

Security

Security Program

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 regulation which is effective 1 September 2004.

Summary. This regulation prescribes policies and guidance pertaining to security programs which include personnel, physical, information, security education and awareness, and Subversion and Espionage Directed Against the US Army. This regulation also assigns responsibility for the protection of Army information, personnel, and property. This regulation does not include specific requirements for Army applicant personnel security procedures.

Applicability. This regulation applies to all military and civilians at all levels of the United States Army Recruiting Command. Any violation of its requirements may subject Soldiers to disciplinary action under Article 92, Uniform Code of Military Justice, and civilian personnel may be subject to adverse action under civilian personnel regulations. Questions pertaining to this regulation or Department of Defense and DA security regulations should be addressed to the Command Security Manager at DSN 536-0238 or 0225 or commercial (502) 626-0238 or 0225. Written inquiries should be forwarded to the Assistant Chief of Staff, G-3, ATTN: RCRO-SEC, 1307 3rd Avenue, Fort Knox, KY 40121-2726.

Proponent and exception authority. The proponent of this regulation is the Assistant Chief of Staff, G-3. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to the deputy G-3 within the proponent agency in the grade of GS-14.

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

Supplementation. Supplementation of this regulation is prohibited.

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. Distribution of this regulation has been made in accordance with USAREC Pam 25-30, distribution A. This regulation is published in the Recruiting Station Administration UPDATE. This regulation is also available electronically on the USAREC Enterprise Portal.

Contents (Listed by paragraph number)

Chapter 1

General

- Purpose ● 1-1
- References ● 1-2
- Explanation of abbreviations ● 1-3
- Responsibilities ● 1-4
- Coordination ● 1-5
- Reports ● 1-6

Chapter 2

Security Inprocessing and Outprocessing
HQ USAREC and activities supported by the
HQ USAREC Security Division ● 2-1
Rctg Bde and Rctg Bn activities ● 2-2

Chapter 3

PS

- Suitability investigations and security clearances ● 3-1
- Security briefings ● 3-2
- Officials authorized to grant security clearances ● 3-3
- Suitability and entrance investigations ● 3-4
- Requesting PS investigations ● 3-5
- Granting access to classified information ● 3-6
- Reporting unfavorable information ● 3-7
- Security education ● 3-8
- PS records and data ● 3-9

Chapter 4

Information Security

- General ● 4-1
- Document retention ● 4-2
- SM appointments and responsibilities ● 4-3

Chapter 5

SAEDA

- General ● 5-1
- SAEDA training ● 5-2

Chapter 6

PHS

- General ● 6-1
- Responsibilities ● 6-2
- PHS plans and reports ● 6-3
- PHS equipment ● 6-4
- USAREC facilities ● 6-5
- End-of-day security checks ● 6-6
- Emergency notification cards ● 6-7
- PHS inspections ● 6-8
- Security of funds and/or negotiable instruments ● 6-9
- Small computers and business machines ● 6-10
- Mailrooms ● 6-11
- Administrative key control ● 6-12

Appendix A. References

Glossary

Chapter 1

General

1-1. Purpose

This regulation prescribes policies, guidance, and implements the United States Army Recruiting Command's (USAREC's) security programs including security inprocessing and outprocessing, personnel security (PS), information security, Subversion and Espionage Directed Against the US Army (SAEDA), physical security (PHS), and information system security. This regulation combines security-related programs into one directive. This information is designed to supplement detailed instructions contained in references and establish policy specifically for USAREC.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations

Abbreviations used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The USAREC Security Program is a command responsibility. It is also the responsibility of all military and civilian supervisors as well as individuals within USAREC. Commanders and supervisors must become familiar with the provisions of this regulation and implement applicable portions.

