Headquarters
United States Army Recruiting
Command 1307 3rd Avenue Fort Knox,
Kentucky 40121-2725
22 January 2019

*USAREC Regulation 380-4

Effective 22 January 2019

Security

Security Program

For the Commander:

WAYNE R. HERTEL
Colonel, GS
Chief of Staff

Official:

Ronnie L. Creech
Ronnie L. Creech
Assistant Chief of Staff, CIO/G-6

History. This publication is a major revision dated 22 January 2019. The portions affected by this major revision are listed in the summary ofchange.

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 U.S. Army. This regulation also assigns responsibility for the protection of Army information, personnel, and property. This regulation does notinclude specific requirements for Army applicant personnel security procedures.

Applicability. This regulation applies to all military and civilians at all levels of the U.S. 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 Department of the Army security regulations should be addressed to the Command Security Officer at DSN 536-0238 or 0225 or commercial (502) 626-0238 or 0225. Written inquiries should be forwarded to the Assistant Chief of Staff, USAREC, ATTN: RCCS-COC, 1307 Third Avenue, Fort Knox, KY 40121-2725.

Proponent and exception authority. The proponent of this regulation is the Assistant Chief of Staff, G3. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulations. Proponent may delegate the approval authority, in writing, to the COC chief.

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.

Relationship to USAREC Reg 10-1. This publication relates to the command security program as it relates to UR 10-1 para 3-24a.

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: RCCS-COC 1307 3rd Avenue, Fort Knox, KY 40121-2725.

Distribution. This publication is avail- able in electronic media only and is intended for command distribution level A.

*This regulation supersedes USAREC Regulation 380-4, dated 16 December 2009.

Contents (Listed by paragraph and page number)

Appendix A

Glossary of Terms

Summary of Change

Chapter 1.
General

1-1. Purpose
This regulation prescribes policies, guidance, and implements the U.S. Army Recruiting Command's (USAREC's) security programs, including security in-processing and out-processing, entry control, personnel security (PS), information security, Threat Awareness and Reporting Program (TARP), physical security (PHS), and information 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.

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

c. Commanders and Assistant Chiefs of Staff (ACS) will appoint SM for Department of the Army (DA) personnel and information security programs as outlined in chapters 1 through 7. Personnel assigned duties as the SM require a current secret security clearance. Commanders and ACS will appoint, in writing, security managers responsible for PHS and those functional requirements of chapter 6 as appropriate. Appointed duties may be performed by either military or civilian personnel. Due to similarity in program functionality within the area of force protection, commanders should appoint the brigade antiterrorism officer with those responsibilities and duties prescribed in chapter 6 as the physical security manager. Support for all requirements of the PS program will be provided for all personnel assigned, attached, or collocated within USAREC activities by that activity's commander or ACS.

(1) Brigade SM's: In addition to other responsibilities described in this regulation, brigade SM responsibilities include ensuring all personnel (brigade and battalion) have the required suitability investigation or security clearance. SM are the only personnel authorized to request investigations from the Office of Personnel Management/National Background Investigation Bureau (OPM/NBIB) or clearance actions from the U.S. Army Consolidated Adjudications Facility (CAF), directly coordinate follow up actions, or coordinate requests for additional information from OPM/NBIB and/or CAF; grant access to and establish user accounts for the Defense Information Security System (DISS); grant up to interim Secret clearances; make suitability determinations and recommend courses of action; grant access to classified information; respond to tasking's or requests for information from the Headquarters, U.S. Army Recruiting Command (HQ USAREC, G3), Security Office; make position sensitivity determinations; conduct investigations of security violations; develop brigade standard operating procedures (SOPs) and operational requirements; conduct oversight functions of subordinate activities; and coordinate actions regarding unfavorable information affecting access to information systems.

