Type "50-mile radius" (If necessary to grant approval over 50 miles, the individual must be on courier orders **(see app D, sec III)** for each trip.*

(8) Block 8. Signature of Courier - *Self-explanatory.* (Security manager must witness signature.)

(9) Block 9. Your unit office symbol and address.

(10) Block 10.

(a) Duty Phone Number - *Your number.*

(b) After Hours Phone Number - Your after hours number.

(11) Block 11.

(a) Name - *Security Manager or Alternate Security Manager's name.*

(b) Title - *Security Manager or Alternate Security Manager.*

(c) Signature - *Security Manager or Alternate Security Manager's signature.*

b. After typing the data, sign block 11c. Issue the card to the courier after witnessing the individual's signature in block 8.

D-5. Courier Authorization Card (DD Form 2501) Receipt Log

Because the card is an accountable item, the courier must sign for receipt of the card. Develop and implement a Courier Authorization Card (DD Form 2501) Receipt Log. Use any format, but it must contain the card number, unit name, courier's full name, courier's signature, issuer's signature (security manager), date issued, and date destroyed. Recommend preprinting the serialized numbers on the log upon receipt of the accountable cards. Retain this log for 2 years following the last entry.

D-6. Courier orders

Use the Courier Authorization memorandum to carry materials beyond a 50-mile radius of a command within CONUS. Individuals will still need to carry the DD Forms 2501 on their person. Carrying materials round trip requires an authorization memorandum for each way. ***(See sample memorandum at fig D-3)***.

Section III
OCONUS-Specific Courier Requirements

[These requirements are in addition to those stated in section I above.]

D-7. Travel Orders (DD Form 1610)

Submit as stated in this regulation, paragraph 6-4.

D-8. USARC Form 81-R (USARC OCONUS Handcarry Classified Information Request)

Submit as stated in this regulation, paragraph 6-4. Completion of all items is self explanatory.

D-9. OCONUS courier orders memorandum

The USARC DCSINT issues OCONUS Courier Orders memorandums for justified courier requests.

D-10. USARC Form 91-R (Foreign Travel Briefing Statement)

Completion of all items is self explanatory.

Sample *CONUS* Briefing
for Couriers Authorized to Hand-carry and Escort Classified Materials

General Instructions. As a designated courier of classified material, you are authorized to hand-carry or escort material while in a travel status between your duty and TDY stations. If traveling beyond a 50-mile radius of your command, you must also have a memorandum from your security manager authorizing you to hand-carry classified information in your possession. In some situations you may not have actual access or specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become, as defined in AR 380-5, the custodian of that information.

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

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

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

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

Preparation. Whenever you transport classified information, it must be enclosed in two opaque sealed envelopes, similar wrappings, or two opaque sealed containers such as boxes or other heavy wrappings without metal bindings. A **locked** briefcase, when used, may serve as an outer wrapping or container. The inner envelope or container shall be addressed to an official government activity (as if for mailing), stamped with the highest classification and placed inside the second envelope or container. The outer covering will be sealed and addressed for mailing (in the event of an emergency) to the government activity. Proper preparation is the responsibility of the activity authorizing transmission. **Do not accept improperly prepared material for transmission**. Receipts will be exchanged when and if required.

Figure D-1. Sample CONUS Courier Briefing

(Continuation of CONUS Couier Briefing)

Hand-carrying Classified Information Aboard an Aircraft. The written authorization memo and your DD Form 2501, Courier Authorization Card, should ordinarily permit you to pass through passenger control points within the U.S. without the need for subjecting classified material to inspection. Except for customs inspection only, airports have established screening points to inspect all hand-carried items. If you are carrying classified material in envelopes you should process through the ticketing and boarding procedures in the same manner as other passengers. When the sealed envelopes are carried in a briefcase (carry-on-luggage), it shall be routinely offered for inspection for weapons. The screening official may check the envelope by X-ray machine, flexing, feel, weight, etc., without opening the envelope. If the screening official is not satisfied with your identification, authorization statement, or envelope, you will not be permitted to board the aircraft and are no longer subject to further screening for boarding purposes. Do not permit the screening official to open envelopes or read any portion of the classified document as a condition for boarding. ***Do not, under any circumstances, read or work on classified materials while onboard the aircraft.***

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

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

Conclusion. **Our primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise**. Security regulations cannot guarantee the protection of classified information nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information. You are reminded that any classified instructions you receive must also be protected. Do not discuss verbal instructions with anyone after you have delivered the material, do not talk about where you were, what you did, or what you saw.