*This regulation supersedes USAREC Regulation 380-4, 16 October 2002.

b. In order to implement a comprehensive security program, appointed security representatives and security managers (SMs) at all levels must have on hand and maintain the appropriate references cited in this regulation.

c. Commanders and directors will appoint SMs and security representatives (e.g., SMs, PHS officers, key custodians, etc.), in writing, as appropriate. Appointed duties may be performed by either military or civilian personnel.

d. Commanders and directors will develop and implement comprehensive written standing operating procedures (SOPs) for applicable security programs for their activities.

e. The USAREC security officer serves as the SM for assigned Headquarters, United States Army Recruiting Command (HQ USAREC) security programs; manages the HQ USAREC Security Division; and serves as the principal staff officer and point of contact for security-related matters for USAREC activities. The security officer provides guidance, policy, and assistance to field commanders and appointed SMs as required. As such, he or she may conduct security-related investigations, inquiries, commandwide inspections, staff visits, training, seminars, and establish policies required by regulations, directives, or as directed by the commander. The security officer reviews security posture at recruiting brigades (Rctg Bdes) and recruiting battalions (Rctg Bns).

f. Rctg Bde, Rctg Bn, and recruiting company commanders will establish and implement security programs within their respective activities in accordance with Army regulations, this regulation, and established SOPs. When required, commanders will coordinate security program requirements and issues or concerns with the HQ USAREC Security Division. Rctg Bdes and Rctg Bns that have installation support agreements for intelligence and security services and/or police and law enforcement services must ensure that all aspects of requirements contained in Department of the Army (DA) and USAREC security regulations are met. Rctg Bdes and Rctg Bns must continually review their installation support agreements to determine what programs are supported and to what extent these programs are supported. Functional areas not specifically supported remain the responsibility of the Rctg Bde or Rctg Bn commander.

g. All personnel (civilian, military, and contractor) assigned or attached to USAREC have the inherent responsibility to be security conscious, to safeguard both classified and unclassified information and Government property. Included is the responsibility to report and/or correct actual or possible violations, reportable incidents, or inadequate security measures.

1-5. Coordination

Direct coordination between organizations, offices, or activities within USAREC is authorized and encouraged. In addition, Rctg Bdes and Rctg Bns may coordinate directly with local supporting security offices and law enforcement agencies on matters of security regulation and policy.

1-6. Reports

Specific reports and other written requirements are contained in each chapter of this regulation and cited Army regulations. All USAREC personnel are required to report within 24 hours, to the HQ USAREC Security Division or their appointed unit SM, any actual, suspected, or possible compromise of classified information or sensitive information; security violation or incident, known or suspected attempts or contacts by unauthorized persons, agencies, or governments; and any other suspicious acts which may impact on security.

Chapter 2

Security Inprocessing and Outprocessing

2-1. HQ USAREC and activities supported by the HQ USAREC Security Division

a. Inprocessing. Directorate supervisors and SMs shall ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided automation information systems (AISs) or access thereto inprocess with the HQ USAREC Security Division upon assignment to the headquarters. The Security Division will verify security investigation and security clearance documentation and initiate actions to request appropriate security investigation or security clearance as required by duty position or career field. The Security Division shall provide and document initial security briefings for all incoming personnel. Briefings will include security-related matters such as SAEDA, information security, information technology security, and PHS. Security files for each individual will be established and maintained by the Security Division.

b. Outprocessing. Directorate supervisors and SMs shall ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto outprocess through the Security Division prior to departure from the headquarters as a result of a permanent change of station, transfer, or termination of employment. The Security Division will verify that each individual has a record of appropriate security investigation or security clearance initiation or completion in their personnel file. The Security Division will notify the Headquarters Commandant, HQ USAREC, and the personnel service center if military personnel do not meet security clearance requirements for transfer. Security investigative or clearance documents required by the next duty assignment shall be prepared and forwarded as appropriate. Required security debriefing and termination statements will be completed and forwarded as required. Notification reports to personnel central clearance facility (CCF) will be prepared and forwarded as required.

2-2. Rctg Bde and Rctg Bn activities

a. Inprocessing. Commanders will ensure that all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto inprocess with the appointed SM within 24 hours of assignment to the activity.

(1) The SM will verify suitability and security investigation and security clearance documentation for each individual assigned and initiate actions to request appropriate suitability and security investigation or security clearance as required by duty position or career field.

(2) Initial security briefings shall be provided and documented for all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors. Briefings will include security-related matters such as SAEDA, information security, and PHS. Security files for each individual will be established and maintained.

b. Outprocessing. Commanders will ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto outprocess with the appointed SM prior to departure from the activity as a result of a permanent change of station, transfer, or termination of employment. The SM shall verify each individual has a record of appropriate security investigation or security clearance initiation or completion. The SM will notify the activity commander and personnel service center if military personnel do not meet security clearance requirements for transfer. Security investigative or clearance documents required by the next duty assignment shall be prepared and forwarded as appropriate. Required security debriefings and termination statements will be completed and forwarded as required. Notification reports to CCF will be prepared and forwarded as required.