(2) Battalion SM. In addition to other responsibilities specifically described in this regulation, battalion SM's responsibilities primarily involve: In-processing and out-processing; entering required information in DISS; validating information via DISS; conducting briefings and debriefings; granting access to classified information; notifying the brigade SM when suitability investigations and/or security clearances are required; maintenance of files, rosters, and records; reporting unfavorable information via DISS incident reports; and assisting personnel in the completion of investigative forms. Battalion SM are not authorized to submit investigations to OPM nor request actions for security clearances to CCF nor establish or maintain communications with these activities.

d. Commanders and ACS' will develop and implement comprehensive written SOPs for applicable security programs for their activities.

e. The USAREC Security Officer serves as the SM for assigned HQ USAREC security programs; manages the HQ USAREC, G3 Security Office; 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 SM as required. As such, he or she may conduct security related investigations, inquiries, command wide 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 brigades and battalions.

f. Brigade, battalion, and company commanders will establish and implement security programs within their respective activities in accordance with Army regulations and formal guidance from HQ USAREC. Functional areas not specifically supported remain the responsibility of the brigade or battalion 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, brigades and battalions may coordinate directly with local supporting security offices and law enforcement agencies on matters of security regulations 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, G3 Security Office 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 In-processing and Out-processing

2-1. HQ USAREC and activities supported by the HQ USAREC, G3 Security Office

a. In-processing. SM shall ensure all personnel (permanent, temporary, term, and volunteers, including military, civilians, and contractors) using government provided automation information systems (AIS) or access there to, in-process with the HQ USAREC, G3 Security Office upon assignment to the headquarters. The Security Office 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 Office shall provide and document initial security briefings for all incoming personnel. Briefings will include security-related matters such as TARP, information security, IT security, OPSEC and PHS. Security files for each individual will be established and maintained by the Security Office either by hardcopy or e-file).

b. Out-processing. Supervisors and SM shall ensure all personnel (permanent, temporary, term, and volunteers, including military, civilians, and contractors) using government provided AIS or access thereto out-process through the HQ USAREC, COC Security Office prior to departure from the headquarters as a result of a permanent change of station, transfer, retirement or termination of employment. The Security Office will verify that each individual has a record of appropriate security investigation or security clearance initiation or completion in their personnel file. Required security debriefing and termination statements will be completed and forwarded as required.

2-2. Brigade and battalion activities

a. In-processing. Commanders will ensure that all personnel (permanent, temporary, term, and volunteers, including military, civilians, and contractors) using government provided AIS' or access thereto in-process with the appointed SM within 24 hours of assignment to the activity.

(1) The SM will verify suitability investigation and security clearance documentation via DISS 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. Perform necessary DISS actions.

(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 TARP, safeguarding sensitive and classified information, and unclassified Army property. Security files for each individual will be established and maintained via hard copy or e-file.

b. Out-processing. Commanders will ensure all personnel (permanent, temporary, term, and volunteers, including military, civilians, and contractors) using government provided AIS or access thereto out-process with the appointed SM prior to departure from the activity as a result of a permanent change of station, transfer, retirement 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. Perform necessary DISS actions.

2-3. Screening Requirements

a. All recruiters will be required to fill out USAREC Form 380-4.3 when in-processing. Commanders will interview the recr*u*iter in order to validate the information and submit the form to the Brigade OCP for review.

b. All contractors will be required to fill USAREC Form 380-4.5 when applying for employment. The COR will vet and review the form before it is submitted to the USAREC Security Managers Office.

Chapter 3.
Personnel Security (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 Counter- intelligence and Security and CCF provide specific requirements for the Personnel Security Program. PS investigations; periodic re-investigations; 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, G3 Security Office, for HQ USAREC and supported activities, and that of brigade and battalion commanders and/or their appointed SM for their respective activities. The HQ USAREC, G3 Security Office and SM at brigades and battalions will only process and request security investigations, periodic reinvestigations, or security clearances for U.S. citizens in accordance with DA regulations and policy. Individuals will not be processed for a 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 management series, duty positions, promotions to E-8 and E-9, 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, with 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 brigade 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 require a copy of the job description, written justification for the need of a

security clearance, USAREC CPO-CPMD and a completed SF 52 (Request for Personnel Action) routed through and approved by the HQ USAREC, G3 Security Office or the brigade security office prior to forwarding to the servicing civilian personnel office

c. Contractor, volunteer, and visitor personnel. Contractor employees, volunteers, and visitors including those requiring access from remote locations, like all personnel accessing AIS, must have a completed suitability investigation prior to granting access to AIS. Investigations must be completed according to the designated information technology (IT) sensitivity level as described in AR 25-2.

d. Non-U.S. citizens are not authorized access to ITs 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 and brigade and battalion SM 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 by either hardcopy or e-file.