If you have questions at any time concerning the security and protection of classified and sensitive material entrusted to you, contact your security manager, or the USARC Command Security Manager.

Figure D-1. (continued) Sample CONUS Courier Briefing

Sample *OCONUS* Briefing
for Couriers Authorized to Hand-carry and Escort Classified Materials

Travelers who are authorized to carry classified material on international flights or by surface conveyance if crossing international borders must have courier orders and receive an OCONUS courier briefing. Courier Card, DD Form 2501, is not valid for overseas travel. A memorandum signed by the USARC Command Security Manager or the USARC DCSINT on USARC letterhead is required and shall, as a minimum, provide the information specified below. Travelers will be informed of and shall acknowledge their security responsibilities by signing a USARC Courier Certificate.

You are liable and responsible for the material being escorted. Throughout the journey, the classified material shall stay in your personal possession, except when it is in authorized storage. The material will not be opened enroute except in the circumstances described below. The classified material is not to be discussed or disclosed in any public place. The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies, or cleared contractor facilities must be used. Classified material may not be stored in hotel safes, personal residences, or any other unauthorized storage facility.

Do not deviate from the authorized travel schedule, unless such deviation is beyond your control (such as cancellation of a flight). In an emergency, you shall take measures to protect the classified material. You are responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents, etc.) are complete, valid, and current.

There is no assurance of immunity from search by the customs, police, and immigration officials of the various countries whose border you will be crossing; therefore, should such officials inquire into the contents of the consignment, you shall present the courier orders and ask to speak to the senior customs, police, or immigration official; this action should normally suffice to pass the material through unopened. However, if the senior customs, police, or immigration official demands to see the actual contents of the package, it may be opened in the presence of that individual, but should be done in an area out of sight of the general public. Precautions should be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other items. Ask the official to repack or assist in repacking the material immediately after the examination. The senior customs, police or immigration official should be requested to sign the shipping documents (if any) or courier certificate that the package has been opened. If the package has been opened under such circumstances, inform in writing the addressee and the dispatching security manager of this fact.

Inventory the classified material to be carried. A copy of the inventory will be retained by your security office and a copy carried by you. Travel orders will identify you by name, title, and organization, and include your passport or identification number. Travel orders will describe the route you are taking (your itinerary may be attached for this purpose; describe the package to be carried (size, weight, and configuration); reflect a date of issue and expiration date; and contain the name, title, and telephone number of an appropriate official within your command who may be contacted to verify the authorization to escort classified material.

Figure D-2. Sample OCONUS Courier Briefing

(Continuation of OCONUS Couier Briefing)

Courier orders shall contain this same information, in addition to a complete description of the material that is to be carried and expiration of authorization to carry the material. Where possible, your courier authorization should show the phone number of the U.S. embassy or consulate closest to the area that you will enter to the country, in case the assistance of the U.S. State Department is needed in clearing customs. As an alternative, the courier orders should show the name and phone number of a point of contact at the activity located in the foreign country that is to be visited. Courier orders will be signed by the USARC Command Security Manager or the USARC DCSINT.

Return all classified material in a sealed package or produce a receipt signed by the security officer of the addressee's organization for any material that is not returned. For guidance on hand-carrying NATO classified material, see AR 380-15. You must coordinate with the appropriate authorities when hand-carrying or escorting classified material on board a commercial aircraft. Adherence to the following is of special importance when the material being hand-carried is other than documentation that might initiate airport screening and access if arrangements were not made in advance:

+ Advance coordination should be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of AR 380-5 and the Federal Aviation Administration (FAA) guidance. During this coordination, the specific requirements for documents should be agreed to. Local FAA field offices can often be of assistance.

+ Be in possession of a DOD identification card that includes your signature. You should have enough copies of travel orders so that one copy can be provided to each airline involved. Copies of your courier order should be on hand and provided if requested.

+ Process through the airline ticketing and boarding procedure the same as other passengers. The package or the carry-on luggage containing classified material should be routinely offered for inspection.

Figure D-2. (continued) Sample OCONUS Courier Briefing

Sample Courier Order Memorandum
Carrying Classified Beyond a 50-Mile Radius

[Note: Carrying Classified will only be done when there is absolutely no possibility of sending via registered mail, including FEDEX). If materials are to be carried round trip, a memorandum for each way is necessary.]