Chapter 3 PS

3-1. Suitability investigations and security clearances

AR 380-67 as supplemented by written policy and guidance from the Department of Army Military Intelligence Counterintelligence and Security and CCF provide specific requirements for the PS Program. PS investigations; periodic reinvestigations; determination of clearance requirements; designation of civilian position sensitivity levels; initial, annual, and foreign travel security briefings; granting interim security clearances; granting access to classified information; reporting unfavorable information; denial and/or suspension of access to classified material; recommending revocation or denial of security clearance; and maintenance of security records and files are the responsibility of the HQ USAREC Security Division for HQ USAREC and supported activities, and that of Rctg Bde and Rctg Bn commanders and/or their appointed SMs for their respective activities. The HQ USAREC Security Division and SMs at Rctg Bdes and Rctg Bns will only process and request security investigations, periodic reinvestigations, or security clearances for US citizens in accordance with DA regulation and policy. Individuals will not be processed for a security investigation or security clearance without a valid requirement as described below:

a. Military (Army). Positions requiring specified investigative and/or clearance by military occupational specialty, branch or career man-

agement series, duty positions, specific automation data processing sensitivity, official assignment instructions, or official educational or travel requirements.

b. Civilians. Employee positions that have designated position sensitivities of noncritical sensitive or critical sensitive, those approved job descriptions requiring security clearances, official assignment instructions, or those specific instructions provided by Department of Defense and DA agencies.

(1) Favorable completion of a suitability investigation is a condition of employment for all civilian employees. This procedure is normally initiated by the servicing civilian personnel office and is basically used as a suitability determination. A final security clearance as required by the position or career specialty may be a condition of initial or continued employment by a Federal employee. Federal employees may be appointed pending completion of investigation and/or granting of final security clearances provided applicable procedures of AR 380-67 are followed.

(2) The HQ USAREC security officer and Rctg Bde and/or Rctg Bn SM are responsible for the approval and designation of civilian position sensitivity levels for their respective activities. Changes to existing sensitivity designations or approval of new sensitivity designations requires a copy of the job description, written justification for the need of a security clearance, and a completed SF 52-B (Request for Personnel Action) be routed through and approved by the HQ USAREC Security Division or the Rctg Bde or Rctg Bn security office prior to forwarding to the servicing civilian personnel office.

c. Contractors and volunteer personnel. Contractor employees and volunteers, like all personnel accessing AISs, must have a completed suitability investigation prior to granting access to AISs. Investigations must be completed according to the designated information technology sensitivity level as described in AR 25-2.

d. Non-US citizens are not authorized access to information technologies until the required suitability investigation has been completed and adjudicated. No interim access to AIS is authorized. Additional guidance may be found in AR 25-2.

3-2. Security briefings

In addition to initial security briefings, the HQ USAREC security officer will prepare, conduct, and document overseas travel briefings, initial security briefings, and annual refresher briefings as required by AR 380-67, AR 381-12, and AR 380-5.

3-3. Officials authorized to grant security clearances

Only the Commander, CCF, may grant final security clearances. Final security clearances are documented on a CCF-generated DA Form 873 (Certificate of Clearance and/or Security Determination). Commanders or their designated SMs (in writing) are the only individuals authorized to grant interim security clearances

as authorized by the provisions of AR 380-67.

3-4. Suitability and entrance investigations

Required suitability and entrance investigations shall be conducted in accordance with the provisions of AR 380-67.

3-5. Requesting PS investigations

Requests for PS investigations shall be processed and forwarded by the commander or the appointed SM as outlined in AR 380-67 and/or current guidance issued by Headquarters, Department of the Army.

3-6. Granting access to classified information

Access to classified information may be granted only by the HQ USAREC Security Division for HQ USAREC and supported activities. Rctg Bn commanders or their appointed SMs may grant access to personnel assigned to their activities provided that each individual meets the criteria established in AR 380-67. Specific procedures for granting access to classified information are contained in AR 380-67.

