

Effective 1 May 2005

Security

Information Security Procedures

For the Commander:

JAMES M. PALERMO
Colonel, General Staff
Chief of Staff

Official:

BRUCE W. MORRIS
Assistant Chief of Staff, G-6

History. This UPDATE printing publishes a revised memorandum which is effective 1 May 2005.

Summary. This memorandum establishes policy and procedures which comply with the

requirements of AR 380-5.

Applicability. This memorandum is applicable to all personnel assigned, attached, or supported by Headquarters, United States Army Recruiting Command.

Proponent and exception authority. The proponent of this memorandum is the Assistant Chief of Staff, G-3. The proponent has the authority to approve exceptions to this memorandum that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of GS-13.

Army management control process. This memorandum contains management control procedures in accordance with AR 11-2 but does not identify key management controls that must be evaluated.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USAREC, ATTN: RCRO-SEC, 1307 3rd Avenue, Fort Knox, KY 40121-2726.

Distribution. This memorandum is published in electronic media only and can be found on the Command Enterprise Portal.

Contents (Listed by paragraph number)

Chapter 1

General

- Purpose ● 1-1
- References ● 1-2
- Explanation of abbreviations ● 1-3
- Responsibilities and duties ● 1-4
- Recordkeeping ● 1-5

Chapter 2

Classification

- General ● 2-1
- Original classification authority ● 2-2
- Derivative classification authority ● 2-3

Chapter 3

Controlled Unclassified Information

- General ● 3-1
- Release authorities ● 3-2
- Education ● 3-3
- Markings ● 3-4
- Access to FOUO information ● 3-5
- Safeguarding ● 3-6
- Disposal ● 3-7

Chapter 4

Classified Information

- Access ● 4-1
- SF 312 ● 4-2
- Custodial procedures ● 4-3
- Mail screening procedures ● 4-4
- Removal of classified material from HQ USAREC buildings ● 4-5
- Telephone security ● 4-6
- End-of-day security checks ● 4-7
- Emergency planning ● 4-8
- Visitors ● 4-9

- Classified presentations and meetings ● 4-10
- Reproduction of classified material ● 4-11
- Security containers ● 4-12
- Transmission of classified information ● 4-13
- Hand-carrying classified information ● 4-14
- Violations or compromises ● 4-15

Appendix A. References

Glossary

Chapter 1

General

1-1. Purpose

This memorandum establishes policy and procedures which comply with the requirements of AR 380-5.

1-2. References

For required and related publications and referenced blank forms see appendix A.

1-3. Explanation of abbreviations

Abbreviations used in this memorandum are explained in the glossary.

1-4. Responsibilities and duties

a. The Headquarters, United States Army Recruiting Command (HQ USAREC) security officer. Designated as the HQ USAREC security manager (SM) and is responsible for establishing an effective Information Security Program for HQ USAREC. This includes establishing local information security policies and procedures; initiating and supervising measures or instructions necessary to ensure continued protection of classified information; assuring that

HQ USAREC personnel requiring access to classified information are properly cleared and continually assessing the individual trustworthiness of personnel who possess a security clearance. The HQ USAREC SM is the commander's authorized representative for Department of the Army security programs. The duties and responsibilities of the SM are:

(1) Advise and represent the commander on matters related to the Information Security Program.

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

(3) Establish procedures of assuring that all persons in HQ USAREC granted access to classified material are properly cleared and have received required security briefings.

(4) Advise and assist all HQ USAREC personnel regarding the classification of material.

(5) Conduct annual reviews of classified holdings for proper marking, downgrading, declassification, or destruction.

(6) Supervise and conduct security inspections and spot checks for all HQ USAREC activities.

(7) Be the single point of contact on security matters for HQ USAREC activities.

(8) Establish effective and comprehensive standing operating procedures for HQ USAREC.

(9) Provide policy, advice, and assistance to commanders, supervisors, and appointed SMs at directorate, recruiting brigade, and recruiting battalion levels throughout the United States Army Recruiting Command (USAREC).