3-3. Officials authorized to grant security clearances

Only the Commander, and the CAF, may grant final security clearances. The only validation source for security clearances is DISS. The HQ USAREC Security Officer and brigade commanders or their designated SM (in writing are the only individuals authorized to grant interim security clearances as authorized by the provisions of AR 380-67. Brigade commanders may only grant up to interim Secret clearances. Battalion commanders are not authorized to grant interim clearances at any level and must forward requests for interim clearances to the brigade. Only the HQ USAREC, G3, Security Office, is authorized to grant TOP SECRET clearances for USAREC activities. Requests for interim TOP SECRET clearances must be forwarded to HQ USAREC, G3, and Security Office through or from the brigade.

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 personnel security investigations

Requests for PS investigations shall be processed and forwarded to the HQ USAREC, G3, Security Office, or the brigade commander or the appointed SM as outlined in AR 380-67 and/or current guidance issued by Headquarters, Department of the Army. When it is determined that a suitability investigation or security clearance requirement exists for personnel assigned to a battalion, the battalion SM will request that action be initiated and completed by the brigade SM. Battalion SM shall assist personnel in the completion of required forms and ensuring information is accurate and complete prior to final submission to the brigade.

3-6. Granting access to classified information

Access to classified information may be granted only by the HQ USAREC, G3, Security Office for HQ USAREC and supported activities. Brigade and battalion commanders or their appointed SM 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 all incident reporting requirements via the incident report in DISS in accordance with the DISS User Guide.

3-8. Personnel security 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 and in accordance with current DA policy. As a minimum, commanders or their appointed security representative shall maintain:

a. PS 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 OPM Federal Investigations Center, Defense Security Service, Defense Security Service Contract Office, CCF, DISS, etcetera. In addition, records of clearance actions and correspondence, briefings, debriefings, reports of unfavorable information, local records checks, etcetera, 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 SM 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, etcetera, to verify identification of an individual. The HQ USAREC, G3, Security Office will maintain such information for all HQ USAREC and supported activities.

c. Safeguarding security information. PS documents or media and other related information such as: Records, rosters, investigative submission copies, returned investigative results, correspondence from OPM/NBIB and CAF regarding actions of a personal nature shall be safeguarded in accordance with AR 380-67. Minimum requirements are as follows:

(1) PS specialists and SM shall control and maintain accountability of all reports of investigation received.

(2) Reproduction, in whole or in part, of PS investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

(3) PS investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lock bar and approved three- position dial-type combination padlock or in a similarly protected area or container. Use of a standard lockable metal filing cabinet in a separate office with controlled access by only PS or SM is an approved method storage. Storage of information in standard locked metal file cabinets, overheads, desk drawers, and etcetera, in open areas such as cubicles does not meet DA standards. A separate office for the brigade security specialist is highly recommended to meet these standards if adequate containers are unavailable or not feasible and to provide a secure environment for the conduct of personal interviews and information exchange regarding highly sensitive and personal information.

(4) Reports or copies of submitted or completed PS investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows: "TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATIONS."

(5) PS investigative documents to include submissions and returned results may be retained only for the period necessary to complete the purpose for which they were originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization.

(6) All PS information documents or media shall be destroyed upon the departure of the individual from the unit. Destruction shall be accomplished in the same manner as for classified information with the classification of Secret and in accordance with the provisions of AR 380-5.

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. Brigade and battalion commanders are required to develop SOPs for this functional area as required by AR 380-5.

4-2. Document retention
All documents will be properly disposed of IAW AR 380-5.

4-3. SM appointments and responsibilities

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

b. Requirement for designation of brigade and battalion and HQ USAREC ACS offices and activity SM is established by paragraph 1-4c.

c. Specific SM responsibilities for safeguarding classified and sensitive information are provided in AR 380-5.

