

DEPARTMENT OF THE ARMY
U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
Fort Sam Houston, TX 78234-5005

FSH Regulation
No. 190-13

13 Aug 97

Military Police
SECURITY OF SPECIFIC ARMY PROPERTY

Issue of supplements to this regulation by subordinate commanders is prohibited, unless specifically approved by the Commander, U.S. Army Medical Department Center and School and Fort Sam Houston.

1. **PURPOSE.** The purpose of this regulation is to prescribe policies, procedures, and responsibilities for the safeguard of certain unclassified U.S. Army property, both sensitive and nonsensitive, and to establish standardized, minimum acceptable security requirements for the specified category of U.S. Army property, and to reduce loss, theft, misuse, and damage of Army assets.

2. **APPLICABILITY.** This regulation applies to all commands assigned or attached to Headquarters, U.S. Army Medical Department Center and School and Fort Sam Houston, to include all tenant organizations.

3. **REFERENCES.** Related publications and required forms are outlined in appendix A.

4. **DISCIPLINARY ACTION AND REPORTING LOSS/THEFT**

a. **Military members.** This regulation is punitive in nature. In accordance with (IAW) the provisions and requirements of applicable laws and/or regulations, appropriate action will be taken with respect to the individual(s) responsible for any violations of the procedures and requirements imposed pursuant to this regulation. Failure to perform the requirements of this regulation provides a basis for disciplinary action under applicable laws, i.e., United States Code of Military Justice, Article 91 (Disobedience of a Lawful Order).

b. **Civilian employees.** Department of Defense (DOD) affiliated civilians may be subject to adverse personnel actions in accordance with federal employment laws, or both.

c. **Loss or theft of government-owned property.** Personnel who experience a loss or theft of government-owned property while

on Fort Sam Houston (FSH) will report such losses or thefts immediately to the FSH military police.

d. Loss or theft off the installation. If a loss/theft occurs while participating in exercises off the installation, in a foreign country, or on another installation, personnel affected will immediately report such losses to the local authorities having jurisdiction, and will then report the loss immediately to FSH.

5. GENERAL. Security is a key word which outlines a theme which has direct relevance, and which merits serious consideration in the set up of most organizational routines. In this regulation the primary focus will be aimed at the preventive measures designed to prevent or minimize any security transgressions from occurring. Security and protection must be afforded to all items and matters of value. However, two types of Army property, administrative office machines, to include automated systems (specifically computer hardware) and arms, ammunition and explosives (AA&E), will be highlighted in this regulation. These assets require a blend of procedural safeguards, an interface of physical protection, and audit controls, i.e., physical protective measures, building security, key control, and testing of active electronic security systems. As a minimum, the security procedures and physical protective measures outlined in this regulation will be carried out to safeguard the property.

6. RESPONSIBILITIES

a. The Commander, U.S. Army Garrison (USAG), will establish policies and standards, exercising staff supervision for physical security of government property.

b. Unit/activity commanders will:

(1) Implement physical security of the specified Army property IAW this regulation, and other applicable directives.

(2) Maintain key and lock control, building security, and testing of active electronic security alarm systems within their respective organizations.

7. SECURITY OVERVIEW. With the tremendous momentum of today's technological advances, the computer is now playing an ever increasing role in the government environment. For this regulation, hardware is defined as physical equipment or devices forming a computer, and its peripheral equipment. The protection of computer hardware itself, including terminals (monitor and keyboard), central processing units (CPU), disc drives, printers,

communication modems, analog-based units (a device that processes infinitely varying signals, such as voltage or frequencies), discs, tapes, diskettes/floppy discs, cassettes, card readers, monitors, key-punch terminals, optics-based equipment (i.e., CD-ROM), and laptop computers, is no different than the protection of other equipment and valuables. The proper security measures for these, including locks, etc., are similar to those which can be used for other types of valuable items.