(Use Local Letterhead)

(Your Office Symbol) (Date)

TO WHOM IT MAY CONCERN

SUBJECT: Courier Designation

1. In accordance with AR 380-5, Department of the Army Information Security Program Regulation, _____ *(courier's name and SSN)*, who is employed or is an employee of the above organization, is on official business and designated as a courier to hand-carry classified material in conjunction with travel indicated below. Material is double wrapped in sealed brown paper and is addressed to: Commander, *(command's address)*.

a. Departure point:

b. Departure date:

c. Destination(s):

d. Known transfer point(s): *(any known intermediate stops)*

e. Issue date:

2. A listing of the transported material is on file at the above address.

3. There is neither time nor alternate means of transmission available to send the material referred to herein that would provide for timely accomplishment, of operational objectives. This letter may be confirmed by calling: *(security managers telephone number)*.

4. This letter of authorization expires (1 day after date of final destination).

(Security Manager's
Signature Block)

Figure D-3. Sample CONUS Courier Memorandum

Appendix E
Sample Plan for Emergency Safeguarding of Classified Material

This plan addresses actions to be taken by ____(Unit)_____ to safeguard classified material from the threat of loss or compromise due to natural disaster, civil disturbance, or enemy action.

a. **When circumstances <u>permit</u> securing classified material**:

(1) Place all classified material into the nearest GSA-approved container, lock the container, and vacate the building or seek shelter as indicated in paragraph c. below.

(2) The senior representative present and the security manager will ensure all safes within the command are locked prior to vacating the building.

b. **When circumstances <u>do not permit</u> securing classified material**:

(1) Hand-carry all classified material in the work area as when vacating the building or seeking shelter.

(2) Upon reaching the assembly point, all personnel hand-carrying classified material will notify the security manager or senior representative present. The security manager or the senior representative should take charge of the classified material or, at a minimum, provide the individual with instructions on protecting the material.

(3) In the event of an urgent evacuation of the building, it may be necessary to leave classified material unsecured in the building. The individual leaving the unsecured classified material will advise the security manager or the senior representative present as soon as possible after exiting the building and reaching safety. The security manager or senior representative will then advise the USARC Command Security Manager or the USARC DCSINT of all classified material that was not secured.

c. **If the threat is caused by**:

(1) Fire, or natural disaster: Proceed to _____(location)_____.

(2) Bomb threat or explosion: Proceed to _____(location)_____.

(3) Civil disturbance, terrorist attack, or enemy action: Remain in the building and await further instructions.

d. Employees will acquaint themselves with this plan, periodically review it, and execute it when conditions warrant.

Appendix F
Classified Conference and Meeting Guidance

F-1. Security managers must maintain maximum security awareness concerning classified presentations, materials and handouts during classified briefings and meetings. Project Officer responsibilities include--

a. Ensuring the host prepares a roster of authorized attendees and that the host verifies all personnel, including TDY visitors, possess the appropriate security clearance for the level of material being presented in the briefing or meeting.

b. Visually scanning the room to detect obvious listening devices or recording devices. Disconnect all telephones in the room.

c. Posting a hallway sign indicating "Classified Briefing In Progress - DO NOT ENTER."

d. Ensuring properly cleared person(s) are physically located to observe all doors. If unable to observe any particular doors, lock and mark them with "NO ENTRY" signs. Observers will ensure no loitering outside the conference room and will periodically check all areas surrounding the room to ensure there is no loitering nearby.

e. Use the project officer's checklist located in FORSCOM Supplement 1 to AR 380-5, appendix T.

f. Ensuring all handouts, notes, minutes or records of classified briefings and meetings are correctly marked, safeguarded, and distributed.

g. Conduct classified meetings and briefings in accordance with provisions of AR 380-5 and FORSCOM Supplement 1.

F-2. Adherence to the above-mentioned security measures is essential in maintaining a high level of security awareness and integrity in the dissemination and safeguarding of classified materials. Anyone planning a classified briefing or meeting, should contact their security manager.