4-4. Safeguarding for Controlled Identified Information, Freedom of Information Act, personally identifiable information, and sensitive information

a. Controlled unclassified information (CUI), Freedom of Information Act (FOIA), personally identifiable information (PII), and sensitive information shall be safeguarded and marked in accordance with applicable instructions contained in AR 380- 5 and AR 25-55.

b. When electronically transmitting CUI, FOIA, PII, and/or sensitive information, the abbreviation "CUI" will be placed at the beginning and end of each transmission. Electronic transmissions containing CUI, FOIA, PII, and/or sensitive information shall be encrypted and UNCLASSIFIED CUI will be selected from the Classification tool bar on the Outlook message screen.

4-5. Destruction of CUI, FOIA, PII, and sensitive information

a. All printed materials that contain CUI, FOIA, PII, and/or sensitive information will be shredded. Minimum shredder specifications for CUI, FOIA, PII, and/or sensitive information are:

(1) Companies and stations. Strip cut with shred size no larger than 5/32-inch-wide with feed capacity of up to 12 pages, operating on 115 volts with 2/5 horsepower motor or crosscut with shred size no more than 5/21 x 1-3/32 inches with feed capacity of up to 8 pages operating on 115 volts, or local power voltage, with a 2/5 horsepower motor.

(2) Brigades and battalions. Strip cut with shred size no larger than 3/16-inch-wide with feed capacity of up to 22 pages, operating on 115 volts, or local power voltage, with 3/4 horsepower motor.

b. Use of commercial equipment and/or other Federal or military equipment is authorized provided minimum standards described above are met and are certified by the activity.

c. Properly shredded material may be placed in the trash or recycle bin.

d. Optical media including CDs and DVDs as well as diskettes and flash drives will be destroyed by burning, melting, chemical decomposition, pulping, pulverizing, crosscut shredding, or mutilation sufficient to preclude recognition, recovery, or reconstruction of the information.

e. External hard drives will be destroyed according to the Army BBP 1.7, dated 2 June 2009. Destruction of all media, both external and internal, shall be conducted according to instructions issued by HQ TRADOC.

4-6. Destruction of classified information and electronically produced media

Brigade and/or battalion SM are responsible for management of procedures for the safeguarding and destruction of classified information and material for their respective activities. Companies and stations have no capability to safe-guard classified information. Any and all classified material discovered in companies or stations will be immediately forwarded to the battalion SM according to applicable instructions for transmission of classified information contained in AR 380-5. Upon receipt, battalion SM without capability to safeguard classified information will immediately forward the information or material to the brigade SM according to applicable instructions for transmission of classified information contained in AR 380-5.

a. Classified documents and printed materials will be destroyed by shredding. Minimum shredder specifications for classified information is crosscut size no larger than 0.08 x 4.5 millimeters with feed capacity of up to 10 pages, operating on 115 volts with 1/2 horsepower motor.

b. Optical media, CDs, DVDs, diskettes, flash drives, and external devices will be destroyed by burning, melting, chemical decomposition, pulping, pulverizing, crosscut shredding, or mutilation sufficient to preclude recognition, recovery, or reconstruction of the classified information.

c. Use of other Federal or military facilities and equipment is authorized provided minimum standards described in AR 380-5 are met and are certified by the activity. Use of commercial activities for destruction is not authorized.

4-7. Distribution of shredders

When procured, all shredders will be delivered to the battalion supply section for accountability and/or further distribution to subordinate activities.

4-8. SIPRNET Procedures

a. All requests will be submitted to the G6- Cyber Security Office for access to the SIPRNET with a valid reason for access.

b. Requests will be submitted on DD FM 2875 (SAAR) and FK FM 5084 (Ft. Knox Network Form).

Chapter 5.
Threat Army Reporting Program (TARP)

5-1. General

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

5-2. TARP training

a. All USAREC personnel will receive an initial briefing during in-processing and attend a biennial TARP briefing. The commander or appointed SM will present the initial briefing. Counterintelligence personnel, the commander, or appointed SM will present refresher TARP briefings biennially (every 2 years). Subject matter requirements are determined in AR 381-12. SM may receive assistance in preparing and presenting TARP instructions from the supporting military intelligence element and the HQ USAREC, G3 - Security Office.

b. Biennial TARP briefing requirements are not considered fulfilled unless antiterrorism training is included as part of the overall briefing.

c. Commanders or SM 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 TARP briefing. Specific situations requiring a special TARP briefing are given in AR 381-12.