(10) Publish a HQ USAREC Security and Access Roster for each directorate and/or activity supported.

*This memorandum supersedes USAREC Memorandum 380-3, 16 February 2000.

b. Directorate and staff activity SMs. Each directorate and separate staff activity shall appoint, in writing, a SM for their activity. The appointed SM is responsible for the administration of security programs within their activity and serve as a central point of contact with the HQ USAREC SM. The directorate and staff activity SM will:

(1) Ensure that all personnel assigned to their activity have received required security briefing from the HQ USAREC Security Division and that each individual inprocess and outprocess through the HQ USAREC Security Division.

(2) Ensure that classified material and official mail is protected and safeguarded and that classified material is destroyed according to AR 380-5 and this memorandum.

(3) Be the single point of contact on security matters for their activity as described in this memorandum. Coordinate actions with the HQ USAREC Security Division as required.

(4) Ensure that personnel having access to classified material or are designated to open official mail have been properly briefed by the HQ USAREC Security Division.

(5) Maintain and update their activity's extract of the HQ USAREC Security and Access Roster as provided by the HQ USAREC Security Division.

(6) Immediately notify the HQ USAREC Security Division when specific requirements exist for certifications of security clearance or investigative information for any travel, training, temporary duty, visits, or change in an individual's requirement for access to classified information.

(7) Report all security violations to the HQ USAREC Security Division.

c. Supervisors. Supervisory personnel have a key role in the effective implementation of the HQ USAREC Information Security Program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information related to national security. The supervisor will:

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

(2) Ensure subordinate personnel attend training, or are temporary duty understand, and follow the requirements of this memorandum and AR 380-5, as well as all other command policies and procedures concerning information security programs.

(3) Continually assess the eligibility for access to classified and sensitive information of subordinate personnel and report to the HQ USAREC SM any information that may have a bearing on that eligibility.

(4) Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information consistent with established security programs.

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

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

1-5. Recordkeeping

The HQ USAREC SM and directorate and special activity SMs will maintain written records of all actions related to security in the office files.

Chapter 2 Classification

2-1. General

The authority to classify a document, extract, or material comes from two sources as outlined in AR 380-5:

- a. Original authority, or
- b. Derivative authority.

2-2. Original classification authority

There are three levels of original classification authority (AR 380-5).

a. TOP SECRET (TS). No one at USAREC has original classification authority for TS material as described by AR 380-5.

b. SECRET. No one at USAREC has original classification authority for secret material as described by AR 380-5.

c. CONFIDENTIAL. No one at USAREC has original classification authority for confidential material as described by AR 380-5.

2-3. Derivative classification authority

This authority is gained when extracting classified information from a document (or several documents), following a classification guide, a directive, or regulation (AR 380-5). Procedures outlined in AR 380-5 will be followed for application of classification, markings, declassification, regrading, and destruction of classified materials.

Chapter 3 Controlled Unclassified Information

3-1. General

While not classified, controlled unclassified information (CUI) protection is a must. Of all the different types of information that require pro-

tection, CUI is the least recognizable and is also a high payoff target for individuals and organizations to gain unauthorized disclosure. On a daily basis, HQ USAREC and supported activities handle a tremendous amount of CUI, particularly For Official Use Only (FOUO), sensitive information (Computer Security Act of 1987), and technical documents. A great percentage of CUI handlers are not aware of proper handling and protection requirements. Producers of compiled information must maintain a list of all sources, and provide this list, on demand to the disclosure officer or the Freedom of Information Act (FOIA) Office.

3-2. Release authorities

In this command, there are only two offices authorized to release CUI to non-DOD entities:

a. The FOIA and Privacy Act Section of Administrative Services Branch of Headquarters, United States Army Accessions Command.

b. The appointed command disclosure officer.