8. **MINIMUM SECURITY STANDARDS FOR OFFICE MACHINES AND COMPUTER HARDWARE.** Computer hardware will be protected by implementing the following measures with NO EXCEPTIONS:

a. Tactfully challenge strangers in the workplace. Be aware of your surroundings, to include the people you may work with on a daily basis. Do not be afraid to ask questions. If you notice someone who is unfamiliar looking around the office, greet them and offer assistance. This way you can find out who they are, but more importantly, they are aware that someone is alert of their presence. Just use good common sense. Soldiers and civilian employees are expected to tactfully approach strangers in the work area for internal security purposes. Employees should notify a supervisor, as appropriate. Only a gross lack of compliance to this procedure would result in possible disciplinary action.

b. Building managers must establish a security education and motivation program. In addition to the Medical Command requirement to conduct ADP related security training, as a minimum twice yearly, it should include awareness training for co-workers on actions and behavior patterns they need to lookout for. If possible, a reward/incentive program with time-off or monetary awards should be implemented, to encourage personnel to come forward with information that leads to an arrest. Attendance documentation of the training will be maintained by the unit/activity Information Systems Security Officer (ISSO) or the Physical Security Officer/Noncommissioned officer.

c. Initiate more stringent key issuance controls. Re-key the office door locks if necessary to prevent access to the facility by non-organizational personnel or personnel who no longer work in that particular area.

d. Align the schedule of cleaning personnel with organizational duty hours, this will prevent access to the facility by non-organizational personnel after duty hours, and will ensure better supervision of office equipment.

e. Purchase cable locking devices. Computer hardware in use in open bay-type offices or areas that have no means of locking a door to secure the equipment within, must be secured with a cable-type locking or other security device. Laptop computers must be secured inside lockable containers, i.e., wall lockers, safes, cabinets, or desks. Under no circumstances will laptop computers be left out in the open, unattended.

f. Standard Form 701, Activity Security Checklist, must be used to conduct an end of the day security check to ensure all doors, windows, and equipment are secured. Management must ensure this internal security function is administered in a fair and equitable manner. If civilian employees perform this function it will be performed during duty hours at the end of the work day.

g. A list of names of personnel that are tasked to work extended hours or on weekends must be submitted to the building manager. Personnel who work extended hours or weekends are responsible for keeping doors secured leading into the building, to prevent access to the facility by non-organizational personnel.

h. Excess equipment must be turned in. The smaller the amount of pilferable equipment, the lower the chance that it will be stolen.

i. Establish regular inventory schedules, this will increase awareness in personnel, and will enable them to detect missing items sooner. Early detection will enable law enforcement personnel to launch a more successful investigation. Additionally, all hand receipt holders must have an affective accountability system with all users of computer hardware (i.e., sub-handreceipt the computer hardware to the individual user). This procedure will enhance the responsibility of the user.

j. Initiate a report of survey. If an investigation of computer hardware theft shows evidence that the hardware was not adequately secured, a DD Form 200, Report of Survey, must be conducted, to determine causative factors that contributed to the loss, highlight weak areas in the security system, and provide alternative recommendations to enhance existing security measures.

9. VULNERABILITY ASSESSMENT. Extravagant and costly security items such as alarms or walk-in vaults are usually not cost-effective for other than mainframe computers and, depending on the local threats, usually are not needed. Physical security requirements must be considered, and selected based on the

sensitivity of the data protected or its vulnerability. If there are concerns about data sensitivity or vulnerability, contact the Physical Security Division, Provost Marshal Office (PMO), for assistance in conducting a vulnerability assessment.

10. **BUILDING SECURITY.** In accordance with FSH Regulation 405-1, Real Estate Control and Utilization, building security applies to individual buildings and/or other facilities under the Real Property Building Manager (RPBM) Program. The procedures and responsibilities are applicable to all RPBMs, directorates, major staff elements, organizations, and tenant organizations located on FSH, and/or subinstallations of FSH, except military housing.