Chapter 6.
Physical Security (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, G3 PHS Officer is responsible for providing assistance, guidance, and support to HQ USAREC and brigade and battalion commanders. Brigade and battalion 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, G3 PHS Officer 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. Weapons Prohibited Labels (USAREC Label 380-4.1)

USAREC Label 380-4.1 (Old UL 21-Warning - Weapons Prohibited) will be posted at the main entrance(s) of each USAREC activity within a Federal building or installation and in activities located off installation IE: Stations. The label will be posted at eye level and in a position in which the label can be plainly seen without obstruction upon entry to the activity.

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, PHS Officer 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 700-5. 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, PHS Officer.

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, etcetera,) 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 pilfer able 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 (USAREC Form 380-4.4)

a. All tenant USAREC activities located on or in Government-owned or Government-leased properties shall follow the host activity's 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 380-4.4 (Old UF 810-Emergency Notification Card) may be used. Activities located in areas where use of a language other than English is used as the 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 (that is, 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 conducted by the battalion, the battalion commander or his or her designated representative 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, PHS Officer conducts announced and unannounced security inspections of HQ USAREC activities. The USAREC, PHS Officer may conduct announced security inspections at brigades and battalions 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 non-appropriated 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 500 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 by duty personnel.

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

6-10. Desktop computers, laptops, tablets, GOV cellphones and business machines

Desktop computers, laptop computers, calculators, tablets, GOV cell phones, 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. Every attempt will be made to utilize cable locks and secure the device at all times. GOV's will have USAREC Label 380-4.2 (Old UL Form 24 - Laptop Security Awareness) affixed to the driver’s window.

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 500 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 apply 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. Brigades and battalions must develop written procedures for the control and accountability of all keys used to protect or secure Government property.

c. DA Form 5513-R is only approved form to be used for the control and management of administrative keys.

Chapter 7.
Access Control Procedures for Bldg. 1307

7-1. Watch officer

Building access is managed 24/7 by the Assistant Chief of Staff (ACS), G3 COC Security Office and the watch officer (WO). The WO’s primary place of duty is the desk at the main entrance.

7-2. Key control

a. Staff directorates will maintain control and accountability of all keys and locks for use within their functional work areas.

b. The Headquarters Commandant retains control and accountability of all facility keys, less keys to desks, cabinets, and similar containers.

c. If a person has forgotten their work area or room key, the HHC Commandant's Office can open the door or the WO can open the door after duty hours if the WO recognizes the employee. The facility manager will be contacted during duty hours. If the WO does not recognize the person, the WO will call the person’s supervisor to authenticate the person for access to their work area for emergencies only.

7-3. Security

Close circuit television video (CCTV) cameras monitor every point of entry to Bldg. 1307, Bldg. 2366, and Bldg. 2389 24/7. The WO monitors, programs, and controls the security system under the direction of the Chief, COC Security.

7-4. Personnel access utilizing a CAC

a. U.S. Army Recruiting Command (USAREC) personnel whose primary place of duty is HQ USAREC will be granted CAC access. Personnel will scan their CAC and enter their (at elevated FPCON) personal identification number (PIN) to gain entry.

b. Fort Knox workforce personnel who perform support duties within building 1307 can be issued CAC access if they require access at least two times a week or eight times per month. The COC chief will develop a system to monitor and determine whether the criteria have been met for CAC programing; this determination is made after the identified person is monitored for at least 30 days. Personnel requesting to be granted access via a CAC will be nominated by a commissioned officer or Department of the Army civilian in a supervisory position assigned to building 1307.

c. Visitor personnel are required to wear their visitor badge on their person where it is easily recognizable at all times

d. Newly-assigned personnel receive a security briefing during them in-processing at the COC Security Office. Once the briefing is complete and the SF 85 (Questionnaire for Non-Sensitive Positions) or SF 86 (Questionnaire for National Security Positions) is complete, the WO will enter pertinent data in the C-CURE 9000 System and issue a 4-digit PIN.

e. Personnel must safeguard their CAC or badge at all times. Loss or theft of a CAC or badge must be reported to the COC immediately and the individual's supervisor.