3-3. Education

Directors, supervisors, and directorate and special activity SMs must aggressively educate all members of their command on:

- a. What is CUI.
- b. Where it exists in their command.
- c. Proper handling procedures. (AR 25-55, AR 380-5, AR 380-10, AR 25-2, and local regulations and procedures.)

3-4. Markings

a. An unclassified document containing FOUO information should be marked "FOR OFFICIAL USE ONLY" in bold letters at least 3/16 of an inch high at the bottom on the outside of the front cover (if any), on the first page, on the back page, and on the outside of the back cover (if any). FOUO will not be abbreviated for marking purposes - it must be entirely spelled out.

b. Additional marking instructions are contained in AR 380-5.

3-5. Access to FOUO information

a. FOUO information may be disseminated within DOD components and between officials of DOD components, etc., to conduct official business. Recipients shall be made aware that the material contains FOUO information. DA Label 87 (For Official Use Only Cover Sheet) will be attached to the top of the document when removed from file containers (i.e., file cabinets or desks) or the document will be covered with nonsensitive papers in such a manner as to prevent unauthorized access to the information.

b. FOUO information will be transported in such a manner that precludes disclosure of the contents. It may be sent by first class mail or parcel post (this does not apply to classified messages or any other classified material containing FOUO information). Bulky items may be sent by fourth class mail.

c. Each part of electrically transmitted mes-

sages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation FOUO before the beginning of the text.

3-6. Safeguarding

a. Duty hours. FOUO information will have a DA Label 87 attached when removed from containers (i.e., unlocked file cabinets or desks) or will be covered with nonsensitive papers in such a manner as to prevent unauthorized access to the information.

b. After duty hours. FOUO material will be stored with other unclassified material in unlocked file cabinets or desks and rooms of locked buildings.

c. Unauthorized disclosure. Appropriate administrative action will be taken to fix responsibility whenever possible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act of 1974 could result in criminal sanctions against responsible person(s). The DOD component that originated the FOUO information will be informed of its unauthorized disclosure.

3-7. Disposal

All FOUO or information protected by the FOIA will be disposed of in the following manner:

a. FOUO material will be destroyed by shredding or by tearing each copy into pieces to preclude reconstruction and placing them in regular or recycle trash containers.

b. Shredded material may then be bagged or boxed and taken to the building recycle point. All carbon paper must be removed.

Chapter 4 Classified Information

4-1. Access

a. Access is the ability or opportunity to obtain knowledge of classified information. There are specific requirements which must be met before an individual is authorized access to classified information. The requirements are as follows:

(1) Has a need to know.

(2) Has a valid and up-to-date security clearance equal to at least the classification level of the information or material.

(3) Understands the information is classified.

(4) Knows how to protect the information according to required security briefing.

(5) Has the ability to protect the information.

(6) Has been granted authority to access classified information by the supporting SM.

(7) Has executed an SF 312 (Classified Information Nondisclosure Agreement).

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

b. If any one of these does not exist, access to the information must be delayed, and the holder's SM is notified for guidance.

4-2. SF 312

The SM will maintain documentary proof that DOD civilians and locally hired DOD consultants possess a valid security clearance, have a need to know, and have executed an SF 312 as a condition of granting access to classified information. Only the SM may grant access to classified information for HQ USAREC and supported activities. Contractors requiring access to classified information must execute the SF 312 through their company. Disposition of executed SF 312s shall be conducted in accordance with provisions of AR 380-5.

4-3. Custodial procedures

Safeguarding and limiting access on the basis of the need to know and a valid security clearance is the responsibility of all users and holders of classified information. The HQ USAREC SM and directorate and special activity SMs are responsible for ensuring that personnel handling classified material are aware of and comply with all requirements and measures for safeguarding classified material while it is in their directorate's, unit's, or activity's control. The custodian of classified material is the person who has it in his or her possession (AR 380-5).

a. Care during duty hours.

(1) Cover sheets. Classified material removed from security containers will be kept under constant surveillance. Cover sheets (SF 704 (SECRET Cover Sheet) or SF 705 (CONFIDENTIAL Cover Sheet)) will be attached to the front of any document removed from the security container. Working papers, drafts, and classified documents generated by activity personnel will also have cover sheets attached.