Appendix G
Samples of Classified Markings

MARKING A CLASSIFIED DOCUMENT DERIVATIVELY CLASSIFIED FROM INFORMATION IN AN OLD DOCUMENT:

+ Derived from: HQDA Memo, 10 Feb 94, Subj: "Security is a Force Multiplier"
+ Declassify on: Source marked OADR
+ Date of Source: 10 Feb 94

(Memo derivatively classified based solely on information classified under old system and was marked "Declassify on OADR")

MARKING A CLASSIFIED DOCUMENT DERIVATIVELY CLASSIFIED FROM A SOURCE CLASSIFIED UNDER OLD SYSTEM AND A SOURCE CLASSIFIED UNDER CURRENT SYSTEM:

+ Derived from: Multiple Sources
+ Declassify on: Sources Marked X3 and OADR
+ Date of Source: 24 May 96

(X3 is new system and requires classification beyond 10 years. Date of source is the most recent source.)

MARKING A CLASSIFIED DOCUMENT DERIVATIVELY CLASSIFIED FROM ONE SOURCE CLASSIFIED UNDER THE CURRENT SYSTEM:

+ Derived from: Oxnard Missile (biennially-1) Classified Guide, dtd 10 Dec 96
+ Declassify on: Source marked X3
+ Date of Source: 21 Aug 96

(Memo is classified because it concerns a system that has a security classification guide reflecting the new system of classifying.)

MARKING A CLASSIFIED DOCUMENT DERIVATIVELY CLASSIFIED FROM MULTIPLE SOURCES WHERE ALL SOURCES ARE CLASSIFIED UNDER THE CURRENT SYSTEM:

+ Derived from: Multiple Sources
+ Declassify on: Sources marked X3 and 4
+ Date of Source: 10 Dec 96

(Memo is derivatively classified based on data from several subjects covered by different security classification guides. Date of Source line is always most recent date of all sources used.)

MARKING AN ORIGINALLY CLASSIFIED DOCUMENT:

+ Classified by: LTG A. Secret, Chief of Intelligence Programs, Army Security is Important Command
+ Reason: 1.5(c)
+ Declassify on: X1

(The OCA, who has been delegated original classification authority for a particular intelligence program is identified, the reason the information is classified is stated, and the exemption category for declassification is indicated.)

MARKING A CLASSIFIED DOCUMENT THAT CONTAINS INFORMATION ORIGINALLY CLASSIFIED AND INFORMATION DERIVATIVELY CLASSIFIED FROM SOURCE DOCUMENT:

+ Derived from: Multiple Sources
+ Declassify on: Source marked X3, 6
+ Date of Source: 21 Aug 96

(One OCA has generated a document that has information that was originally classified on 21 Aug 96 and also contains information from a source document dated 11 Nov 96 and also contains information from a source document dated 11 Nov 95 by another OCA, therefore it is considered a derivatively classified document. The declassification date is the most restrictive date or event (one that occurs farthest in the future (X3, 6 - information cannot be declassified within 10 years or an indefinite declassification date)). The date of the source is always the date of the most recent source used.)

Glossary

Section I
Abbreviations

AGR.....Army Guard Reserve
AIS .....automated information system(s)
C .....CONFIDENTIAL
CFP.....concept formulation package
COMSEC....communications security
CONUS.....continetal United States
CPRs.....Civilian Personnel Regulations
DA .....Department of the Army
DCS .....Defense Courier Service
DCSINT.....Deputy Chief of Staff for Intelligence
DISA.....Defense Information Systems Agency
DOD .....Department of Defense
EO .....Executive Order
FORSCOM..U.S. Army Forces Command
FOUO .....For Official Use Only
FSP .....Force Support Package
GSA.....General Services Administration
INSCOM.....Intelligence and Security Command
ISS .....information systems security
MARKS .....The Modern Army Record Keeping System
MPRJ .....Military Personnel Records Jacket
MSC.....Major Subordinate Command
NATO.....North Atlantic Treaty Organization
NDA .....Nondisclosure Agreement
NOFORN....Not Releasable to Foreign Nationals
NSA.....National Security Agency
OADR.....Originating Agency's Determination Required
OCA.....Original Classification Authority
OCONUS....Outside the Continental United States
ODCSINT...Office of the Deputy Chief of Staff, Intelligence
OPF.....Official Personnel File
S .....SECRET
SAEDA.....Subversion and Espionage Directed Against the U.S. Army
SAP.....Special Access Program
SCI.....Sensitive Compartmented Information
SF .....Standard Form
SOP.....standing operating procedures
SSO.....Special Security Officer
STU-III .....Secure Telephone Unit, Third Generation
TDY.....temporary duty
TPU.....troop program unit
TS .....TOP SECRET
UCMJ.....Uniform Code of Military Justice
USAR.....U.S. Army Reserve
USARC .....United States Army Reserve Command
USC .....United States Code
USR .....Unit Status Report

Section II
Terms

Access
The ability and opportunity to obtain knowledge of classified information.