7-5. Temporary visitor badge (USAREC Form 380-4.1)

a. A temporary (T) badge is provided to personnel IAW the COC Chief's guidance and at the discretion of the watch officer. Personnel issued a T badge must surrender a picture ID card and must wear the badge on their person at all times. The person using a T badge must enter and exit at the main entrance only; the badge is valid for 1 day only.

b. Personnel who do not require an escort (cleaning crews, workforce personnel who forgot their CAC, and prime contractors, for example) may receive a T badge. These personnel may enter and exit the building only at the main entrance.

7-6. Visitor ID badge (USAREC Form 380-4.2)

a. Personnel who visit building 1307 for a designated period of time, will receive a visitor badge to allow the person access to the building while being escorted by the sponsor at all times.

b. The sponsoring organization must provide a by-name list of event participants when feasible. The WO should receive the request 48 hours in advance. When events occur regularly, the WO will issue the sponsor a set number of access cards (no escort).

c. Event access is controlled by the WO and may be requested by memorandum or email to the COC Security Chief or lead WO.

7-7. Very important person (VIP) access

The chief protocol officer is responsible for VIP vetting and escort duties. The COC Chief and watch officer desk personnel will be notified by protocol of all VIP visits, including name of event, at least 72 hours prior.

7-8. Deliveries to bldg. 1307

a. Parcels deliveries (United Parcel Service, Federal Express, etc.) shall be routed and received only at the Mail and Distribution Center. Deliveries at the main WO desk (edible arrangements, flowers, etc.) are routed to the person receiving the delivery. The WO will call the recipient, who must then pick up the delivery at the main desk.

b. The telephone at the COC desk is for visitors, vendors, and guests to contact the sponsor. The sponsor will meet the visitor, vendor, or guest at the main desk. Delivery personnel must be escorted at all times while in building 1307 and will be treated as requiring a Visitor badge.

c. The delivery doors (ground level and loading dock) are always secure and require controlled access by the WO, or the person receiving the delivery.

d. When deliveries or authorized personnel require access through these doors, the delivery sponsor will unlock the doors as required. All vendor deliveries will be handled at the loading dock.

e. Loading dock doors are under video camera surveillance at all times. Personnel requesting access from the dock will identify themselves via intercom and state their business to the WO.

f. After duty hours deliveries, to include weekends will be accepted, provided the delivery POC has made prior coordination with the COC. The delivery person must come to the main entrance. COC personnel will sign for the delivery and attempt to notify the delivery POC as well as the mail-room POC.

7-9. Bldg. 1307 door hours/control

a. The WOs control the activation and de-activation of the door alarm system.

b. Doors are on an automatic timer. The loading dock gate will remain locked at all times.

c. On weekends and holidays, the east, west and northeast doors remain secured.

d. Access to the loading dock cipher door will be limited to those with a need for access. Access will be granted by HQ CMDT who will publish a memorandum listing the name of personnel granted access. The cipher door combination will be changed semi-annually or sooner if the combination is compromised.

e. The WO will control both entry and exit during non-duty hours. Authorized personnel entering the building during non-duty hours will be required to use the north and south main entrances. When contractors or personnel who are not authorized access to the building are required to work during non-duty hours, the directorate will provide a sponsor to ensure that personnel are controlled and perform duties as required.

f. The WO will conduct security checks of all areas of the building as required and conduct random anti-terrorism measures (RAM) when directed by the COC Chief.

7-10. Unauthorized entry/active shooter.

a. If WOs determines that personnel have by-passed the building 1307 access control system and could pose a threat, the WOs will take the following immediate action

(1) Call 911 to report the security breach.

(2) Activate the duress alarm and the C-CURE 9000 system feature for building lock down. A flashing yellow strobe light above each exit door indicates an emergency situation and individuals should not try to enter the building.

(3) Broadcast over the PA system that an unauthorized person/active shooter has entered the building & and all personnel must move to a secure location immediately.