3-7. Reporting unfavorable information

AR 380-67 provides requirements for reporting unfavorable information. When a commander learns of credible derogatory information within the scope of AR 380-67, the commander or appointed SM will complete and forward DA Form 5248-R (Report of Unfavorable Information for Security Determination) to the Commander, CCF. The HQ USAREC Security Division will report credible derogatory information for all HQ USAREC and supported activities.

3-8. Security education

Commanders will establish and implement security education and awareness programs in accordance with AR 380-67.

3-9. PS records and data

Maintenance of individual PS records and rostered security information is an essential tool for the effective management of the PS Program. Information contained in security files or records, and on access or security rosters shall be protected according to the sensitivity of the information contained therein. As a minimum, commanders or their appointed security representative shall maintain:

a. Personal security records. A security file will be maintained for each individual assigned or attached to the activity. Contained in the file will be a verification by the commander or SM, as to the individual's investigative and/or clearance status as verified with the official investigative or clearance authority, such as Office of Personnel Management Federal Investigations Center, Defense Security Service, Defense Security Service Contract Office, CCF, Joint Personnel Access System, etc. In addition, records of clearance actions and correspondence, briefings, debriefings, reports of unfavorable information, local records checks, etc., will be maintained. Files will be maintained in accordance with AR 25-400-2 requirements. File

contents are to be maintained until the individual is no longer assigned to the activity, at which time the contents will be destroyed by appropriate method.

b. Security data or rosters. Activity commanders or appointed SMs will maintain a current and up-to-date record or listing of all personnel assigned to their activity that reflects the current status of security investigation, clearance, and level of access granted. The listing may be generated from a computer database, typewritten or handwritten, and will be updated at least quarterly. The listing must contain verification of security clearance and level of access granted and enough personal information, such as name, social security number, date of birth, place of birth, etc., to verify identification of an individual. The HQ USAREC Security Division will maintain such information for all HQ USAREC and supported activities.

Chapter 4 Information Security

4-1. General

Classified information and materials within USAREC will be handled, stored, transmitted, and destroyed in accordance with AR 380-5. Rctg Bde and Rctg Bn commanders are required to develop SOPs for this functional area as required by AR 380-5.

4-2. Document retention

The annual clean-out day, as required by AR 380-5, for all USAREC activities is the third Thursday of July.

4-3. SM appointments and responsibilities

a. The Commander, USAREC, will designate in writing an SM for USAREC as required by AR 380-5.

b. Requirement for designation of Rctg Bde, Rctg Bn, and directorate or activity SMs are established by paragraph 1-4c.

c. Specific SM responsibilities are provided in AR 380-5.

Chapter 5 SAEDA

5-1. General

SAEDA requirements for USAREC are established in AR 381-12.

5-2. SAEDA training

a. All USAREC personnel will receive an initial briefing during inprocessing and attend biennial SAEDA briefing. The commander or appointed SM will present the initial briefing. Counterintelligence personnel, the commander, or appointed SM will present refresher SAEDA briefing(s) biennially (every 2 years). Subject matter requirements are determined in AR 381-12. SMs may receive assistance in preparing and presenting SAEDA instructions from the supporting military intelligence element and the HQ USAREC Security Division.

b. Biennial SAEDA briefing requirements are not considered fulfilled unless antiterrorism train-

ing is included as part of the overall briefing.

c. Commanders or SMs will make every effort to prepare current, interesting, and relevant presentations. Individuals who are especially vulnerable to foreign intelligence agent approaches by virtue of their position, travel, duties, or activities will receive a special SAEDA briefing. Specific situations requiring a special SAEDA briefing are given in AR 381-12.

Chapter 6 PHS

6-1. General

AR 190-13 and AR 190-51 establish policies for protecting and safeguarding Government property. AR 190-13 identifies requirements for all tenant commanders. Additional requirements are established in this chapter.