Agency
A unit or organization that has primary responsibility for performing duties or functions as representative of, and within the assigned authority of, its higher headquarters. Within the Department of Defense (DOD), this term includes Department of the Army.

Applicable associated markings
Markings, other than those designating classification level, that are required on classified documents. The associated markings include the "classified by" line, downgrading and declassification instructions, special warning notices, Special Access Program caveats, etc.

Automatic declassification
The declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under EO 12958.

Classification
The act or process that determines if information is to be classified.

Classification guidance
Any instruction or source that prescribes the classification of specific information.

Classification guide
A documentary form of classification guidance issued by an original classification authority. It identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified National Security Information (or "classified information")
Information that has been determined (pursuant to EO 12958 or any predecessor order) to require protection against unauthorized disclosure. It is marked to indicate its classified status when in documentary form.

Classifier
An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

Code word
A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher.

Command
Headquarters, Department of the Army (HQDA) to include the Office of Secretary of the Army and the Army Staff, Major Commands (MACOMs), Major subordinate commands and other organizations formed within the Army to support HQDA or a MACOM.

Communications security (COMSEC)
The protection resulting from all measures designed to deny unauthorized persons information of value *that* might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

Compromise
An unauthorized disclosure of classified information.

Confidential source
Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security, with the expectation that the information or relationship, or both, are to be held in confidence.

Continental United States (CONUS)
The 48 contiguous states in the United States territory, including territorial waters, within the North American continent, between Canada and Mexico.

Counterintelligence
Those activities *that* are concerned with identifying and counteracting foreign intelligence activities, organizations, or individuals engaged in espionage, subversion, or terrorism, or other inimical activity posing a threat to the US Army, its technology or industrial base.

Controlled cryptographic item (CCI)
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified by controlled (Equipment and components so designated bear the designator "Controlled Cryptographic Item" or "CCI.)

DOD component
The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified Combatant Commands, and the Defense Agencies.

Downgrading
A determination that information classified at a specific level shall be classified at a lower level.

Event
An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

Foreign government information
(1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.
(2) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.
(3) Information received and treated as "Foreign Government Information" under the terms of a predecessor order to EO 12958.

Formerly Restricted Data
Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

Information
Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, (proponent), to regulate access to the information.

Information security
The system of policies, procedures, and requirements established under the authority of Executive Order 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Mandatory declassification review
Review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of EO 12958.

Multiple sources
Two or more source documents, classification guides, or a combination of both.

National security
The national defense or foreign relations of the United States.

Need-to-know
A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Network
A system of two or more computers that can exchange data or information.

Nickname
A nickname is a combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

Original classification
An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original classification authority
An individual authorized in writing, either by the President, Secretary of the Army or DCSINT to originally classify information to a prescribed level.

Regrade
To raise or lower the classification assigned to an item of information.

Restricted Data
All data concerning (a) design, manufacture or utilization of atomic weapons; (b) the production of special nuclear material; or (c) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under Section 142 of the Atomic Energy Act of 1954, as amended.

Safeguarding
Measures and controls that are prescribed to protect classified information.

Security clearance
A determination that a person is eligible under the standards of DOD 5200.2-R for access to classified information.

Self-inspection
The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under EO 12958 and its implementing directives.

Senior Agency Official or Senior Official
An official appointed in writing by the head of an agency under the provisions of Section 5.6(c) of EO 12958 to be responsible for direction and administration of the Information Security Program. Within the Department of the Army, the Secretary of the Army has appointed the HQDA Deputy Chief of Staff for Intelligence (DCSINT) as the Senior Agency Official.

Sensitive Compartmented Information
Classified information concerning, or derived from, intelligence sources, methods, or analytical processes, and that is required to be handled within formal access control systems established by the Director of Central Intelligence.

Systematic classification review
The review process for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

Telecommunications
The preparation, transmission, or communication of information by electronic means.

Unauthorized disclosure
A communication or physical transfer of classified information to an unauthorized recipient.

Upgrade
To raise the classification of an item of information from one level to a higher one.

Violation
(1) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.
(2) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 12958 or its implementing directives.
(3) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 12958.