(2) When classified material is transported from one location to another, it will be covered in such a manner as to prevent viewing (i.e., briefcase, manila folder, or brown envelope).

b. Work habits. Whenever an individual uses classified information there may be a tendency to become careless with its protection. Work habits need to be developed that will provide appropriate security for the classified material, regardless of whether the information is contained in a document, working paper, draft, or on any recordable media. Personnel in possession of classified material will ensure entry into work area is controlled when processing classified information. Individuals working with classified information should be aware of any visitors in the area and cover and protect their materials.

c. Safeguarding waste materials. Waste materials (i.e., recordable media, microfiche, carbons, drafts, working papers) will be stored in a General Services Administration (GSA) approved security container until such time as they can be destroyed.

d. Each activity and individual receiving classified material has the responsibility to properly safeguard, control access to, store, and destroy classified material obtained from internal and external sources

4-4. Mail screening procedures

Personnel authorized to pick up, deliver, receive, or open first class, certified, or registered mail must have a valid security clearance. Personnel authorized to pick up, deliver, or open first class, registered, or certified mail will be listed on an access roster which is maintained and distributed to HQ USAREC directorate and special activity SMs by the HQ USAREC Security Division.

a. Individuals picking up mail will ensure it is continually protected until it can be determined that it contains no classified material.

b. First class, registered, or certified mail will not be left unattended on desktops or in inboxes and outboxes until classification has been determined.

c. Mail that contains classified information will be placed in a security container or, if no longer needed, destroyed.

4-5. Removal of classified material from HQ USAREC buildings

Only the SM may authorize removal of classified information, after duty hours, from any HQ USAREC building. Appropriate security measures apply and an operational requirement must exist to remove the documents after duty hours.

4-6. Telephone security

The telephone is not a secure means of communication. Individuals using a telephone in an area where classified or sensitive information is being discussed should use caution. Do not discuss sensitive or classified information in an area where it may be picked up on an open telephone line. Use only secure telephones when discussing classified information and do not let yourself be overheard during someone else's telephone conversation. Secure telephone equipment is located in the Command Operations Center for use by authorized individuals.

4-7. End-of-day security checks

An end-of-day security check will be conducted using SF 701 (Activity Security Checklist). An integral part of the security check will be, as a minimum, where applicable, checking each security container to ensure it is locked and that reproduction machines and/or shredders are checked to ensure classified material has not been left unattended or partially destroyed. This checklist will be posted at the lockup door for each individual office or section. This checklist may include such items as: Recording that computers are powered off, all unnecessary utilities are turned off, windows locked, and file cabinets, desks, and so on are locked or other end-of-day procedures that are deemed necessary by the activity supervisor.

4-8. Emergency planning

a. All activities with classified material shall establish emergency plans as required by AR 380-5 to provide for the protection of classified material in a manner that will minimize the risk of personal injury or loss of life to personnel in the

case of fire or natural disaster.

b. Post emergency plans in a conspicuous place, such as on the wall near the storage container or for the senior person present to deviate from established plans when circumstances warrant.

c. The emergency evacuation and destruction plan will be tested annually.

4-9. Visitors

a. On occasion, personnel from this command visit other activities and organizations. Many times these visits involve access to classified information or material, creating a need to certify individual security clearance information. To facilitate the certification of security clearances, the individual, supervisor, or directorate or special activity SM must contact the HQ USAREC Security Division with information sufficient to complete a verification memorandum for forwarding to the activity being visited. To prevent access difficulties and/or delays, notification must be provided to the HQ USAREC Security Division no later than 10 days from the date of the scheduled visits.

b. When any HQ USAREC or supported activity is contacted by or is inviting, hosting, or sponsoring a visit of any person or organization that involves foreign personnel or when access to classified information is involved, the HQ USAREC SM will be notified.

4-10. Classified presentations and meetings

Activities that hold or sponsor any type of classified presentation will appoint a security representative, normally and when possible the directorate or special activity SM, to be responsible for the overall security at the site of the presentation. The security representative will ensure:

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

b. That only rooms or areas approved by the HQ USAREC Security Division are used for conversations or discussions involving classified material.

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

d. All personnel are evacuated from the presentation room, prior to initiating an access roster check.

e. Access rosters (name, rank, social security number, clearance, and organization) to verify authorized attendees are compiled and used at a controlled entrance point.

f. Attendees must be identified by presenting a picture identification (ID) (military or civilian employee ID card, passport, driver's license, etc.) before admittance into the presentation area. Support personnel (i.e., guards, monitors, etc.) will verify personal information by comparing the access roster and the presented

ID. If there are discrepancies, the attendee must be referred to the security representative. Under no circumstances will the attendee be allowed to enter that presentation area until the security representative verifies their authorization to attend.

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

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

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

j. Note taking, unless strictly controlled, is prohibited.

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

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

4-11. Reproduction of classified material

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

4-12. Security containers

Only GSA-approved security containers will be used to store classified material. Each container will be marked externally with the container serial number or symbol. This marking is for ID and will not indicate either the level of classified material contained within or the evacuation priority (AR 380-5). All security containers used for the storage of classified material will have a red "OPEN" sign displayed on the top drawer of the container when unlocked and when locked and properly checked, a white "CLOSED" or "LOCKED" sign will be displayed on the top drawer of the container. The tops and sides of all security containers shall be kept free of all extraneous materials except emergency actions procedure instructions, which shall be posted on the side of the container. Open containers will not be left unattended at any time. When not in use or when taken out of service, the combination will be changed to 50-25-50 and a notice, "This Container Will Not Be Used for Storage of Classified Material," will be posted on the front of the container.

a. The HQ USAREC Security Division and the Command Operations Center have GSA-approved security containers for the storage of

classified material. HQ USAREC activities requiring storage of classified material, but not having a GSA-approved container may coordinate the use of these containers. Containers located throughout HQ USAREC must be under the supervision and control of the individual activity SM and supervisory personnel.

b. Forms. SF 700 (Security Container Information), SF 702 (Security Container Check Sheet), a reversible open and closed sign, and an emergency evacuation and destruction plan will be posted on a side of the container or in the vicinity of each security container (AR 380-5).

(1) SF 700. SF 700 will be completed and part 1 will be attached to the inside front locking drawer of each security container. Part 3, which contains the combination, will be marked with the highest classification of material stored in the security container and will be placed inside part 2 envelope and sealed. Part 2 envelope will be marked with the same classification level as part 3. Part 2 envelope will be stored in the security container located in the HQ USAREC Security Division. The security container located within the Command Operations Center will be used for the part 2 of SF 700 for the security container located in the HQ USAREC Security Division.

(2) SF 702. SF 702 will be used on each security container. The date and time the container is unlocked and locked will be recorded. The last entry of the day will also record the initials and time that the container was checked. This must be someone other than the person locking the container. Any available person may conduct the check. If the container is not opened on a day the office is opened, record the date and initial the "checked by" column. SF 702 will be kept on file for 24 hours after it has been filled out on both sides, then discarded, unless it is needed for an investigation of a possible security violation.

c. Combinations. Combination to each security container will be changed at least annually, or when a person having access to the container is transferred, discharged, reassigned, or their security clearance is revoked or access suspended. Combination will also be changed if the combination has been or is suspected of being compromised. (Should North Atlantic Treaty Organization information be stored in the security container the combination will be changed every 6 months (AR 380-5)). NOTE: Individuals who have been given the combination to the security container are responsible for memorizing the combination. It will not be carried in a billfold, purse, or written on a calendar, etc.

d. Open storage. Neither the HQ USAREC Security Division nor any other HQ USAREC activity has approved open storage areas.

e. Container markings. Security containers will be marked externally with the security container number. It will not be marked to indicate the level of classification of material contained, evacuation priority, nor will it show the classification level of a particular drawer. Part 1, SF

700 will be used to record the container's number. Evacuation priority markings will be placed on the inside top lip of each security container drawer (AR 380-5).

4-13. Transmission of classified information

Compromise of classified documents results when required procedures are not followed in the transmission of classified material. Procedures for mailing classified information are outlined in AR 380-5.

a. Mail. The procedures for mailing classified material varies with the level of classification of the material or information.

b. Messages. TS, SECRET, and CONFIDENTIAL messages will be transmitted through the Fort Knox Communications Center, Director of Information Management, building 1110.

c. Distribution system. Use of unclassified, uncontrolled channels or "typical" distribution in "shotgun" envelopes is unauthorized.

4-14. Hand-carrying classified information

(Does not apply to communications security material.) Appropriately cleared personnel will be authorized, in writing, by the HQ USAREC SM or via courier card, to hand-carry or escort classified material between USAREC, Fort Knox, and continental United States activities to be visited subject to the following conditions:

a. Surface transportation.

(1) When there is insufficient time to mail the classified material and the activity to be visited does not have the document on file.

(2) The courier will receive a briefing, given by the HQ USAREC SM, prior to travel and will sign a briefing statement to that effect. The statement will be retained on file until the individual is no longer employed by HQ USAREC.

(3) DD Form 2501 (Courier Authorization Card) will be issued to couriers.

b. Air. Approval to hand-carry classified material on commercial airlines within the US, its territories, and Canada requires approval in writing from the HQ USAREC security officer.

(1) Every effort should be made to mail the information and make hand-carrying unnecessary.

(2) If the material will not fit into a briefcase or envelope and must be packaged, the approval authority will make advance arrangements with the airlines to ensure that package is not opened for inspection.

(3) Ensure storage arrangements at the temporary duty location are made upon arrival.

(4) Approval to hand-carry classified material outside the US, its territories, and Canada must be approved in writing by Headquarters, Department of the Army. All the requirements of AR 380-5 must be addressed. Requests will be submitted through the HQ USAREC Security Division to Headquarters, Department of the Army.

4-15. Violations or compromises

The HQ USAREC SM and each directorate and

special activity SM will ensure that the discovery of a security violation is immediately reported to the security officer. Procedures and requirements for reporting suspected or known violation or compromises are established in AR 380-5.

**Appendix A
References**

**Section I
Required Publications**

AR 25-2
Information Assurance. (Cited in para 3-3c.)

AR 25-55
The Department of the Army Freedom of Information Act Program. (Cited in para 3-3c.)

AR 380-5
Department of the Army Information Security Program. (Cited in paras 1-1, 1-4b(2), 1-4c(2), 1-4c(5), 1-4d, 2-1, 2-2, 2-2a, 2-2b, 2-2c, 2-3, 3-3c, 3-4b, 4-2, 4-3, 4-8a, 4-12, 4-12b, 4-12c, 4-12e, 4-13, 4-14b(4), and 4-15.)

AR 380-10
Foreign Disclosure and Contacts With Foreign Representatives. (Cited in para 3-3c.)

**Section II
Related Publications**

AR 15-6
Procedures for Investigating Officers and Boards of Officers.

AR 340-21
The Army Privacy Program.

AR 380-13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations.

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

AR 381-10
US Army Intelligence Activities.

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

**Section III
Referenced Forms**

DA Label 87
For Official Use Only Cover Sheet.

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 704
SECRET Cover Sheet.

SF 705
CONFIDENTIAL Cover Sheet.

Glossary

CUI

controlled unclassified information

DOD

Department of Defense

FOIA

Freedom of Information Act

FOUO

For Official Use Only

GSA

General Services Administration

HQ USAREC

Headquarters, United States Army Recruiting
Command

ID

identification

SM

security manager

TS

TOP SECRET

USAREC

United States Army Recruiting Command