6-2. Responsibilities

a. PHS is a commander's responsibility. The HQ USAREC security officer is responsible for providing assistance, guidance, and support to HQ USAREC and Rctg Bde and Rctg Bn commanders. Rctg Bde and Rctg Bn commanders are responsible for PHS programs for their respective units.

b. PHS programs must provide the means to counter threat entities during peacetime, mobilization, and war. Commanders, supervisors, and individuals responsible for the use, transport, accountability, security, or possession of Government property shall take every precaution to ensure adequate security is provided for that property at all times. PHS measures employed must be adequate, reasonable, and economical. They must retard unauthorized access to information, material, and equipment and prevent interference with the operational capability of the activity. However, great care must be exercised to ensure security is not sacrificed for the sake of convenience. If doubt exists as to the standard being used to secure Government property, the HQ USAREC Security Division will determine what the approved standard will be.

c. When deficiencies exist, commanders shall initiate reasonable compensatory measures until the deficiency is corrected. In those cases where a weakness may exist and property or equipment may be exposed, the use of constant surveillance (guards) is the best compensatory measure. Protection of the Government's interest and loss prevention are the goals of this policy. Inefficiency, procrastination, fraud, waste, and abuse lead to losses or create crime-conducive conditions.

6-3. PHS plans and reports

Commanders shall develop a PHS plan and PHS survey reports for their activities, as applicable, according to guidance provided in AR 190-13.

6-4. PHS equipment

Requests for PHS equipment such as intrusion detection systems, electronic entry control systems, and closed circuit television will be submitted to the HQ USAREC Security Division for approval prior to issue, purchase, lease, or lease

renewal.

6-5. USAREC facilities

Policies, procedures, and methods related to management of USAREC facilities are contained in USAREC Reg 405-1. Commanders must ensure that facilities continue to meet basic structure security requirements as established by AR 190-51. The safeguarding and protection of property and materials in the possession of USAREC activities will be provided as established by AR 190-13 and AR 190-51 or by compensatory measures as approved by the commander or the HQ USAREC Security Division.

6-6. End-of-day security checks

When closing a USAREC-occupied building or separate office located in a building with more than one activity (section, division, department, agency, etc.) at the end of the duty day, a designated person(s) will make a security check of the building or office to ensure all doors, windows, and other openings are properly secured and that containers storing controlled or pilferable items and sensitive or classified information are locked. Occupants of separate offices are responsible for conducting end-of-day security checks for their individual offices. Other items may be included as required by the commander or supervisor of the activity. Records of these security checks will be annotated on SF 701 (Activity Security Checklist). Where practical, SF 701 will be posted at the lockup door. When completed, SF 701 will be retained for 30 days.

6-7. Emergency notification cards

a. All tenant USAREC activities located on or in Government-owned or Government-leased properties shall follow the host activities procedures for use of emergency notification cards. Activities not located on Government-owned or Government-leased properties shall ensure notification information is posted on or adjacent to all entrances of buildings or on gates leading to the building. USAREC Form 810 (Emergency Notification Card) may be used. Activities located in areas where use of a language other than English is used as primary language shall include both English and the primary use language on the card. Cards are to be posted so as to protect against adverse weather conditions and vandalism (i.e., inside of doors or windows).

b. Where possible, every precaution should be taken to prevent the disclosure of individual names, addresses, and home telephone numbers of response personnel. Numbers of the unit, charge of quarters, staff duty officer, police, or security guard services should be used. Coordinating with and providing names, addresses, and home telephone numbers to the charge of quarters, staff duty officer, police, or other agencies may be necessary. When Privacy Act information must be included on the notification card, appropriate Privacy Act statement must also be included on the card.

6-8. PHS inspections

a. During annual facilities inspections con-

ducted by the Rctg Bn, the Rctg Bn commander shall also conduct an informal PHS inspection to ensure proper security measures are being employed to safeguard personnel, equipment, and material. Written results of the inspections, citing deficiencies, and recommended corrective measures will be maintained until the next inspection is conducted.

b. The USAREC security officer conducts announced and unannounced security inspections of HQ USAREC activities. The USAREC security officer may conduct announced security inspections at Rctg Bdes and Rctg Bns at intervals of at least once every 2 years. Results of inspections shall be prepared, forwarded, and maintained in accordance with AR 190-13.

6-9. Security of funds and/or negotiable instruments

a. Commanders, supervisors, and individuals that handle, store, and transport funds are responsible for all such funds and shall take precautions to ensure the protection of funds. This will include, but is not limited to the following:

(1) Adequate storage sites and containers with limited access to fund storage areas, to include key or combinations to these sites and containers.

(2) Proper fund custodians are appointed with separation of functions and access.

(3) No mingling of official funds with coffee funds in the same container or cash box. Cash will not be stored in containers securing classified information.

b. The following minimum measures will be in effect for all activities that store cash or negotiable instruments on their premises on an overnight basis, unless otherwise provided for in other regulations.

(1) All funds that are secured on an overnight basis that are appropriated funds or are nonappropriated funds in excess of \$200 will be secured in a tool resistant safe that is provided with a built-in three position dial combination lock that is equipped with a relocking device. Approved General Services Administration (GSA) security containers with Underwriter's Laboratory tool resistant ratings of TL-15 or higher may be used. If tool resistant money safes are not available, GSA approved Class 1 through 2, two-drawer security file containers may be used for the security of funds that are not in excess of \$500. Approved GSA Class 3 through 6 security file containers, weighing in excess of 750 pounds, will be used for the security of funds that are over \$500, but less than \$3,000. Security file containers are authorized for fund storage only when there are no better containers available or when purchase of new tool resistant containers would not be cost effective.

(2) Funds that are less than \$200, that are to be secured on an overnight basis, must be secured in an approved, lockable safe or steel container. Safes and containers that cost more than the amount of monies being secured within will not be purchased solely to conform to this regulation. Two-drawer Class 1, 2, and 6 security containers or Army field safes with built-in

combination locks may be used for funds of less than \$200.

(3) The use of small portable cash boxes for overnight storage is prohibited unless stored within approved containers as described in (1) and (2) above.

(4) Padlocks will not be used to secure fund safe doors after duty hours.

(5) All safes, weighing less than 750 pounds, will be secured to the structure by approved methods. One method is to secure the safe to the structure by use of steel eye-bolts anchored to the floor, with short lengths of chain (5/16 inch thickness) beneath the safe that are secured to the anchor with harden steel padlocks, or, by welding the safe to the anchor.

(6) Safes that are on wheels will have the wheels removed or will be bolted or secured to the structure in an approved manner.

(7) Fund containers will be secured in a locked room or building of a secure structure as described in AR 190-51 or, be in a room or structure that is under constant surveillance of duty personnel.

(8) Combinations to fund safes will be safeguarded, stored, and changed in accordance with AR 380-5.

6-10. Small computers and business machines

Desktop computers, laptop computers, calculators, typewriters, and similar machines are desirable objects and are highly susceptible to theft. Every effort will be made to ensure adequate security of such property. As a minimum, all such items will be accepted on a hand receipt by a responsible person within each office or activity and serial number inventories shall be conducted at least quarterly. Buildings or offices in which such items are stored or used will have adequate doors, windows, and locking devices. If located in rooms with lockable doors, the doors will be closed and locked at the close of business. Specific guidance and procedures will be published in command policy letters for laptop computer security and other items of specific concern to the Commanding General.

6-11. Mailrooms

Minimum security standards are located in DOD 4525.6-M. Access control will be established and limited to unit mail personnel and the commander only. Signs will be posted on entrances to designate authorized entry only. SF 702 (Security Container Check Sheet) will be posted on the outside of all safes and containers containing certified or classified mail and on the outside of the entrance door. Certified and registered mail, as well as payroll checks, stamps, indicia, or other similar items will be as a minimum, secured in a field safe or similar container that is provided with a built-in combination lock or that can be secured by approved hasp and combination padlock. Safes or containers weighing less than 750 pounds must be secured to the structure by an approved method. Classified mail will be screened, accounted for, secured, and transported in accordance with AR 380-5.

6-12. Administrative key control

a. Control, accountability, and PHS of Government property are interdependent. A comprehensive key control and property accountability system are basic to an effective PHS Program. Control of locks and keys provides primary safeguards for Government property and assets.

b. The term administrative keys applies to all keys other than those for arm ammunitions and explosives, alarm systems, or special access keys which require a higher level of control. Implementation and supervision of administrative lock and key control shall be in accordance with AR 190-51. Rctg Bdes and Rctg Bns must develop written procedures for the control and accountability of all keys used to protect or secure Government property.

c. There are three approved USAREC forms to be used for the control and management of administrative keys by all USAREC activities. They are:

(1) USAREC Form 1191 (Master Key Inventory).

(2) USAREC Form 1192 (Key Sign-In and Sign-Out Record).

(3) USAREC Form 1193 (Key Inventory Log (Monthly and Semiannually)).

Appendix A References

Section I Required Publications

AR 25-2
Information Assurance. (Cited in paras 3-1c and 3-1d.)

AR 25-400-2
The Army Records Information Management System (ARIMS). (Cited in para 3-9a.)

AR 190-13
The Army Physical Security Program. (Cited in paras 6-1, 6-3, 6-5, and 6-8b.)

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive). (Cited in paras 6-1, 6-5, 6-9b(7), and 6-12b.)

AR 380-5
Department of the Army Information Security Program. (Cited in paras 3-2, 4-1, 4-2, 4-3a, 4-3c, 6-9b(8), and 6-11.)

AR 380-67
The Department of the Army Personnel Security Program. (Cited in paras 3-1, 3-1b(1), 3-2, 3-3, 3-4, 3-5, 3-6, 3-7, and 3-8.)

AR 381-12
Subversion and Espionage Directed Against the US Army (SAEDA). (Cited in paras 3-2, 5-1, 5-2a, and 5-2c.)

DOD 4525.6-M
Department of Defense Postal Manual. (Cited in para 6-11.)

USAREC Reg 405-1
Facility Management. (Cited in para 6-5.)

Section II Related Publications

AR 5-9
Area Support Responsibilities.

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

AR 25-55
The Department of the Army Freedom of Information Act Program.

AR 50-5
Nuclear and Chemical Weapons and Materiel-Nuclear Surety.

AR 50-6
Nuclear and Chemical Weapons and Materiel, Chemical Surety.

AR 190-5
Motor Vehicle Traffic Supervision.

AR 190-11
Physical Security of Arms, Ammunition and Explosives.

AR 190-40
Serious Incident Report.

AR 380-10
Foreign Disclosure and Contacts With Foreign Representatives.

AR 525-13
Antiterrorism.

AR 530-1
Operations Security (OPSEC).

AR 600-37
Unfavorable Information.

AR 614-200
Enlisted Assignments and Utilization Management.

AR 635-200
Active Duty Enlisted Administrative Separations.

AR 680-29
Military Personnel - Organization and Type of Transaction Codes.

AR 735-5
Policies and Procedures for Property Accountability.

DA Pam 190-12
Military Working Dog Program.

DA Pam 190-51
Risk Analysis for Army Property.

DA Pam 710-2-1
Using Unit Supply System (Manual Procedures).

DA Pam 710-2-2
Supply Support Activity Supply System: Manual Procedures.

(O) DOD 2000.12-H
DOD Antiterrorism Handbook.

DOD 5200.1-PH-1
Classified Information Nondisclosure Agreement (SF 312), Briefing Pamphlet.

DOD 5200.2-R
Department of Defense Personnel Security Program.

DOD 5220.22-R
Industrial Security Regulation.

DOD 5400.7-R
DOD Freedom of Information Act Program.

FM 3-19.30
Physical Security.

FM 19-10
The Military Police Law and Order Operations.

FM 19-15
Civil Disturbances.

TB 5-6350-264
Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS).

Section III Prescribed Forms

USAREC Form 810
Emergency Notification Card. (Cited in para 6-7a.)

USAREC Form 1191
Master Key Inventory. (Cited in para 6-12c(1).)

USAREC Form 1192
Key Sign-In and Sign-Out Record. (Cited in para 6-12c(2).)

USAREC Form 1193
Key Inventory Log (Monthly and Semiannually). (Cited in para 6-12c(3).)

Section IV Referenced Forms

DA Form 873
Certificate of Clearance and/or Security Determination.

DA Form 5248-R
Report of Unfavorable Information for Security Determination.

SF 52-B
Request for Personnel Action.

SF 701
Activity Security Checklist.

SF 702
Security Container Check Sheet.

Glossary

AIS

automation information system

CCF

central clearance facility

DA

Department of the Army

GSA

General Services Administration

HQ USAREC

Headquarters, United States Army Recruiting
Command

PHS

physical security

PS

personnel security

Rctg Bde

recruiting brigade

Rctg Bn

recruiting battalion

SAEDA

Subversion and Espionage Directed Against the
US Army

SM

security manager

SOP

standing operating procedure

USAREC

United States Army Recruiting Command