a. An RPBM and an alternate, along with an appropriate building/facility point of contact (POC) will be designated by directors, staff office chiefs, or organizational commanders, for each building or facility assigned to the organization. When practical, the primary duty assignment of the individual designated should be in the building for which they are building managers, assistants, or POCs. When a building or facility is occupied by more than one organization, the building manager will be designated by the major agency. The RPBMs for contractor-occupied buildings will be assigned by the organization that is served by the contractor. The government activity jointly occupying a building with a contractor will assign the RPBM. The individual appointed as alternate will assume the duties and responsibilities of the RPBM in his/her absence.

b. Directors, staff office chiefs, or organizational commanders will provide the PMO written notification of the initial assignment of RPBMs, their alternates or POCs, in memorandum format, to include facility number, and present utilization. This memorandum will be used solely by the military police to contact appropriate personnel in the event a building or facility is found unsecured.

c. It is the responsibility of the RPMB to ensure FSH Poster 42, Notification of Military Police, is posted on the exterior entrances of their respective buildings/facilities.

d. Primary/alternate RPBMs serve as representatives to the major user, and in cooperation with all occupants and users of a building or facility, are responsible for the execution of the major users' responsibilities mandated by FSH Regulation 210-10, FSH Installation Design Guide.

e. Real Property Building Managers, in coordination with all occupants, users, and tenant activities of the building/facility,

are required to establish a physical security plan. This should include publication of rules for the opening and closing of the building/facility during normal duty hours, and for after duty hours admittance, and the security measures that must be observed. Ensure security checks of office areas at the end of the duty day are conducted. These checks will include the locking of windows, doors, offices, and the building itself. These are the minimum requirements. Security checks must be annotated on SF 701.

f. If a building/facility is found unsecured after duty hours, the military police will contact the personnel in the order designated on the notification memorandum. Outdated and incomplete memorandums cause delays in properly notifying the POCs to respond, and ties up the patrols at the unsecured building/facility. Unnecessary detention of police patrols degrades the response to other emergencies.

g. Brief the occupants/users of the building/facility on their collective responsibility for protection of the property, including pecuniary liability for loss and damage in excess of fair wear and tear, unless it is the result of acts beyond their control. Security awareness is everyone's responsibility.

h. Conduct monthly inspections of the assigned building/facility and its installed equipment, with particular attention to doors, windows, lights, and electronic security equipment to determine their functional and operational conditions. Assistance can be provided by the Physical Security Division, PMO, to determine the adequacy of the protective measures.

i. Follow-ups are required on all discrepancies and irregularities that are noted during security inspections or recommendations by the Physical Security Division, to ensure corrective actions are accomplished.

j. Ensure that building/facility occupants/users do not tamper with or adjust any of the electronic security systems

11. **KEY CONTROL AND ACCOUNTABILITY.** Locking devices are useless unless proper key control is maintained. A good lock and key issue and control system is the most essential factor in safeguarding property. Herein are minimum procedures and an established standardized system for the control of keys and locks that secure Army unclassified and nonsensitive property at the unit and installation level. Additional guidance is provided in appendix D, AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive); chapter 3, AR 190-11, Physical

Security of Arms, Ammunition, and Explosives, and chapter 8
FM 19-30, Physical Security.

a. Organizational commanders, or activity chiefs are responsible for controlling and safeguarding all supplies equipment areas within their command/activity.

b. Organizational commanders, activity chiefs, will appoint, in writing, primary and alternate key custodian(s). Units and activities will publish rosters identifying those personnel authorized to draw keys, and have access to designated areas.

c. The key custodian will:

(1) Issue and receive keys that safeguard nonsensitive Army supplies, and equipment below the wholesale level.

(2) Ensure that the alternate key custodian issues, receives, and accounts for keys in his or her absence, and that they clearly understand these control procedures.

(3) Maintain a key control register at all times to ensure continuous accountability for keys of locks used to secure government property.

(4) Be listed on an access roster for the key depository.

d. The following key control and accountability procedures are BASIC to three functional areas of importance to all units/activities; administrative keys, motor pool keys, and keys for AA&E facilities:

(1) Key control register

(a) Keys will be signed in and out on the register those personnel on the key access roster.

(b) Key control registers will contain the printed name and signature of the person issuing the key, the person issued to, date/hour key was returned, and the signature of the individual receiving the returned key. These entries will be completed in pen and ink.

(c) The official document is DA Form 5513-R, Key Control Register and Inventory.

(d) Key control registers will be maintained as outlined in AR 25-400-2, The Modern Army Recordkeeping System.

(2) Key depository.

(a) A key depository is a lockable container, such as a safe or filing cabinet, or a key depository made of at least 26 gauge steel, equipped with, as a minimum, a tumbler-type locking device, and is permanently affixed to a wall that will be used to secure keys.

(b) It will be located in a room where it is kept under surveillance around the clock, or in a room that can be locked during non-duty hours.

(c) The key custodian is ultimately responsible for the security of the key to the key depository. The key will be issued, and signed for on the register.

(3) Key and lock accountability.

(a) Keys to locks in use, which protect property of an office, unit or activity, will be checked at the end of each duty day. Differences between keys on hand, and the key control register will be reconciled. Padlocks and their keys will be inventoried by serial number, semiannually. A written record of the inventory will be retained until the next inventory is conducted. Although the reverse side of DA Form 5513-R provides for the semiannual inventory data entries, it is recommended that a separate memorandum be used to record the inventory, which includes the date the inventory was conducted, and whether any discrepancies were noted, action taken, and signature. When a key to a padlock is lost or missing, an inquiry will be conducted, and the padlock replaced or recored immediately. A key and lock inventory will be maintained which includes a list of the following:

Keys

Locks.

Key serial numbers

Lock serial numbers.

Location of locks.

(6) The number of keys maintained for each lock. This list will be secured in the key depository.

(b) Padlocks and keys which do not have a serial number will be given one. This number will be inscribed on the lock or key, as appropriate. Inventories will be conducted using DA Form 5513-R, and FSH Form 65, Key and Lock Inventory.

12. COMMERCIAL AND JOINT-SERVICES INTERIOR INTRUSION DETECTION SYSTEMS (J-SIIDS). All units and activities that have facilities protected by J-SIIDS and Commercial Intrusion Detection Systems (CIDS) must comply with prescribed procedures, and assign responsibilities for proper use of all J-SIIDS and CIDS installed at FSH and Camp Bullis. The all important task of maintaining around-the-clock protection of personnel, sensitive items, and material in the custody of the Army cannot be over emphasized. The government or commercial electronic alarm systems being used by a unit or activity enhances the physical security protection, and detects attempted or actual intrusions during the absence of personnel. However, to be effective, the alarm systems must be operated by people who are reliable, responsive, and whose identity is known, and kept current. The installation PMO alarm monitor personnel will:

a. Provide 24-hour monitoring of all alarm systems on and off the installation, such as U.S. Army Reserve Centers, Texas Army National Guard Armories, etc., that have a Memorandum of Agreement (MOA) established for that purpose.

b. Inform the military police desk sergeant of the alarm condition. The desk sergeant will dispatch a military police unit, or units, to the facility, if warranted. If the alarm activation is off the installation, the appropriate civilian law enforcement agency will be notified.

(1) In case of an alarm activation, the alarm monitor will telephonically notify individuals whose names appear on the activities' alarm system roster beginning with the first name on the roster, and continuing downward on the list until contact is made. The time, date, and person notified, will be annotated on the alarm sheet.

(2) Maintain a quick reference book of all alarm systems in use. Safeguard rosters as FOR OFFICIAL USE ONLY and in accordance with the Privacy Act.

c. Units and activities will:

(1) Establish and maintain an access roster consisting of no less than four names as POCs for the alarm monitors to contact in case of an alarm activation (format procedures are outlined in appendix B).

(2) Submit a copy of the updated access roster on a memorandum to the PMO, ATTN: Physical Security Division, Building 2250, Stop # 38, Fort Sam Houston, Texas 78234-5038, semiannually, or sooner, if personnel changes occur. Telephonic requests for addition or deletion of personnel on the access roster will not be accepted. Deviations from the memorandum format will not be accepted.

(3) Ensure all names are listed in order of preference, and an indication is made if the individual is to be contacted during duty, or non-duty hours.

d. Individuals will:

(1) Become familiar with their responsibilities in case they are called concerning an alarm activation.

(2) Upon notification of an alarm activation, respond to the alarm location within 30 minutes after notification.

(3) Keep their supervisor informed of current telephone numbers and/or address changes that may cause them to be outside the 30 minute response time.

e. The procedures and standards for testing and inspecting the alarm system are outlined in FSH Form 66-E, Alarm Test Record.

13. CONTROL AND ACCOUNTABILITY OF AA&E: Investigations and incidents involving AA&E, and the guidance on actions to be taken will be as follows:

a. Commanders will immediately notify the FSH military police, whenever one or more of the following incidents occur:

(1) Actual or attempted breaking and entering of an AA&E storage facility.

(2) The loss, theft, or recovery of AA&E

b. The notification will be as complete as possible, but under no circumstances will it be delayed because of incomplete data.

14. CONTROLLED ACCESS TO AA&E. Commanders will ensure personnel undergo complete, and favorable command oriented security screening, and evaluations, prior to authorizing such personnel unaccompanied access to arms and Category I and II ammunition. Criminal records screening will be conducted by the PMO and the local civilian police agency, and must be requested by commanders in memorandum format. The memorandum will contain the full name of the person being screened, to include maiden name and any aliases, the address, the social security number, the date of birth and the place of birth.

a. The screening/evaluation will be recorded on DA Form 7281-R, Command Oriented Arms, Ammunition and Explosives (AA&E) Security Screening and Evaluation Record.

b. It is prohibited to carry, move, or store AA&E in privately owned vehicles. Movement of Category I and II AA&E on or off the installation will be under the supervision of a commissioned officer, warrant officer, noncommissioned officer (E-5 or above), or DOD civilian (GS-5 or above). Armed guard surveillance will be provided when such AA&E are transported off the installation. Movement of Category III and IV AA&E will be under the supervision of a designated responsible individual. Ammunition and explosives will not be left unattended or unsecured at any time.

c. If government vehicles are not available, marksmanship arms and ammunition may be transported directly to or from ranges, matches, and authorized storage locations in privately owned vehicles.

15. PRIVATELY OWNED FIREARMS (POFs). Privately owned firearms will not be carried when performing military duties, or when participating in field exercises. Privately owned firearms stored in unit arms rooms will be stored separate from military firearms, and will be controlled and accounted for in the same manner as is required for military firearms. Guidance and policies on POFs are outlined in FSH Regulation 190-7, Control of Privately Owned Weapons.

APPENDIX A

RELATED PUBLICATIONS AND FORMS

Publications:

- AR 25-400-2, The Modern Army Recordkeeping System.
 - AR 190-11, Physical Security of Arms, Ammunition and Explosives.
 - AR 190-13, The Army Physical Security Program
 - AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive).
 - AR 380-19, Information Systems Security
 - AR 710-2, Inventory Management Supply Policy Below the Wholesale Level.
 - AR 735-5, Policies and Procedures for Property Accountability.
 - FM 19-30, Physical Security.
 - FSH Reg 210-10, Installation Design Guide.
 - FSH Reg 190-7, Control of Privately Owned Weapons.
 - FSH Reg 405-1, Real Estate Control and Utilization.
2. Forms:
- SF Form 701, Activity Security Checklist
 - DD Form 200, Report of Survey.
 - DA Form 5513-R, Key Control Register and Inventory.
 - DA Form 7281, Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record.
 - FSH Poster 42, Notification of Military Police.
 - FSH Form 65, Key and Lock Inventory.

FSH Reg 190-13

FSH Form 66, Intrusion Detection System (IDS) Test/Inspection Record.

3. Appendix B. Example of Access Roster Memorandum

APPENDIX B

Example of Access Roster Memorandum

Office Symbol

Date

MEMORANDUM FOR Provost Marshal, ATTN: Physical Security
 Division, Bldg 2250, Fort Sam Houston,
 TX 78234-5038

SUBJECT: Activation/Deactivation of the Intrusion Detection
 System (IDS), Alarm # _____, Bldg _____ (or address if off
 the installation)

1. The following personnel are authorized to activate/deactivate
 the IDS and to serve as POCs in case of alarm activations during
 duty hours:

<u>NAME:</u>	<u>SSN:</u>	<u>DOB:</u>	<u>DUTY TELEPHONE:</u>	<u>POSITION:</u>
McGee, Martin	000-00-0000	19 May 60	221-XXXX	Commander
Homann, Phil	000-00-0000	13 Jul 68	916-XXXX	XO
Estes, Julia	000-00-0000	11 May 45	221-XXXX	Supply Sgt
Chenu, Jean	000-00-0000	10 Jun 43	221-XXXX	Unit Clerk
Bates, Lester	000-00-0000	11 Jan 23	221-XXXX	Mail Clerk
Sims, Susan	000-00-0000	15 Sep 75	221-XXXX	Secy

2. The following personnel are on-call after duty hours for the
 dates indicated:

<u>DATE:</u>	<u>PRIMARY/PHONE:</u>	<u>ALTERNATE/PHONE:</u>
1-7 Sep 97	1LT Homan/221-XXXX	SFC Estes/221-XXXX
8-14 Sep 97	SFC Estes/221-XXXX	SPC Chenu/221-XXXX
15-21 Sep 97	SPC Chenu/221-XXXX	SPC Bates/221-XXXX
22-28 Sep 97	SPC Bates/221-XXXX	1LT Homan/221-XXXX
29 Sep-5 Oct 97	1LT Homan/221-XXXX	SFC Estes/221-XXXX

3. Duty hours for this unit are 0715-1700, Mon thru Fri.

4. If the primary or alternate POC cannot be contacted, or is
 unable to respond to the alarm, contact the undersigned at _____

Name and Title

FSH Reg 190-13

Office Symbol

Date

MEMORANDUM FOR Provost Marshal, ATTN: Physical Security
Division, Fort Sam Houston, TX 78234-5038

SUBJECT: Activation/Deactivation of Intrusion Detection System
(IDS), Alarm # _____, Bldg _____ (or address if off the
installation)

1. The following personnel are authorized to activate/deactivate
the IDS and to serve as POCs in case of alarm activations during
duty hours.

<u>RANK/NAME:</u>	<u>SSN:</u>	<u>DOB:</u>	<u>DUTY PHONE:</u>	<u>POSITION:</u>
CPT Boss, Ima	000-00-0000	3 Jun 51	221-XXXX	Commander
1SG Kick, Willi	000-00-0000	11 May 50	221-XXXX	1SG
SFC Jones, Rick	000-00-0000	15 Dec 55	221-XXXX	Supply Sgt
SPC Smith, Mary	000-00-0000	1 Jan 50	221-XXXX	Unit Clerk

2. The following personnel are to be contacted in case of alarm
activations after duty hours:

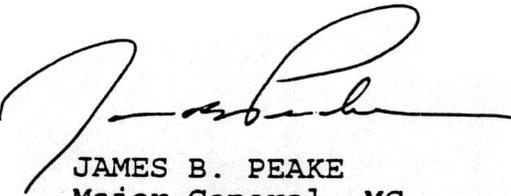
<u>RANK/NAME:</u>	<u>HOME PHONE:</u>	<u>CELL PHONE:</u>	<u>BEEPER:</u>
-------------------	--------------------	--------------------	----------------

SPC Smith
SFC Jones
1SG Kick
CPT Boss

3. Duty hours for this unit are 0715-1700, Mon thru Fri

Name and Title

The proponent of this regulation is the Provost Marshal's Office. Users are invited to send comments and suggested improvements on DA Form 2028, Recommended Changes to Publications and Blank Forms, to the Commander, U.S. Army Medical department Center and School and Fort Sam Houston, ATTN: MCGA-DPS, Fort Sam Houston, TX 78234-5038.



JAMES B. PEAKE
Major General, MC
Installation Commander

DISTRIBUTION:

A
B
C