(4) Send an ALERT message to all USAREC personnel instructing them to remain in a secure locked location until told that the area is clear by military police or USAREC leaders.

b. Authorized personnel will not allow other personnel to enter the building behind them without scanning their individual CAC. Personnel observed entering the building and not following the correct procedures will be reported to the WO. Personnel who enter the building by bypassing the access control system will be disciplined if the breach is intentional. A first offense will result in a warning and notification to the person’s supervisor via the Chief, COC. Additional breaches will result in the person’s CAC access being suspended, thereby requiring the person to enter the main entrances for a minimum of seven days.

7-11. Bldg. 1307 CAC entry procedures

a. Hold the CAC approximately 1 inch in front of the card reader, a green light will flash and a beep / click will be heard which indicates successful access. The door will be release for individuals to enter.

b. The second method for CAC entry is to insert the CAC into the reader with the chip up and facing out. A green light will flash and a beep/click will be heard which indicates successful access. The door will be release for you to enter.

c. Heightened security or an elevated FPCON will require individuals to insert the CAC into the card reader, a yellow light will flash and a beep will be heard. Enter the 4-digit PIN followed by the # sign and look for a green light followed by a click. The click noise indicates successful access.

Appendix A
References

Section I
Required Publications

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

AR 25-55
The Department of the Army Freedom of Information Act Program. (Cited in para 4-4a.)

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, 6-5, and 6-8b.)

AR 190-51
Security of Unclassified Army Property (Sensitive and Non-sensitive). (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, 3-9c (6), 4-1, 4-2, 4-3a, 4-3c, 4-4a, 4-6, 4-6c, 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, 3-8, and 3-9c.)

AR 381-12
Subversion and Espionage Directed Against the U.S. 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 700-5
Integrated Logistics Support. (Cited in para 6-5.)

Section II
Prescribed Forms

USAREC Form 380-4.1 (Old UF 1903) Temporary Visitor Badge (Prescribed in para 7-5.)

USAREC Form 380-4.2 (Old UL 1904) Visitor ID Badge (Prescribed in para 7-6.)

USAREC Form 380-4.3 Arming the Recruiter Screening Form (Prescribed in para 2-3).

USAREC Form 380-4.4 (Old UF 810) Emergency Notification Card. (Prescribed in para 6-7a.)

USAREC Form 380-4.5 (New) Suitability Report. (Prescribed in para 2-3b.)

USAREC Label 380-4.1 (Old UL 21) Weapons Prohibited. (Prescribed in para 6-3.)

USAREC Label 380-4.2 (Old UL 24) Laptop Security Awareness. (Prescribed in para 6-10)

Section III
Referenced Forms

SF 52-B
Request for Personnel Action.

SF 701
Activity Security Checklist.

SF 702
Security Container Check Sheet.

DD FM 2875
System Authorization Access Request.

FK FM 5084
Fort Knox Network AUP Agreement.

Glossary

ACS
Assistant Chief of Staff

AIS
Automation information system

CCF
Central clearance facility

CUI
Controlled unclassified information

DA
Department of the Army

DISS
Defense Information Security System

FOIA
Freedom of Information Act

GOV
Government-owned vehicle

GSA
General Services Administration

HQ USAREC
Headquarters, U.S. Army Recruiting Command

IT
Information technology

OPM
Office of Personnel Management

PHS
Physical security

PII
Personally identifiable information

PS
Personnel security

SAEDA
Subversion and Espionage Directed Against the U.S. Army

SM
Security manager

SOP
Standing Operating Procedure

USAREC
U.S. Army Recruiting Command

SUMMARY of CHANGE

USAREC Reg 380-4

Security Program

This administrative revision, dated 24 June 2021.

- Adds the need for USAREC Form 380-4.5 (Suitability Request).

- Changes the For Official Use Only (FOUO) to the Controlled Identified Information (CUI).

- Changes the Joint Personnel Adjudication System (JPAS) to Defense Information Security System (DISS)

USAREC

ELECTRONIC PUBLISHING SYSTEM

DATE:	22 JANUARY 2019
DOCUMENT:	USAREC REG 380-4
SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION