DEFENSE LANGUAGE INSTITUTE FOREIGN LANGUAGE CENTER AND PRESIDIO OF MONTEREY PHYSICAL SECURITY GUIDE

POM PHYSICAL SECURITY STANDARD OPERATING PROCEDURE
No. 190-13

TABLE OF CONTENTS

1. PURPOSE. To describe policy, responsibilities, procedures and standards for the Physical Security Program at the Installation, unit and activity level.

2. APPLICABILITY.

a. This Standard Operating Procedure is applicable to all units, activities and personnel located at the Defense Language Institute Foreign Language Center & Presidio of Monterey which includes military, civilian, Non-appropriated Fund (NAF) and contractor activities. Its principles are applicable to government property including funds, supplies, equipment, consumables or expendables.

b. Classified and medically sensitive item security procedures are outlined in other appropriate regulations, such as AR 380-5 or AR 190-50. See AR 190-11 for weapons and sensitive items security and Intrusion Detection Systems (IDS), DA Pam 385-64, Ammunition and Explosives Safety Standards.

c. Tenant and NAF activities subject to regulatory requirements from their higher headquarters will follow such guidance. Contractors will follow contractual agreements and/or guidance promulgated by the Presidio of Monterey. In any area where specific guidance is lacking, this Physical Security SOP will prevail.

d. "Supplementation of this SOP by Units, Activities and Personnel is not permitted."

3. POLICY.

a. Commanders, supervisors and individuals responsible for the use, transport, accountability, security or possession of government property, will ensure adequate security, is provided for that property at all times. If doubt exists, Presidio of Monterey Police Department Physical Security Branch will determine what the "approved standard" will be. The standards set forth in this SOP are minimum requirements. Checklists provided in Appendix A of this SOP contain questions to ensure compliance with minimum standards. In the absence of specific guidelines commanders, supervisors and individuals, will exercise prudent judgment and employ whatever measures are available that will reasonably safeguard government property from any possible loss, compromise or destruction. Construction standards set forth in this SOP apply to new work, modifications or repairs. Existing structures and standards will not be changed to conform to this SOP, unless approved by Presidio of Monterey Police Department (POMPD) Physical Security.

b. Physical Security measures employed must be adequate, reasonable and economical. They must prevent or retard unauthorized access to information, material/equipment, and prevent interference with the operational capability of the installation. When deficiences exist, commanders must initiate reasonable protective measures until the deficiency is corrected. The submission of work orders alone may not be sufficient. 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. Nonstandard methods and devices must be approved by the Physical Security Branch to ensure there is a resistance or surveillance factor equivalent to that of an approved standard.

c. Great care must be exercised to ensure security is not sacrificed for the sake of convenience. Protection of the Government's interest and loss prevention is the goal of this Physical Security SOP. Inefficiency, procrastination, fraud and abuse lead to losses and create crime conducive conditions. Detection and prevention can only be accomplished if all concerned are alert and pro-active. Commanders, Directors, and supervisors are charged with ensuring compliance with the terms of this Physical Security SOP within their areas of responsibility. Failure to do so may result in pecuniary liability or other adverse actions should losses occur or if violations are discovered.

4. RESPONSIBILITIES.

a. The Installation Commander will appoint a Physical Security Council comprised of concerned members of the Directorate of Law Enforcement (DLE), Directorate of Public Works (DPW), Directorate of Resource Management (DRM), Directorate of Security (DSEC), Directorate of Logistics (DOL), Criminal Investigation Division (CID), and other units and activities as deemed appropriate or necessary.

b. The Installation Physical Security Council will be chaired by the Deputy Garrison Commander. The council will meet annually or as otherwise directed to review the security policies and posture of the installation. The Council may establish budgetary and policy priorities for all matters related to security on the Presidio of Monterey, ensuring such priorities are properly considered at the Installation Master Planning Board, or Working Program Budget Advisory Committee.

c. The DLE Physical Security Branch will:

(1) Serve as the principal staff agency for the Physical Security Council.

(2) Maintain and update the Installation Physical Security Plan (PSP).

(3) Program and conduct periodic/annual Physical Security Inspections and Physical Security Surveys of the Complex, Mission Essential/Vulnerable Areas (MEVA) and other activities to remain cognizant of security changes or requirements impacting those areas.

(4) Manage the Installation Intrusion Detection System (IDS).

(5) Provide Commanders and unit Physical Security personnel with support and guidance on Physical Security matters as needed.

(6) Plan, direct and manage the Installation Physical Security Program in its day-to-day operation, to include monitoring new construction/renovation projects/plans to ensure Physical Security features have been included.

d. The Director of Contracting (DOC) will ensure that requests for contracting action, which are security related, i.e., lights, CCTV, fencing, vaults, IDS etc., are returned without action if prior

coordination and approval have not been made with DLE Physical Security. Requests for contracting action related to classified information or equipment purchases shall be coordinated with DSEC before processing.

e. The Director of Logistics (DOL) will ensure that no equipment purchases for security items such as, caging, safes etc., are made without prior coordination with DLE Physical Security Branch. Classified equipment purchases will be coordinated with the DSEC before processing.

f. Commanders and heads of activities/units are responsible for

(1) Reviewing appropriate portions of this Physical Security SOP and implementing its standards within their organizations. Work orders for maintenance or purchase of security devices will be coordinated through DLE Physical Security prior to submission to DPW, DOL or Contracting.

(2) Unit Commanders/Activity Managers will appoint in writing, a unit Physical Security Officer/NCO in the grade of E6 or above. Alternates may be in the grade of E5. Civilian appointees should be in the grade of GS-5 or above, and have direct access to the Commander/Director or activity head.

g. Unit Physical Security Officers/NCO's will conduct walk-through visual inspections of all unit/activity buildings, sheds, storage rooms and areas on a periodic basis to ensure operating personnel are aware of standards and policy, and that they are in compliance with those standards. If applicable, the checklists should be used when conducting walk-through inspections. Other similar inspections should be conducted before weekends/holidays to ensure the area is prepared and secure. Commanders may designate other unit personnel to conduct these inspections. Discrepancies and suggestions must be reported to the unit commander in a timely manner to ensure they can initiate appropriate corrective action. Seek advice and guidance from the DLE Physical Security Branch. See Appendix A, for samples of checklists.

h. In cases where buildings and areas are shared by multiple units or activities, one unit/activity will assume overall responsibility for security matters therein. This unit will be referred to as the landlord. All others will be referred to as tenants and, will defer to the landlord all questions of security. Landlords will establish an SOP which outline responsibilities, security measures, lockup procedures, access controls, key control, and emergency responses to bomb threats, fire, unsecured buildings etc. Coordination must be made between occupying unit/activities.

5. EXCEPTIONS TO POLICY. Exceptions to the provisions of this SOP may be granted on a case-by-case basis when correction of a deficiency is not feasible, or when security afforded is equivalent to, or better than that provided under standard criteria. All requests for exceptions will be routed directly to the DLE, Physical Security Branch for consideration and approval.

6. PERIMETER BARRIERS.

a. A perimeter barrier is a medium which defines the physical limits of an installation, area, building or room; and, which restricts or impedes access thereto. Perimeter barriers may be of two general

types, natural or structural. The installation perimeter barriers for the Complex generally consist of both types, with large portions of the perimeter being without substantial structural barriers. When needed, standard 9-gauge aluminized chain link fencing, with a 7 foot fabric topped by a three strand barbed Wire top guard (FE-6), will be used in all fencing applications. Periodic inspection and maintenance of the installation perimeter barriers and fence lines is the responsibility of DPW. See Appendix B, for examples of fence details.

b. The structural perimeters of individual activities and buildings should be defined and points of general access identified. Periodic inspection and identification of needed repairs to these perimeters is the responsibility of unit commanders and activity heads.

c. Openings in perimeter barriers (windows gates, doors etc.) will be kept to a minimum. All openings or entrances will be secured when not in use. Openings, such as windows or doors, that are not needed, or necessary for emergency exits or environmental purposes, should be locked or blocked/covered by screens or similar material. Other openings, such as vents and utility holes, greater than 96 square inches, through which unauthorized access to a building or area might be gained, will also be blocked/covered as necessary. Air conditioners and vent covers will be secured to the structure. When plywood covers are used, they will be at least 1/2-inch thick, secured to the structure by carriage bolts. The interior ends of the bolts will be secured with nuts that are peened or otherwise secured to prevent removal. Steel mesh or wire coverings must be 10-gauge expanded metal or wire mesh or, 9-gauge chain link aluminized fencing, on a metal frame that is secured to the structure by carriage bolts as described above; or, by another approved method. See Appendix C, of this SOP for an example of a standard window screen installation.

d. As much as possible, one door to an activity will be designated as a lockup door. This door is the first opened and the last closed, all other doors will be locked from the interior of the building using slide bolts, hasps, etc. All exterior doors will, at a minimum, be 1-3/4" solid or laminated wood, and be secured by locking devices as indicated above. The exterior lockup door will be secured by locking devices which have a 1-inch throw deadbolt. Deadbolts will be 5/8" x 7/8" with a concealed hardened steel roller. The use of double cylinder lock sets is not approved except in classified areas. Anti-friction lock sets or inter-lock sets with deadbolts must conform to the ANSI A156.13 Standard. Existing doors will be secured as prescribed by this

paragraph and will not be secured solely, by the key-in-knob locks. Strike plates will use plate reinforcements that are secured with 3" screws. Cylinder rings will be provided with hardened steel inserts.

e. Other exterior doors which are not solid core (with the exception of commercial aluminum and glass doors) must be secured in an approved manner, i.e., thin panels will be reinforced with plywood on interior sides; glass panels in thin wooden doors will be covered by screens or plywood. In lieu of reinforcement, paneled doors will be replaced by solid core wood or metal doors. Commercial aluminum framed or steel doors, with or without glass panels, will be secured by approved panic devices; mortised, heavy duty laminated hook bolts; or, other approved hardware. See Appendix D, of this SOP for examples of approved and non-approved locks, padlocks, and hardware.

f. No brass shackled or brass bodied locks will be used for exterior applications on gates, doors, or in conjunction with hasps. Only approved case hardened padlocks and devices will be used to secure government property (except in those areas where non-spark brass is required by safety regulations). (See Appendix D)

g. Padlocks on gates or exterior doors should be protected against force by use of metal shrouds. Where this is impractical, hasps and staples should be of substantial construction and be firmly affixed to the structure or gate. Padlocks will be secured to the companion staple when not in use, or, will be secured and controlled by the individual with the key. Padlocks and hasps will not be used on any door which may be used for fire exit or emergency purposes. Approved panic hardware will be used in all such cases. (See Appendix D-4)

h. Double doors, not otherwise securely locked, will have deadbolts/cane bolts (1/2-inch diameter or larger) installed on interior sides of one or both doors, top and bottom, with a minimum throw (recess) of l-inch. Flush/extension bolts built into doors are acceptable devices, although not as strong. Dutch doors will be secured in a similar manner. The use of padlocks and hasps alone is insufficient for Dutch doors. Security devices must be installed that connect the two halves of Dutch doors, as well as the top and bottom (header and threshold) of each half. The use of Dutch doors should be strictly limited. An astragal of metal should be firmly affixed to the exterior of any door(s) which have a gap between the door and frame (or other doors as in the case of double doors), through which the lock or latch may be attacked or manipulated. Astragals should run the length of the door, top to bottom or side to side; but, if impractical, for the sake of cost not less than 24-inches when used in vertical applications.

i. The use of wire mesh or chain link covers on windows or other openings (10-gauge metal or 9-gauge chain link), unless otherwise specified by Regulation, will be limited if more economical means can be used, i.e., the use of key operated sash locks or sash pins (see pages D-2, and D-3, Appendix D, of this SOP). Depending upon the threat, the criticality of the property, and the vulnerability of the activity, such

screens may be necessary. Screens that are capable of swinging outward to open and to facilitate maintenance, will be locked in an approved manner on interior sides.

j. Panic hardware used on doors will be of the type that allows instant exit in case of emergency However, where devices used are not lockable, they will be applied only to solid doors that have no windows. Every precaution will be taken to protect non-locking latches from manipulation. If doors are locked or chained together after duty hours, special precautions must be taken each duty day to ensure exit doors are open and functioning properly. Exit doors in troop billets or activities where personnel are working or living around the clock will not be padlocked or chained.

k. The preferred panic devices are those with vertical rods (extension bars) to the top and bottom of one or both doors. With any door, the locking devices may malfunction if not properly installed. Deteriorated and abused doors are another cause of malfunctions. Responsible unit/activity personnel should be continually aware of the

condition of doors and locks. See page D-4, Appendix D, of this SOP for examples of panic hardware.

l. An internal lockup procedure will be implemented in each building and activity. Personnel will be assigned to this duty at the beginning of each duty day, ensure that all doors are unlocked and prepared for emergency exit, if necessary and, at the end of each duty day, ensure all doors, windows and equipment are secured.

m. Exterior door/gate/window hinges that are not already protected, will be welded, peened, bradded or otherwise pinned to prevent easy removal. See Appendix E, of this SOP for examples of security hinges.

7. KEY AND LOCK CONTROLS.

a. All units and activities will establish minimum key and lock control measures as described below. These measures are applicable to administrative keys only. Control measures described in other pertinent regulations for sensitive items and medical or classified items have precedence. In the absence of guidance elsewhere, the minimum standard measures described herein are to be applied in every case.

b. Administrative Controls.

(l) A key and lock custodian and alternate(s) in the grade of E5 or GS-5 or above, will be appointed in writing. Custodians and alternates shall be responsible for the proper accounting and security of all keys to the activity. Persons without unaccompanied access to property and storage areas will not be appointed as custodians or alternates. In those cases where keys must be available at any time, authorized Charge of Quarters (CQ), or Staff Duty Officer/Staff Duty Noncommissioned Officer (SDO/SDNCO) may be designated to secure, issue, and/or receive keys.

Under no circumstances will personnel who have been relieved of duty or who are subject/pending disciplinary action be assigned as CQ or SDO/SDNCO duties with unaccompanied access to unit keys and property. To the greatest extent possible, CQ personnel should not be given unaccompanied access to activity or government property keys. Their sole function should be to provide surveillance of the area and monitor access to the locked containers in which property keys are stored.

(2) Where multiple functions exist within an activity, multiple custodians/alternates may be assigned, with separate key boxes and functions at each level.

(3) The number of personnel authorized to possess and use keys will be limited to those persons who have an absolute need, as determined by the unit commander/supervisor responsible. Persons designated to have access to a key system or separate keys therein, will be identified in writing. Access forms will show the name, duty position, and key number/area authorized. The access form should be kept by the custodian/alternate who issues keys for ready reference.

(4) No keys for locks protecting government property will be issued for personal retention or removal from the installation. Keys for office buildings and individual rooms in troop billets may be issued

for personal retention. Keys for maintenance buildings, supply buildings/rooms, motor parks and property storage areas will be secured after duty hours in the custody of an established SDO/SDNCO; or, in an approved depository. Arm Room keys will be secured separately from all other items.

(5) All keys, when not in use, will be secured on the person to whom assigned, or be secured in lockable container, such as a safe, filing cabinet, or key depository made of at least 26-gauge steel, that is equipped with an approved 5-pin tumbler locking device or combination lock/padlock. Depositories/containers that are easily removed will be securely affixed to the structure. The key depository will be located in a room where it is kept under surveillance around-the-clock, or in a room that can be securely locked during non-duty hours.

(6) Portable key containers will be secured, when not in use, in locked steel cabinets or safes. Other methods for securing portable key containers must be approved in writing by the DLE Physical Security Branch. Requests for approval should be made on a standard Memorandum which describes the container, the procedures in use, and the reasons for exception.

c. Accountability Procedures.

(1) All keys in the possession of a unit/activity will be strictly accounted for at all times. A complete written inventory of all keys by serial number and location will be maintained on a Key Control Register and Inventory DA Form 5513-R. The form will be retained by the Key Custodian until major changes occur and a new one is made out, at which time the old form may be destroyed. See Appendix F, of this SOP for an example of this form.

` (2) A monthly visual inventory count of all keys in the system will be conducted by the custodian/alternate. The count will be recorded on DA Form 5513-R, Monthly Key Control Register and Inventory. The completed form will be kept in unit files for one year. See Appendix F, of this SOP for an example of this form. On a semi-annual basis, a 100% serial number inventory of all keys in the system will be conducted by the custodian/alternate. Personally retained keys will be returned to the key custodian during each monthly inventory for accountability.

(3) Monthly and semiannual inventories of keys, to include daily changes, will be recorded on DA Form 5513-R. In cases where keys are maintained by the CQ and SDO/SDNCO on a 24-hour basis, a single line on DA Form 5513-R Key Issue and Turn-In, may be used to record the inventory. DA Form 5513-R will be kept in unit files for one year after completion, at which time it may be destroyed. See Appendix F, of this SOP for an example of this form.

(4) Keys issued for personal retention and daily use will be signed out on a separate DA Form 5513-R Key Issue and Turn-In, which will be maintained by the Custodian.

(5) A daily 100% visual count of all primary keys (those operational keys secured in the daily use key box/depository) will be conducted by the custodian/alternate at the start of each duty day and prior to any keys being issued. The inventory count will be compared against the closing visual count that was annotated on DA FORM 5513-R as

the last entry for the previous day. 24-hour sign out/in logs will be closed at 2400 hours each day. Discrepancies between the closing and opening inventory counts will be investigated and resolved before issuing any keys. Keys that are still out should be accounted for prior to closing. In those cases where CQ and SDO/SDNCO are securing and issuing keys on a 24-hour basis, inventories will be conducted by those personnel whenever a change of custody occurs between them. These inventories will be recorded on the DA Form 5513-R which is retained at the depository site.

(6) Duplicate keys may be secured at the unit's next higher headquarters if desired, otherwise, they will be secured in a separate container/sealed envelope or safe in the unit area. Duplicate keys may be secured with other items in the same container provided the keys are in a separate box, envelope, or similar container, sealed, with the quantity listed on the outside. Duplicate keys can be inventoried by container, provided there is no evidence of tampering with the seal.

(7) Duplicate keys secured at the next higher headquarters, or in the unit safe, do not have to be inventoried daily, but must be inventoried by the custodians during monthly and semi-annual inventories.

(8) Key control records will be secured with the custodian. Key sign out/in logs may be secured in the key box/depository. Access to these documents must be controlled in order to guard against tampering. The use of whiteout or correction tape is not authorized, Instead, errors will be lined out and initialed and the next line used.

d. Lock and Combination Controls

(1) Combinations to padlocks and safe locks will be strictly controlled and protected to prevent loss or compromise.

(2) Combinations will be recorded on SF Form 700 (Security Container Information). The information copy of the form will be posted inside the container/vault, out of direct view by the public whenever the container is open. The form may be destroyed upon change of the combination. See Appendix F, of this SOP for an example of this form.

(3) The record copy of the combination will be sealed in the envelope provided.

(4) The envelope will be sealed in such a manner that will allow easy detection of any attempt to open the envelope.

(5) The sealed envelope will be secured at the next higher headquarters

(6) In case of loss, theft or compromise of a lock or combination, the lock will be changed. In addition, changes of combinations will occur annually; or, upon relief or rotation of the person possessing the combination. Lock rotation or replacement should be considered under similar circumstances.

e. Locking devices/padlocks and hasps. See Appendix D, of this regulation for examples of such devices.

f. Lock replacement or repair must be identified by the unit on a Navy Form 9 (Work Request) to the DPW. High security padlock and cylinder repair is accomplished by the General Equipment Repair Shop, Units may coordinate directly with that shop for work. Replacement or repair of IDS control panel locks and keys must be coordinated with the Physical Security Branch first.

g. With the exception of DPW utility room access, the use of master keyed lock's and set locks for the security of government property is prohibited. In the case of existing buildings (such as troop billets), where master locking systems may have been installed, office doors and supply rooms in those buildings will have the locks changed to ensure government property areas are on a separate key system from that of personal property and rooms. CQ personnel will not be given building master sets for government property unless a clear and immediate mission requires it. DPW projects will ensure that no future installation of locks use a master key system involving government property areas. In troop billets, personal room locks may be individually keyed and mastered to the building master only.

8. BUILDING SECURITY CHECKS.

a. Unit/activity Physical Security Officers/NCOs will perform security checks of storage and unit areas on a periodic basis.

b. After duty hours, unit/activity security personnel (CQ/SDO/SDNCO) will perform periodic security checks of all unit/activity storage areas IAW established SOP's.

c. When closing a building at the end of a duty day, designated persons will make a security check of the building to ensure all doors, windows and other openings are properly secured. SF Form 701 (Building Security Check Sheet) will be posted at the lockup door. The completed form will be kept in unit files for 90 days. See Appendix F, of this SOP for an example of this form.

d. All buildings, used principally for the storage of government property, will have an emergency notification card posted on all entrances of the building or on gates leading to the building. Notification cards will be no smaller than 3"x5"; and, will have the following printed thereon:

“IN CASE OF EMERGENCY OR IF BUILDING IS FOUND UNSECURED NOTIFY FEDERAL POLICE AT: 242-7851/52/53"

e. Notification cards will not contain the name, address or home telephone number of responsible personnel. Police numbers will be the only numbers used. Police numbers will not be used for buildings/activities that which have military personnel assigned as CQ or SDO/SDNCOs. In case of emergency only CQ, SDO/SDNCO or police personnel will call response personnel, who in turn, before responding, will call back to verify the existence of an emergency.

f. Emergency notification numbers of response personnel will not be given out over the telephone to unknown persons/callers.

9. PERSONNEL ACCESS AND CONTROL.

a. The Presidio of Monterey and the Annex is operated as an open post. The post should be closed only when necessary to protect Army assets from sabotage and destruction, on in protecting personnel from terrorist actions.

b. Unaccompanied access by non-DOD personnel to unit areas, such as barracks and storage areas, will not be granted. Such visitors must have an escort from the unit, or have clearance from the unit or activity Commander to visit the areas unaccompanied. This precaution should apply to non-unit DOD personnel as well. Police and fire personnel are exempt from this provision during the performance of their official duties.

c. The use of access lists from various installation staffs is not to be construed as unlimited access. Regardless of any access roster provided, such personnel will coordinate with the unit Command before entering the unit area. In case of unannounced inspections by DLE or IG personnel, the identification of such personnel will be verified before they are allowed access, either by phoning their headquarters, or upon presentation of authorized DA Credentials.

d. The identity and destination of visitors in work areas, spaces, rooms or buildings, should be ascertained. No such individuals should be allowed free access to the facility or area, or to find their own way. They will be challenged and escorted to a supervisor or Command Post where their access need can be verified.

e. Activities will arrange office spaces (if possible) to ensure active public entrances or gates are under surveillance, and that visitors can be identified, escorted or otherwise assisted. Common areas, such as snack and vending rooms, will be controlled or be under observation to the greatest extent possible.

f. Visitors entering through unmanned gates or entrances will be warned by posted signs before entering, and/or restrictions they may be subject to as a condition of entry.

10. MATERIAL CONTROL.

a. Personnel and vehicles entering, exiting or traveling within the boundaries of the POM Complex are subject to search or inspection when authorized by the Installation Commander or other appropriate official, such as subordinate commanders, U.S. Magistrates or Military Judges, in accordance with established laws and regulations.

b. Commanders or supervisors working with vendors/contractors will provide such persons with adequate guidance concerning the security of their property and that of the U.S. Government. Care will be taken to ensure that contractor property is not mixed with government property. Areas will be designated for the consolidation of contractor tools and materials. Security of contractor construction sites will be provided for in contractual agreements, and should include direction for the marking and recording of serial numbers, registration procedures, on-site security guards, lighting and fencing for the site.

c. Government property will not be removed from the installation without proper documentation or authorization, such as hand receipts, property pass, or other similar documentation. Responsible officials will ensure drivers, or other individuals in possession of government

property, obtain the proper documentation prior to exiting the installation. These conditions may be exempted during military unit training conditions.

d. Hand receipt holders and/or operating personnel must be cognizant of the condition and disposition of property in their area on a daily basis. Visual inventories should be conducted each duty day and at the close of business before weekends/holidays. Failure to be aware of what property is present: its condition or location; or, to see it only during periodic inventories, invites losses and makes timely detection of losses more difficult. Commanders, supervisors, NCOs and managers, must become active and aggressive with property control and security. AR 710-2, outlines the Command Supply Discipline Program (CSDP). Commanders, supervisors, NCOs and managers responsible for property, should become familiar with this program.

e. Classified shipments will be IAW applicable regulations.

f. Locks and seals will be used on all shipments to the greatest extent possible. Seal accountability will be IAW AR 190-51.

11. PACKAGE CONTROL.

a. Packages, containers, carrying cases and similar items within the boundaries of the POM Complex are subject to search of inspection when authorized by the Installation Commander or other appropriate official, such as subordinate commanders, U.S. or Military Judges and Magistrates, in accordance with established policies.

b. Mail packages are subject to search under either DOD Army or DOD Postal regulations.

c. Commanders and heads of activities are responsible for establishing package controls to minimize the loss of property, and to preclude sabotage and/or espionage.

d. Activities should provide procedures for the control and restriction of employee owned packages at the work place (excluding lunch items). Employees should, upon entering and upon leaving the work place, inform supervisors of the contents of privately owned packages brought into the work place. Activities should provide suitable and secure locations for personal lockers and package storage areas.

12. VEHICLE CONTROLS.

a. When parked, such vehicles will be locked and the ignition keys removed by the responsible person or dispatch office. Windows will be rolled up and locked.

b. Contractor vehicles authorized entry to the installation will conform to installation policy and regulations.

c. The operation, storage and parking of POV's on the POM complex will be IAW with established policy.

13. PILFERAGE CONTROL.

a. Commanders and supervisors should ensure one individual does not have control over all transactions, such as shipping, ordering,

receiving and transport. Limit Blanket Purchase Authority (BPA). Ensure BPA officials do not also control inventory and accountability.

b. Ensure trash disposal activities are monitored.

c. Employ spot checks for cargo vehicles.

d. Mark all tools and high value equipment as U.S GOVT., or U.S PROPERTY. The practice of hot branding vehicle tires or the use of paint to mark tires is not authorized. A yellow, chemically self-vulcanizing label marked U.S GOVT. (NS 2640 01-108-7256) will be used.

e. Employ frequent unannounced inventories of property and records.

f. Establish effective package controls for employees.

g. Prevent employees from parking POV near doorways and docks.

h. Establish appropriate perimeters and control of gates and doors.

i. Investigate actual or suspected losses immediately.

14. SIGNS.

a. Conditions of entry, and warnings pertaining to search and seizure while on the installation, will be posted at entry control points of the installation boundary.

b. To minimize unauthorized entry or trespassing, and to assist in the prosecution of offenders, the boundary of the installation will be clearly posted with signs at such intervals that at least one sign will be visible from any approach to the boundary. Such signs are a DPW responsibility.

c. Restricted Area signs will not be used unless authorized by the appropriate regulation or as designated by the Installation Commander. To prohibit entry to areas where use of the term "Restricted Area" is not authorized, use the term "AUTHORIZED PERSONNEL ONLY", instead.

d. Storage areas and buildings will be posted with appropriate signs directing visitors to the proper entry point.

15. PROTECTIVE LIGHTING.

a. Protective lighting is a primary aid to security. The degree and intensity of lighting will vary according to circumstances and locality. As a general rule, the following will be considered:

(1) Lights of sufficient intensity at main gates and entrances that are controlled by security or responsible activity personnel.

(2) Lights over all lockup doors.

(3) Lights for restricted areas and sensitive item storage.

(4) Lights along remote buildings and interior fence perimeters and, in parking lots for Crime Prevention purposes.

(5) Exterior lights on buildings that are exposed to breakage will be provided with lens covers/screens.

b. Specific lighting requirements will be established by DPW and DLE.

16. SECURITY OF FUNDS.

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

(1) Adequate storage sites and containers, with limited access to fund storage areas, and keys, are in effect.

(2) Adequate cashier's cage or disbursement point.

(3) Adequate armed guards and procedures for the transportation of the funds and negotiable instruments.

(4) IDS for fund storage sites and duress alarms for cashiers, with IDS signs posted on the entrance to the alarmed room. Signs will be posted on exterior walls only if the alarmed area/room has an exterior wall.

(5) Established funds handling procedures will be followed.

(6) Proper fund custodians appointed, with separation of functions and or access.

(7) Written authorization for change funds and size thereof.

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 NAF funds in excess of $200.00, will be secured in a tool resistant safe that is provide with a built-in three position dial combination lock that is equipped with a re-locking device. GSA approved security containers with Underwriter's Laboratory (UL) 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 $500.00. GSA approved Class 3 through Class 6 security file containers, weighing in excess of 750 pounds, will be used for the security of funds that are over $500.00, but not in excess of $3,000. Security file containers are authorized for fund storage only when there are no better containers available and when purchase of new tool resistant containers would not be cost effective. See Appendix G, of this SOP for examples of security containers and UL-Ratings. Fund containers will be secured in a locked room/building of a secure storage structure as described in AR 190-51; or, be in a room or structure that is under constant surveillance of duty personnel.

(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 money being secured within, will not be purchased solely to conform with this regulation. Two-drawer Class 1, 2, and 6, security containers, and, Army Field Safes with built-in combination locks, should be used for funds in these amounts. The storage containers must be secured in a lockable room of a lockable structure or building as approved by DLE. The use of small portable cash boxes for secure overnight storage is prohibited, when portable cash containers are used during duty hours, such as in dining facilities or at NAF cash collection points, they will be kept under the control and surveillance of the cashier. When not in use, or when business is completed, the boxes will be locked by padlocks or built-in locks, and will be further secured in approved safes or containers in an approved structure as described in AR 190-51. If doubt exists, DLE Physical Security should be contacted.

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

(4) Safes weighing less than 750 pounds will be secured to the structure by approved methods. Hardened steel padlocks are approved for use. One method is to secure the safe to the structure by use of steel eye-bolts anchored in the floor, with short lengths of chain (5/16 thickness) beneath the safe that are secured to the anchor by Harden Steel padlocks; or, by welding the safe to the anchor. Safes that are on wheels will have the wheels removed or will be bolted/secured to the structure wall or floor.

(5) Approval to secure appropriated funds in government offices or buildings must be obtained in writing from the Installation Finance Officer. Funds will be kept to a minimum when overnight storage is necessary and, only in those amounts necessary to support a change fund. Fund custodians will ensure that adequate measures are put into effect to have all cash receipts or other negotiable instruments, that are not authorized for overnight storage, deposited without delay.

(6) Structural and security standards will be approved by DLE Physical Security Branch before funds are secured on an overnight basis. NAF approved funds must be identified to DLE for inclusion in the Installation Physical Security Plan.

(7) All cashiers and register points with change funds in excess of $200, will have duress alarm installed for their use. Full IDS will be considered for any site storing in excess of $500, if alternative security measures cannot be met.

(8) Keys and combinations to locks and fund safes will be safeguarded IAW this regulation SF Form 702 (Security Container Check Sheet) will be affixed to each fund safe, and will be annotated each time the safe is opened and closed. See Appendix F, of this SOP for a sample of this form.

(9) Safes shall be secured in rooms with lockable doors. Windows and other openings will be limited. If needed, such openings will be locked, covered or sealed, in an approved manner.

(10) Authorized signature stamps/dies, validating stamps or indicia plates, used to certify/authorize checks or money orders, will

be accounted for at all times, and will be secured in the fund safe or other secure container at the close of business each day. Blank checks, money orders or bonds, will be secured in a burglar-resistant safe, vault or container. If such safes, vaults or containers are not available, a Class 3 through Class 6, four drawer security file/container will be used. Books of account, vouchers and related financial paperwork, may be secured in the same container as the items described in this paragraph, in separate drawers or files or, they will be secured in other lockable containers or field safes.

(11) Responsible officers/fund custodians will coordinate with the Installation Finance Officer to have a cash verification check conducted as appropriate.

17. TACTICAL RADIOS AND COMMUNICATIONS EQUIPMENT.

a. Unless specified in writing by the Installation Commander, tactical radios and portable communications equipment will be secured in the following manner.

(1) Locked in a secure building or vehicle as described in AR 190-51 or:

(2) Secured to a vehicle by a 5/16-inch chain and approved padlock.

b. During transport by commercial means, commanders will coordinate with the Transportation Office to ensure maximum consideration is given to proper packing and protection of shipments, particularly those that are not under surveillance or military control.

18. INDIVIDUAL RELIABILITY PROGRAM (IRP).

a. General

(1) The IRP is applicable to all personnel whose duties require unsupervised, unaccompanied access to arms, ammunition and explosives (AA&E), or other sensitive items storage facilities. Duty positions requiring entry into the IRP include the following.

(a) Unit Armorers and Assistant Armorers.

(b) All personnel (authorized by commanders/supervisors of civilian personnel) to receive ammunition from the ASP, which is located in Ft Hunter Liggett.

(c) Any other unit soldier the commander requires to have unaccompanied access, such as First Sergeant, Supply Sergeant, and Physical Security NCOs.

(2) The IRP is not required for Commissioned Officers, Warrant Officers or DA Civilian (GS-09 or above).

(3) Units/Organizations will restrict the number of personnel requiring unaccompanied access to AA&E and sensitive items to the absolute minimum consistent with operational necessity.

b. Commanders/supervisors of civilian personnel are responsible for:

(1) Implementing the IRP IAW the provisions of this SOP.

(2) Select individual(s) within the organization identified in para 18a above to undergo IRP screening.

(3) Ensure record screening (as described below) is accomplished at unit/organization level. A sample format for record screening requests is shown in Appendix F, of this PS SOP.

c. Individual's Personnel Records indicate positive and negative information, such as awards, letters of appreciation/commendation, previous assignments involving sensitive duties, reductions, letter of indebtedness, and/or record of alcohol or drug related problems; or, any indication of maladjustment socially or emotionally.

d. Unit/organization Legal files. Record information concerning previous/pending UCMJ action(s).

e. Individual Medical Record. Record information indicating medical problems that may affect the individual's ability to perform duties under the IRP.

f. Ensure that the request for local files check of available records at Presidio of Monterey is submitted to DLE, SJA, DSEC and CPO (civilian employees only).

g. Conduct a review of information obtained in paragraph 18c thru 18e above, and through personal interview make an assessment of the reliability, trustworthiness, and suitability of individuals nominated for the IRP.

h. Make the final determination of which individual(s) will be in the IRP.

i. Ensure local files checks are conducted every three years for IRP personnel. Designate a unit/organization IRP representative to assist in the implementation of the program.

j. Ensure personnel entered into the IRP are trained and thoroughly familiar with their responsibilities to safeguard AA&E or sensitive items IAW AR 190-11, AR 190-51 and Physical Security SOP.

k. Directorate of Law Enforcement is responsible for:

(1) Conducting the check of local law enforcement files.
(2) Forward adverse information concerning the IRP applicant.

l. Staff Judge Advocate Office (SJA)

(1) The Criminal Law section of the SJA will provide available information concerning previous UCMJ action(s) against IRP nominated personnel.

(2) Forward to the requesting unit/organization a summary of any UCMJ action on file.

(3) SJA Labor Counsel will advise CPO regarding the processing of civilian personnel disqualified from the IRP.

m. Civilian Personnel Office (CPO)

(1) CPO will request action for local files checks on DOD civilian employees requiring entry into the IRP.

(2) Forward request for a check of arrest and criminal history records to DLE concerning civilian personnel nominated for the IRP.

(3) Process and forward clearance requests to the Directorate of Security for civilian personnel requiring a security clearance under the IRP.

(4) Assist the DLE and the SJA Labor Counselor in processing civilian personnel disqualified from the IRP.

n. Coordinating Instructions.

(1) Security Clearance. Security Clearances are not required for entry into the IRP. Personnel whose duties will afford them access to classified Category I/II AA&E will have the required security clearance. The security clearance files checks conducted at the POM Complex for granting a clearance may be used in lieu of the local files checks requirements above. Personnel with a current security clearance are exempt from the files check procedure, but must be interviewed by the Commander concerned. A record of the interview must be kept.

Local files checks on officers, warrant officers and DA civilians (GS-09 and above), nominated for entry into the IRP, are not required, Commanders will designate the officers whose duties require unaccompanied access to AA&E/storage facilities. The designated officer will be thoroughly familiar with the procedures for the control, accountability and safeguarding of AA&E, IAW, AR 190-l1, AR 190-51 and this SOP.

(2) Documentation. Units/organizations will maintain the following documents concerning personnel afforded unsupervised, unaccompanied access to AA&E/storage facilities.

(a) Unaccompanied Access Roster. A locally produced roster will list all unit/organization IRP personnel. The roster will include the individual's name, rank, duty position, and the date local files checks were completed. Officers designated for unaccompanied access will also be listed.

(b) Commander's assessment and local files check (see Appendix F, of this SOP for a form). Copies of the Request for Local Files Check will be maintained in the individual's unit/organization file, either company or higher level. The document will reflect the date the individual was entered into the IRP. Local files checks used for the IRP are valid for three years. After three years the process will be repeated, if required.

(c) Derogatory Information. Derogatory information discovered during the evaluation process will be reported to the DSEC. Such information will be maintained in the individual's organization file. Commanders and supervisors of civilian personnel can adjudicate derogatory information affecting suitability for entry into the IRP.

(d) A DA Form 7281-R, (Security Screening and Evaluation Record), will be used for Army employees and contract personnel. The original DA Form 7281-R will be filed in the individual's official personnel folder. One copy will be retained in the files of the certifying official, the medical facility servicing the individual's medical record and the employee. All personnel listed on the DA Form 1687,(See Appendix F of this SOP for a sample of the form), submitted to the ASP in Ft Hunter Liggett will be IRP certified.

(3) Evaluation Process. The evaluation process of personnel performing duties under the IRP is continuous. Questionable activity on the part of personnel having unaccompanied access to AA&E will be reviewed by the commander. Commanders/supervisors of civilian personnel will determine if retention in the IRP is warranted. The following are examples of disqualifying factors.

(a) Drug and/or alcohol abuse.

(b) Mental instability or disorders.

(c) Judicial or non judicial punishment.

(d) Behavior or actions showing contempt for the law.

(e) Any other conduct which the commander determines raises questions about an individual's reliability or trustworthiness.

19. GENERAL PROVISIONS.

a. Computer and business machine security.

(1) Desk top computers, calculators, typewriters and similar machines are desirable objects and are highly susceptible to theft. Every effort will be made to ensure adequate security for such items.

(2) All such items will be accepted on hand receipt by a responsible person within each office or activity. Frequent serial number inventories (not less than quarterly) should be conducted for those items that are physically located in storage or in buildings or activities. Operating personnel should conduct visual inventories daily. Consideration should be given to marking all items as U.S Property, for easy identification in case of theft and caution should be exercised to ensure electrostatic engravers are not used, since they might damage sensitive micro-components of the computer.

(3) The buildings in which such items are stored, or used, will have adequate doors, windows and locks. (See Basic Structure Checklist; and, Administrative and Housekeeping Supplies and Equipment Checklist, Appendix A, of this Physical Security SOP). If located in rooms with lockable doors, the doors will be closed and locked at the close of business. If structure doors and windows do not meet minimum standards, and lockable office doors do not exist, computers, disk drives, printers, high value typewriters, and other similar machines, will be secured in containers (locally fabricated or commercially purchased). In lieu of containers, anchor pads or similar devices will be used to secure the machines in place to prevent theft. Cable security devices will only be used on low value typewriters, such as manual machines, calculators; and, computer peripherals such as modems and key boards.

See Appendix D, of this Physical Security SOP for examples of locking devices for office machines.

b. Organizational clothing, equipment, and personal property belonging to soldiers who are AWOL/Deserter from the unit will be collected and inventoried by unit officers or NCOs designated by the Unit Commander. Organizational/government items will be inventoried against the individual property/clothing records. Personal property will be inventoried by item, quantity, dexcription and serial number (if any), and, recorded on a blank sheet of paper or other format if desired. All items will be secured in a locked bag, wall locker, or similar container, that is further secured in the unit supply or storage room designated for such items. The inventory record will be signed by the person conducting the inventory. One copy of the inventory will be kept in the individual clothing record file and one copy will be placed in the bag containing the individuals property.

(1) Access to the locked container/storage area will be strictly controlled.

(2) Keys to containers will be secured by the unit key custodian in a sealed envelope in such a manner that tampering will be easily detected.

(3) The sealed envelope will be secured in an approved key depository/file. The envelope will be opened only if an emergency exists to conduct inventories or, upon return of the owner.

(4) Monthly, the property containers will be inspected (when key inventories are conducted) for damage or tampering. Periodic physical inventories may be conducted if the Unit Commander deems it necessary.

(5) SF Form 702 will be posted on containers or storage area doors to indicate access times and dates. This form will be retained in unit files for 90 days upon completion. (See Appendix F, of this SOP for a sample of the form).

c. Personal property belonging to individuals on Leave/TDY, will be secured in a locker or cabinet, in a locked room.

d. Unit Mail Rooms will be secured in the following manner:

(1) Structural and perimeter barriers will meet the standards outlined in Paragraph 6 of this SOP.

(2) Key control will follow standards outlined in Para 7 of this SOP.

(3) Security checks, wherever possible, will be conducted as outlined in Paragraph 8, of this SOP.

(4) Access control will be established and be limited to unit mail personnel and the Commander only.

(5) Signs will be posted on entrances to designate authorized entry only. SF Form 702 will be posted on the outside of all safes/containers, containing certified or classified mail; and, on the outside of the entrance door.

(6) Classified mail will be secured in accordance with AR 380-5.

(7) Certified and Registered Mail, as well as payroll checks, stamps, indicia or other similar items, will as a minimum, be secured in a field safe or similar container that is provided with a built-in combination lock or, that can be secured by an approved hasp and combination padlock. Safes or containers weighing less than 750 pounds will secured to the structure, wall or floor.

e. In those cases where specific items have not been identified in this regulation, i.e., medical items, etc., commanders will use AR 190-51 as the immediate guide for determining security measures. If in doubt, coordination should be made with the DLE Physical Security Branch for a determination of standards.

f. Commanders/supervisors will initiate investigations whenever reported losses occur, are suspected; or whenever a storage area is subjected to actual or-attempted break-in. The provisions of AR 735-5 (Property Accounting) will be used for other property losses; or as otherwise directed by the Installation Commander.

The proponent of this Standard Operating Procedure is the Directorate of Law Enforcement. Users are invited to send comments or suggested changes to Installation Commander, DLIFLC & POM, ATTN: ATZP-DLE, Monterey CA 93944.

GLOSSARY

ABBREVIATIONS

AA&E	ARMS, AMMUNITION AND EXPLOSIVES
AAFES	ARMY, AIR FORCE EXCHANGE SERVICE
ASP	AMMUNITION SUPPLY POINT
BPA	BLANKET PURCHASE AUTHORITY
BSO	BOMB SCENE OFFICERS
CCTV	CLOSED CIRCUIT TELEVISION
CID	CRIMINAL INVESTIGATION DIVISION
CPO	CIVILIAN PERSONNEL OFFICE
CQ	CHARGE OF QUARTERS
CSDP	COMMAND SUPPLY DISCIPLINE PROGRAM
DA	DEPARTMENT OF THE ARMY
DOC	DIRECTORATE OF CONTRACTING
DOD	DEPARTMENT OF DEFENSE
DLE	DIRECTORATE OF LAW ENFORCEMENT
DOL	DIRECTORATE OF LOGISTICS
DPW	DIRECTORATE OF PUBLIC WORKS
DRM	DIRECTORATE OF RESOURCE MANAGEMENT
DSEC	DIRECTORATE OF SECURITY
EOD	EXPLOSIVE ORDNANCE DISPOSAL
GSA	GENERAL SERVICES ADMINISTRATION
IAW	IN ACCORDANCE WITH
IDS	INTRUSION DETECTION SYSTEM
IG	INSPECTOR GENERAL
IRP `	INDIVIDUAL RELIABILITY PROGRAM
MEVA	MISSION ESSENTIAL/VULNERABLE AREA
NAF	NON-APPROPRIATED FUND

NCO	**NON-COMMISSIONED OFFICER**
POMA	**PRESIDIO OF MONTEREY ANNEX**
POM	**PRESIDIO OF MONTEREY**
PSI	**PHYSICAL SECURITY INSPECTION**
PS	**PHYSICAL SECURITY**
PSS	**PHYSICAL SECURITY SURVEYS**
SDNCO	**STAFF DUTY NON-COMMISSIONED OFFICER**
SDO	**STAFF DUTY OFFICER**
SJA	**STAFF JUDGE ADVOCATE**
SOP	**STANDARD OPERATING PROCEDURE**
UCMJ	**UNIFORM CODE OF MILITARY JSUTICE**
UL	**UNDERWRITER'S LABORATORY**
US	**UNITED STATES**

APPENDIX A

PHYSICAL SECURITY CHECKLIST

1. PURPOSE. To provide unit/activity security managers a quick reference tool for self-inspection. All possible questions pertaining to subject areas are not contained in these checklists. The questions provide a basic starting point for determining the existence of adequate security measures.

2. REFERENCES. See individual checklists.

3. APPLICABILITY. The questions contained in these checklists indicate minimum standards for areas being inspected. Risk analysis procedures contained in DA Pam 190-51 have already been applied and incorporated into these checklists. If not all inclusive, or if the threat changes, the provisions of AR 190-51 will be reapplied.

4. PROCEDURE. Checklists are marked with "Yes","No" and "Not Applicable (N/A)" response areas. "Yes" indicates the existence of the required security standard. "No" indicates that the standard does not exist or is not in compliance. Immediate corrective action should be initiated to bring the response back to the "Yes","No" column. "N/A" indicates that the standard is not used or necessary at this activity.

5. TABLE OF CONTENTS (CHECKLISTS).

6. Individual checklists may be reproduced, as needed, on office copiers.

CHECKLIST FOR BASIC STRUCTURE

AR 190-51
FM 19-30

	YES	NO	N/A
1. EXTERIOR DOORS			
a. Do the doors provide a comparable degree of security as that provided by the structure?	___	___	___
b. Are windows in doors protected by metal screens (10 gauge wire mesh or expanded metal- or 9-gauge chain link on heavy frames or, are they covered/sealed over 1/2" plywood)?	___	___	___
c. Are screens and covers secured to the structure by means of carriage bolts with the interior ends peened to prevent removal?	___	___	___
d. Has one door been designed as the "lock-up" door (first in, last out)?	___	___	___
e. Are lockup doors solid core - 1 3/4", or reinforced with 1/2" plywood or 16 gauge sheet metal?	___	___	___
f. Are all doors securely locked in an approved manner?	___	___	___
(1) Mortised anti-friction latch with l" throw dead bolt (ANSI A156.13).	___	___	___
(2) Pin tumbler key-in-knob, supplemented by a l" throw deadbolt.	___	___	___
(3) Single cylinder, jimmy proof, rim lock, or laminated swing bolts (aluminum Framed glass doors)?	___	___	___
(4) Five pin tumbler case hardened steel padlock (series 200/5200) used in conjunction with a heavy duty steel hasp.	___	___	___
(5) Steel locking bars, cane bolts, dead bolts, or panic hardware with extension bolts top and bottom.	___	___	___
(6) Other less secure method?	___	___	___

	YES	NO	N/A
g. Are door bucks, frames and keepers rigidly anchored and in good condition?	___	___	___
h. Are hinges firmly anchored?	___	___	___
i. Are hinge pins protected against removal (spot welded, peened, bradded or pinned)?	___	___	___
j. Are gaps between double doors, or doors and frames, covered or protected by an astragal to prevent attack upon, or manipulation of the lock or latch?	___	___	___
k. Are all doors secured on the interior side (with the exception of the lock-up door)?	___	___	___
l. Are fire exits and fire doors properly secured to aid easy exit?	___	___	___
m. Are double cylinder locks prohibited?	___	___	___
n. Are roll-up doors/windows secured on the interior side by approved locking devices?	___	___	___
o. Are sliding doors properly secured by locks or bottom rail bars?	___	___	___
p. Are sliding doors secured in such a manner that they cannot be lifted out of the track?	___	___	___
2. INTERIOR DOORS			
a. Are the doors in serviceable condition?	___	___	___
b. Are adequate locks used?	___	___	___
(1) Key-in-knob or other type?	___	___	___
(2) Padlock (Series 200/5200) with hasp?	___	___	___
3. WINDOWS			
a. Are windows in serviceable condition?	___	___	___
b. Are accessible windows secured/locked?	___	___	___
(1) Key operated sash lock?	___	___	___

	YES	NO	N/A
(2) Covered by screens?	___	___	___
(3) Padlocks and hasps?	___	___	___
(4) Sealed, covered by plywood or nailed shut?	___	___	___
(5) Other less secure methods?	___	___	___
c. Are sliding windows secured in such a manner that they cannot be lifted out of the track and be removed?	___	___	___
4. OTHER OPENINGS			
a. Are all vents, openings or trap doors (in excess of 96 square inches) secured on the interior side in an approved manner; or, otherwise secured to prevent access?	___	___	___
b. Are air conditioning units or ducts secured to the structure to prevent removal; or, have modifications been made to prevent access, such as, interior screens or bars?	___	___	___
c. Are outside boiler rooms or closets, which have adjacent walls, secured or reinforced to prevent access, such as, interior screens or bars?	___	___	___
d. Are ceiling or floor crawl spaces blocked to prevent access from that point?	___	___	___
5. INTERIOR WALLS			
a. Do interior office/room walls reach to the ceiling or floor above?	___	___	___
b. Are false or suspended ceilings through, which access may be gained to adjacent rooms, secured to prevent access?	___	___	___
6. FLOORS			
Do floors provide equivalent security to that provided by walls and ceiling of the basic structure?	___	___	___

CHECKLIST FOR ADMINISTRATIVE KEY CONTROL

AR 190-13
AR 190-51

	YES	NO	N/A
1. Does the unit/activity have a key control SOP?	___	___	___
2. Has the unit activity/ commander/directorate appointed a key and lock custodian and alternate(s) in writing?	___	___	___
3. Are keys issued and received only by key custodians and alternates or, by Charge of Quarters (CQ) and staff duty officer/NCOs (SDO/NCO) as authorized by the unit commander?	___	___	___
4. Is the number of personnel authorized to use keys limited to those persons who have absolute need?	___	___	___
5. Are such persons designated by the commander/ directorate in writing, which indicates the key and area they are authorized access to?	___	___	___
6. Is the access list utilized by the custodian when issuing keys?	___	___	___
7. Is it prohibited to issue keys for personal retention (with the exception of those for personal quarters, troop billets, or where a mission dictates)?.	___	___	___
8. When not in use, are keys secured on the person of the individual to whom assigned or secured in a lockable container, such as a safe, filing cabinet or a depository made of at least 26-gauge steel that is equipped with a pin tumbler-type (preferably 5-pin) locking device or combination padlock (S&G 8077A), and securely affixed to the wall or structure to prevent easy removal?	___	___	___
9. Is the key depository 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?	___	___	___
10. Are all keys in the system strictly controlled?	___	___	___

	YES	NO	N/A
11. Is a complete written inventory of all keys by serial number, location of locks and total number of keys for each maintained on a Key Control Register And Inventory (DA Form 5513-R?	___	___	___
12. Is the Key Control Register Inventory retained in the unit files permanently, unless significant changes occur in the key inventories?	___	___	___
13. Are personally retained keys returned to the key custodian monthly for a "show inventory"?	___	___	___
14. Is a monthly visual inventory count of all keys in the system conducted by the custodian/alternate, and recorded on DA Form 5513-R (Monthly Key Control Register And Inventory?	___	___	___
15. Is the DA Form 5513-R retained in unit files for one year after completion?	___	___	___
16. Are changes in inventory counts recorded on DA Form 5513-R?	___	___	___
17. Are all keys in the system inventoried by serial number semiannually?	___	___	___
18. Are serial number inventories recorded on DA Form 5513-R?	___	___	___
19. Is a closing visual inventory count of primary keys (operational or daily use keys) conducted at the end of each duty day or shift?	___	___	___
20. Are key issued and turn in logs, that are kept open on a 24-hour basis, closed at 2400 hours each day?	___	___	___
21. Is a 100% visual count of primary keys in the depository conducted at the opening of each duty day, prior to issuing keys and the count compared to the last closing inventory shown on DA Form 5513-R?	___	___	___
22. Are keys, that are issued for daily use, signed out/in on DA Form 5513-R?	___	___	___
23. Are all entries made in ink?	___	___	___

	YES	NO	N/A
24. Are sign in/out logs used until completely filled?	___	___	___
25. Are completed logs maintained on file (inactive) for one year before being destroyed?	___	___	___
26. Are keys, that are issued for use beyond normal daily periods, issued on a hand receipt, or signed out individually on a separate DA Form 5513-R from the key custodian?	___	___	___
27. Are duplicate keys secured in a sealed envelope and secure container in the unit or at the next higher headquarters?	___	___	___
28. Are duplicate keys inventoried and accounted for by the key custodian/alternate on a monthly and semi-annual basis in the same manner as the primary keys?	___	___	___
29. Are control documents (Key Control Register, hand receipts, logs, registers and inventories) secured in the key container or a central file under the control of the key custodian?	___	___	___
30. Are master keys or keyed alike locks prohibited from use on supply rooms, motor pools, tool rooms and similar property rooms?	___	___	___
31. Are CQ personnel prohibited from possessing master keys for property rooms and areas other than individual living spaces?	___	___	___
32. Are all administrative keys secured in a separate depository from sensitive and JSIIDS keys?	___	___	___

CHECKLIST FOR ADMINISTRATIVE AND HOUSEKEEPING SUPPLIES AND EQUIPMENT

AR 190-51 AR 210-6 AR 230-1 AR 230-65 AR 380-19 AR 710-2 AR 735-5 DA PAM 710-2-1

	YES	NO	N/A
1. Are work buildings and rooms, in which office machines and property are located, secured whenever an individual assigned to the activity is not present?	___	___	___
2. Is furniture in day rooms or similar common areas used mainly during non-duty hours protected by controlling access to these areas to the greatest extent possible?	___	___	___
3. Does the Charge of Quarters, duty officer, NCD, or other designated individual periodically check offices and property areas after duty hours?	___	___	___
4. When size and weight allow, are small office machines (hand held calculators, typewriters locked in a desk or cabinet; and, further secured in a locked room of a secured building?	___	___	___
5. Are expendable and consumable supplies at unit and office levels, centrally stored in secure cabinets, containers, rooms, or buildings when not issued for actual use?	___	___	___
6. Are keys and access to storage facilities controlled?	___	___	___
7. Are desk top computers secured in buildings or structures meeting requirements of Appendix B, AR 190-51?	___	___	___
8. Are computers accounted for on inventory documents and assigned by hand receipt?	___	___	___
9. Are computers and companion equipment secured after duty hours in a locked room of a properly locked building?	___	___	___
10. If a securely locked building and room is not provided, are computers secured in locked cabinets or secured by anchor devices in an approved manner?	___	___	___
11. Does the hand receipt holder for computers and ADF equipment conduct frequent (not less than quarterly) serial number inventories of the property?	___	___	___
12. Are computers marked as U.S property?			

ORGANIZATION CLOTHING AND INDIVIDUAL EQUIPMENT NOT STORED AT CENTRAL ISSUE FACILITIES

AR 190-51
AR 735-5
AR 710-2
DA PAM 710-2-1

	YES	NO	N/A
1. Is issued clothing marked per AR 700-84?	___	___	___
2. Is individual clothing and equipment of personnel living in troop billets secured in a locked container or in a locked room, or supply room?	___	___	___
3. Does the responsible commander prohibit soldiers from storing individual field equipment in POVs?	___	___	___

CHECKLIST FOR FACILITY ENGINEERING SUPPLY AND CONSTRUCTION MATERIAL STORAGE AREAS

AR 190-51
AR 420-17
AR 735-5

	YES	NO	N/A
1. Do buildings storing supply and portable construction material meet the structural standards IAW AR 190-51?	___	___	___
2. Are outside storage areas enclosed by a perimeter fence?	___	___	___
3. Does the fence meet the standards of an FE-6 fence?	___	___	___
4. Are points of issue for supplies and construction material kept to a minimum?	___	___	___
5. Are "Off Limits to Unauthorized Personnel" signs posted at the facility entrances?	___	___	___
6. Is access to the facility and to keys and padlocks controlled?	___	___	___
7. Are supplies issued only to authorized personnel for whom signature authorization cards (DA 1687) are on file?	___	___	___
8. Are incoming shipments of supplies checked upon receipt?	___	___	___
9. Are work orders reviewed to determine if the recipient has requested excessive supplies for the job to be done?	___	___	___
10. Is the entry of privately owned vehicles into the storage building or outside storage areas prohibited?	___	___	___
11. Are personal packages in the storage areas prohibited?	___	___	___

CHECKLIST FOR AUDIOVISUAL EQUIPMENT AND TRAINING DEVICES AT TRAINING AND AUDIOVISUAL CENTERS

AR 190-51
AR 25-1
AR 735-11
DA PAM 710-2-1

	YES	NO	N/A
1. Is the equipment secured in a separate building or room under security standards as stated in Appendix B, AR 190-51?	___	___	___
2. Are audiovisual equipment and portable, high-value training aids seperated from other equipment and stored in a secure seperate container, room or building?	___	___	___
3. Are "Off Limits to Unauthorized Personnel signs posted at facility entrances?	___	___	___
4. Is access to the facility and to keys and padlocks controlled?	___	___	___
5. Are audiovisual equipment and portable, high value training aids inventories per AR 710-2?	___	___	___
6. Is a copy of the inventory kept on file until the next inventory is conducted?	___	___	___
7. Is an inventory check-out point located next to the center exit to preclude personnel from remaining in the center when equipment has been checked out?	___	___	___
8. Is access to the equipment storage area limited to center personnel authorized to issue the equipment?	___	___	___
9. Does the center maintain separate property book accountability for all equipment?	___	___	___

CHECKLIST FOR HAND TOOLS, TOOL SETS AND KITS AND SHOP EQUIPMENT

AR 190-51
AR 710-2
AR 735-5
DA PAM 710-2-1

	YES	NO
1. Are tool sets and kits with lockable tool boxes secured with key-operated tumbler-type padlocks when not in use?	___	___
3. Are portable handtools, tool sets or kits and shop equipment stored in a secure location when not under the surveillance of a responsible person (user, tool room keeper or guard)?	___	___
4. Are non-portable items secured in the building or van in which they are located, with windows and doors that are lockable?	___	___
5. Are portable items secured by one of the following methods:		
a. A locked building or room meeting the requirements of AR 190-51, Appendix B, or a locked metal cage in a secure building?	___	___
b. A locked built-in cabinet, bin, or drawer in a secure room or building?	___	___
c. A locked drawer or compartment of a furniture item (wall-locker, desk, and so forth) in a secure room or building?	___	___
d. Attached to the building structure with a chain or cable and padlock, or permanently fastened to a working surface?	___	___
e. Locally fabricated, lockable racks, that when locked, prevent tool box lids from being opened or individually placed larger tools from being removed?	___	___
f. A locked, enclosed truck/van, armored vehicle, or vehicle trunk?	___	___

	YES	NO	N/A
g. A locked vehicle equipment box or secured, either directly or in a locked container, to the vehicle itself?	___	___	___
h. A locked CONEX container?	___	___	___
6. Are common tools and portable shop equipment, when not on hand receipt, or sub-hand receipt to a user, controlled through a locally devised receipt, sign-in/sign-out log, or exchangeable tag (CHIT) system?	___	___	___
7. Is access to tools and shop equipment controlled to the maximum extent possible?	___	___	___
8. Are hand tools with a nonmilitary application, that are particularly subject to pilferage, given special accountability?	___	___	___

A-13

CHECKLIST FOR COMMUNICATIONS AND ELECTRONICS EQUIPMENT AT INSTALLATION LEVEL

AR 190-51
AR 710-2
AR 735-5
DA PAM 710-2-1

	YES	NO	N/A
1. Are portable items provided double barrier protection, consisting of one or more of the following methods	___	___	___
a. A locked, separate building, enclosed van, trailer or armored vehicle protected by a perimeter fence?	___	___	___
b. A locked steel cage located in a secure building?	___	___	___
c. A locked built-in container (bin, drawer, cabinet) or a free standing locked container that is secured to the structure) and, within a secure building?	___	___	___

NOTE: The definition of Portable (Ref: AR 190-51) is capable of being carried in the hand or on the person. As a general rule, a single item weighing less than 100 pounds (45.34 kilograms) is considered portable.

2. Are non-portable items secured in a building with doors and windows locked during the hours the facility is non-operational?	___	___	___
3. Are particularly bulky or heavy items, that are stored outside, protected by a perimeter barrier (fence); lights, and checked after duty hours periodically?	___	___	___
4. Are "Off Limits to Unauthorized Personnel" signs posted on the activity entrance?	___	___	___
5. Are portable, pilferage-coded items separated from other equipment and stored in a separate room, area, or container with controlled access?	___	___	___
6. Is the activity lighted during the hours of darkness IAW FM 19-30?	___	___	___
7. Is access to the maintenance activity, and keys and padlocks protecting assets, controlled?	___	___	___

	YES	NO	N/A
8. Are privately owned vehicles prohibited to park within 50 feet of the storage facility entrances or loading dock?	___	___	___
9. Are periodic command directed inventories conducted per AR 710-2?	___	___	___
10. Are copies of the inventory kept on file until the next inventory is conducted?	___	___	___

CHECKLIST FOR SAFES AND FUND SECURITY

AR 37-103
AR 215-2
AR 380-5

	YES	NO	N/A
1. Is a Fund Custodian appointed in writing?			
2. Is there written authorization for the size of the fund?	___	___	___
3. Is the storage site structure adequate?	___	___	___
4. Are windows and doors adequately constructed and locked?	___	___	___
5. Is the room construction, in which the funds are secured, adequate, and is it properly locked?	___	___	___
6. Are the funds secured after duty hours in an approved safe/container?	___	___	___
7. Are adequate access and key control measures in effect?	___	___	___
8. Are cashier funds separated properly (drawers, cages, etc.)?	___	___	___
9. Is an IDS duress switch installed and functioning?	___	___	___
10. Is a full IDS installed and properly functioning?	___	___	___
11. Are cashiers prohibited from mingling funds; or from storing cash in containers securing classified material?	___	___	___
12. Are controls in effect to ensure no unauthorized funds are mingled with government funds?	___	___	___
13. Are cashiers prohibited from having personal purses and pocket books with them while they disburse funds?	___	___	___
14. Is there proper separation of duties which ensure cashiers and custodians (the same person) does not issue, account for, disburse and handle funds?	___	___	___
15. Are funds in excess of $200, that are secured on an overnight basis, secured in a tool resistance safe?	___	___	___

	YES	NO	N/A
16. When Class three through six security containers are used, is the overnight fund storage amount limited to $3,000?	___	___	___
17. Has the activity ensured that it has not purchased or uses a safe/container that is more costly than the amount of funds that are secure within?	___	___	___
18. Does the activity ensure that padlocks are not used to secure safes/containers after duty hours, in lieu of built-in dial combination locks?	___	___	___
19. Are safes/containers, weighing less than 750 pounds, secured to the structure in an approved manner?	___	___	___
20. Are funds, negotiable instruments, and blank checks/ bonds properly secured during duty hours to ensure against pilferage?	___	___	___
21. Have the structural standards of the storage site been reviewed by DLE and approved?	___	___	___
22. Has a Physical Security Inspection been conducted on the storage site within the last l8 months?	___	___	___
23. Are signature stamps, dies, validating stamps or indicia properly secured?	___	___	___
24. Has a cash verification check been conducted?	___	___	___

CHECKLIST FOR SECURITY OF EQUIPMENT/PROPERTY OF SOLDIERS ON LEAVE, TDY, ETC.

AR 190-51
AR 700-84
AR 710-2

	YES	NO	N/A
1. Has the unit commander designated an officer or NCO to inventory all the equipment and property that is to be safeguarded?	___	___	___
2. Did the designated-person conduct a 100% inventory, and was the inventory recorded?	___	___	___
3. Did the inventory record show all items of property by type, quantity, description and/or serial number?	___	___	___
4. Did the owner get a copy of the inventory record?	___	___	___
5. Did the unit file its copy of the inventory record in the individual's clothing record file?	___	___	___
6. Were all items secured in a lockable container?	___	___	___
7. Is the lockable container secured in the supply room or other secure storage area?	___	___	___
8. Does the secure storage area have tight access/key control?	___	___	___
9. Are keys to item containers sealed in an envelope that is secured by the key custodian?	___	___	___
10. Is the sealed envelope secured in an approved container?	___	___	___
11. Is the sealed envelope inspected monthly during the key custodian key inventories?	___	___	___
12. Is SF Form 702 (Security Container Checklist) posted on the doors to the item container or the storage area?	___	___	___

APPENDIX G
SECURITY CONTAINERS/SAFES

1. REFERENCES.

a. US Navy Physical Security Equipment Manual, Jul 86, Naval Civil Engineering Laboratory, Fort Hueneme, California 93043

b. AR 215-2, Management and Operation of Army MWR Programs and NAFIs.

c. AR 37-103, Finance.

d. AR 380-5, DA Information Security Program.

2. BURGLARY-RESISTANCE SAFES.

a. Such safes provide moderate to high levels of protection against both surreptitious and forced entry techniques. Depending on the specific classification of the safe, the forced entry protection ranges from attacks with common handtools and portable electric-powered tools to attacks with heavy duty oxy fuel cutting torches and explosives. The lower classifications of burglary-resistant safes provide protection against forced entry mainly at the door and front face of the safe (example, TR or TL-15). The higher classifications of safes provide forced entry protection on all six sides (example, TRTL-15x6).

b. All safe classifications are furnished with Group two combination locks, burglary-resistant safes are tested by Underwriters Laboratories, Inc. (UL) to provide certain levels of protection. Table G-1 lists the different UL classifications of burglary-resistant safes and the level of protection provided. Burglary-resistant safes are suitable for the storage of unclassified but sensitive items, such as drugs, precious metals, funds and negotiable instruments. Certification and identification labels should be affixed to the inside of the safe to identify the level of protection. Only burglary-resistant safes will be ordered for use as funds containers.

3. SECURITY CONTAINERS.

a. Security files/containers are used for storage of classified and other sensitive material and equipment including documents, communications gear, weapons and ammunition, controlled substances etc. Security files/containers may be used to secure limited amounts of money if already in use, and approved fund containers are not available; or, are uneconomical to purchase. Funds may not be stored in safes/containers securing classified material without the written

approval of the DSEC, Six classes of security containers have been manufactured and are in use. Table G-3 lists the levels of protection provided by each class. Class 1, 2, 3, and 4 containers are no longer manufactured; however they are still authorized for use. Class 1 and Class 2 containers are the only GSA-approved security containers that are insulated. Neither of these containers is currently being produced. The Class 3 container was replaced on the Federal Supply Schedule by the uninsulated Class 6 container. The Class 4 container was replaced by the uninsulated Class 5 container.

b. There are two types of steel security files/containers: insulated and uninsulated. Insulated files provide protection from fire for the stored material therein. As mentioned in Para 3a above, Class 1 and Class 2 containers are the only GSA approved insulated containers. Uninsulated containers are available and come in a variety of sizes and shapes.

c. Approved containers are tasted by the General Services Administration (GSA) and have been certified to provide levels of protection against forced and surreptitious entry. A GSA-approved label is shown on page G-5, of this Appendix; and a sample UL Label is shown on page G-6.

d. Federal Specifications.

(1) AA-F-358F: Uninsulated file/containers.

(2) AA-F-363B: Uninsulated map and plan, weapons and security communications containers.

e. Non-GSA approved containers exist and are available in many shapes and sizes. Containers of this type may not be purchased for the storage and security of funds without approval by Directorate of Law Enforcement.

APPENDIX H
BOMB THREAT PROCEDURES

1. PURPOSE. To establish the policies and procedures to be used in the event of a bomb threat.

2. APPLICABILITY. The provisions of this policy are applicable to all military and civilian personnel assigned or attached to POM, and POM Annex Complex.

3. DEFINITION. A bomb threat is any message delivered by any means, warning or claiming the presence of one or more explosive or incendiary devices.

4. RESPONSIBILITIES.

a. Unit activities/commanders/directorate managers and supervisors will be directly involved in actions taken during bomb threats and will ensure that each member of the unit/activity is trained and aware of the actions to be taken in the event a bomb threat occurs. Unit activities/commanders/directorate managers have overall responsibility for all responses to threat activity in their area.

b. Each unit/activity will develop a supplemental SOP or include in current SOPs, information and procedures that address the particular circumstances and operational needs of the unit/activity should a bomb threat occur. Individual SOP guidance will include:

(1) The appointment and responsibilities of a unit Bomb Scene Officer (BSO).

(2) Notification procedures to be followed upon receipt of the bomb threat. (See paragraph 5).

(3) Procedures for evacuation.

(4) Criteria for evacuation of sensitive areas.

(5) Security during and after the evacuation.

(6) Pre designated assembly areas.

(7) Search procedures and designation of search team members.

(8) Establishment of the Emergency Coordination Point.

(9) Training of unit personnel, to include classes by EOD on the recognition of various bomb and devices.

(10) After action reporting procedures.

c. The DLE Physical Security Branch will provide guidance in the preparation of SOPs upon request.

d. In case of evacuation and/or detonation of a bomb, which may result in the compromise/destruction of classified/sensitive information or materials, notify the Directorate of Security (DSEC) at 242-5460. Properly cleared and qualified personnel from this office will respond to the site and assist in preventing loss or compromise of the classified items.

e. During duty hours, the unit/activity commander/director or their designated representative (chain of command) will take charge of threat sites in their areas and will act as Bomb Scene Officer (BSO). After duty hours, the Staff Duty Officer/Non-commissioned Officer (SDO) will respond to all bomb threat sites and will act as the BSO until the arrival of the unit/activity commander/directorate or designated member of the unit chain of command.

f. Bomb Scene Officers (BSO) will:

(1) Coordinate all operations and activities at the bomb threat site until termination of the threat. Coordination should be done from a central point easily accessible to responding emergency units.

(2) Gather and evaluate information from unit personnel and/or search teams at the site and pass this on to the emergency units as they arrive, i.e., Explosive Ordnance Disposal (EOD), Fire Department, ambulances, and the DLE Police.

(3) Coordinate with the arriving emergency units, particularly the police and, provide any information pertaining to the actual or suspected location of bombs or explosive devices.

(4) Designate unit personnel as search teams.

(5) Give final clearance for the building to be reoccupied after the and/or team search is complete.

g. The Unit/activity commander and directorate are responsible for the training of their personnel and the coordination of their respective responses to bomb threats and/or explosions.

h. The DLE Police will respond to all bomb threats as the initial investigating agency. They will cordon off the targeted area (which may be a building, street, floor or room of an activity), provide traffic control, maintain security around the targeted area, and coordinate with the BSO for any additional information concerning the bomb threat.

i. The DLE Police Desk will notify the Fire Department, ambulance, EOD CID and Command Group, whenever a bomb threat is received.

j. The Fire Department will be prepared to respond to the scene of each bomb threat in order to minimize damage should a detonation occur.

k. Ambulances/medical personnel will be prepared to respond to the scene of each bomb threat and administer emergency medical treatment in the event of a detonation.

l. EOD will receive the initial threat warning from the police desk, but will not normally respond unless an actual or suspected device is found.

m. Individual AAFES concessions will follow normal AAFES notification procedures and evacuate the premises. In the absence of a BSO, the responding police unit will maintain security in the area until the arrival of an AAFES BSO.

5. NOTIFICATION PROCEDURES:

a. Units/activities will maintain a current roster of phone numbers for all emergency services, i.e., police, fire, EOD, medical.

b. Any person receiving a bomb threat will:

(1) Immediately notify the chain of command and the DLE Police Desk. Individuals notifying the DLE Police Desk will include information as to whether or not a device has been found and whether or not evacuation of the targeted areas has been ordered/completed.

(2) If the threat is transmitted by letter or message, protect the letter or message from damage to preserve it as evidence.

(3) If the threat is by phone, use the Bomb Threat Checklist (see page F-8, of this Appendix) as a guide for gathering information about the caller and/or the explosive/incendiary device. This checklist will be available at all office and business phones within the unit/activity.

c. Should an explosive/incendiary device or suspected device be found, EOD will be immediately notified by the DLE Police.

6. EVACUATION PROCEDURES:

a. All units/activities (except as designated in paragraph 6.b below) will evacuate personnel from the area/facility in every case of bomb threat.

b. In activities not normally open to the public or into which unescorted public access cannot occur (i.e., SCIF), the unit BSO will (before evacuation) evaluate the threat and the criticality of the mission of the targeted activity/facility IAW criteria established

in the activity/facility SOP. If doubt exists as to the safety of personnel or if the presence of an actual bomb is suspected, based on the information available, evacuation will be ordered as a precautionary measure. The DLE police desk will be notified of the evacuation.

c. Some areas, for security reason, may require partial instead of total evacuation. Internal procedures will be devised to maintain communications with stay behind personnel (do not use radios, as their emissions may detonate explosive devices).

d. Announcements for evacuation will be made in a calm manner. The use of term "bomb" will be avoided in public areas. Public address systems, when used, will have a preprinted announcement available near the microphone.

e. Supervisors and key personnel will be trained to supplement the public address system by moving to prearranged positions to usher/direct people out of the area or around blocked exits and to give directions to pre designated assembly areas. These supervisors/key personnel should also be instructed to be alert for possible pilferage by evacuees.

f. Evacuated personnel will assemble at unit/activity command designated areas that are at safe or reasonable distance (approximately 300 feet) from the targeted area/facility, preferably away from parked cars, and trash bins. Supervisors will perform a head count of assembled workers and inform the BSO of missing or injured unit/activity personnel. Members of the public and crowds will be directed to disperse away from the area or to congregate at designated assembly areas.

g. When an "all clear" is given by the BSO, unit/activity personnel will enter the building by one entrance and will secure the facility before continuing normal operations. Supervisors should ensure emergency exits are closed and prepared for normal operations.

7. SEARCH PROCEDURES (See pages H-10 thru H-16, of this SOP).

a. Good housekeeping is essential should any search become necessary offices/areas that are "cluttered" will be difficult to search and provide fruitful ground for hidden bombs and devices.

b. Activity personnel should be aware of everything in their area. They must be suspicious of unknown items such as briefcases or packages.

c. When a threat occurs, personnel must:

(l) Make the proper notifications (chain of command or BSO).

(2) Quickly scan their immediate areas for suspicious items.

(3) Upon order of the BSO or the chain of of command, personnel will evacuate the area/facility in an orderly manner, scanning the area for suspicious items as they leave.

(4) If pre designated search teams are assigned, they will begin to search assigned areas prior to and as they evacuate the area/facility. The use of civilian employees in search teams will be limited to management and supervisory volunteers only.

(5) Except as provided in paragraph 4.m above, EOD, Fire and Police personnel will not be used in lieu of unit personnel as primary search teams.

d. Once evacuated, the area/facility will not be reentered without permission of the BSO or chain of command.

e. If any suspicious items are found:

(1) Ensure no one touches it except EOD personnel.

(2) Ascertain whether or not it belongs there (if possible).

(3) Close off the area and/or make notation of it. Report it to the BSO and/or the DLE Police. The DLE Police Desk will notify EOD of the presence and location of the suspected device.

8. PACKAGE/ENVELOPE BOMBS.

a. Supervisors should make their personnel aware of the possible characteristics of envelope/package bombs which should cause suspicion, i.e.:

(1) May bear restricted endorsements such as "personal" or "private."

(2) The addressee's name and/or title may be inaccurate.

(3) The package may reflect distorted handwriting or the name and address may be prepared with homemade labels or cut/paste lettering.

(4) The package may have protruding wires, aluminum foil or oil stains visible, and may have an unusual odor.

(5) Letter type bombs may feel rigid or appear uneven and lopsided.

(6) Parcel bombs may be unprofessionally wrapped with several combinations of tape used to secure the package.

(7) Parcel bombs may make a buzzing or ticking noise, or a sloshing sound.

b. If in doubt about the contents of a package or envelope, do not handle it any further. Do not submerge it in water. Notify a supervisor or BSO immediately. Keep the area around the object clear until EOD can inspect it.

BOMB THREAT CALL CHECKLIST

QUESTIONS TO ASK: **EXACT WORDING OF THE THREAT**

1. When is bomb going to explode? _____
2. Where is it right now? _____
3. What kind of bomb is it? _____
4. What does it look like? _____
5. What will cause it to explode? _____
6. Why? _____

Sex of Caller_____ Age _____ Race _____ Length of Call _____

CALLER'S VOICE:

___Calm	___Laughing	___Lisp	___Disguised
___Angry	___Crying	___Raspy	___Accent
___Excited	___Normal	___Deep	___Familiar
___Slow	___Distinct	___Ragged	___If voice is familiar,
___Rapid	___Slurred	___Clearing Throat	who did it sound like? _
___Soft	___Nasal	___Deep Breathing	_____
___Loud	___Stutter	___Cracking Voice	_____

BACKGROUND SOUNDS:

___Street Noises	___House Noises	___Factory Machinery	___Local
___Crockery	___Motor	___Animal Noises	___Long Distance
___Voices	___Office	___Clear	___Booth
___PA System	Machinery	___Static	Other _____
			_____

THREAT LANGUAGE:

___Well Spoken (Educated)	___Foul	___Incoherent	___Message read by threat maker
	___Irrational	___Taped	

REMARKS: _____
_____

CALL REPORTED TO SUPERVISOR (NAME): _____

NAME: _____ **DATE:** _____

POSITION: _____ **PHONE NUMBER:** _____

H-7

9. FACTORS THAT MUST BE CONSIDERED IN PLANNING AN EVACUATION OF A BUILDING:

a. In evacuating any building, people must be routed through the most public areas of the building, corridors and stairwells, and these are the areas that are most likely to contain an explosive or incendiary device. Search these areas before evacuation.

b. Routes of evacuation and priorities for a bomb threat . Routes and priorities established will be based on the type of building and the location of people within the building. Persons to act as guides to lead the evacuation and to control the personnel during exit must be pre designated and trained. It is recommended that the evacuation be conducted on an annual basis.

c. Routes of evacuation and priorities when a bomb is found. Routes and priorities established will also depend on the type of building and the location of people in relation to the area in which the bomb is located. In multistory buildings, rooms on floors above the danger point and immediately below should be evacuated first. Also, on the same floor, evacuate three rooms away on all sides.

d. Before giving the order to evacuate, the commander/director should consider the following:

(l) The Caller: What did he/she say? Did the caller sound serious in his threats?

(2) Has this been a recurring thing?

(3) Are employees excused from work when such threats are experienced?

(4) Is it possible that this call was precipitated by news reports of other calls?

(5) Will immediate evacuation of the premises expose personnel to greater danger?

(6) What is the size of the building: How many people are involved?

e. OTHER CONSIDERATIONS: Some of the questions that must be answered and provided for in preparing the Bomb Threat Plan are:

(1) Who has the authority to order evacuation? The commander/director or supervisor of the building concerned. (DLE Police do NOT order evacuation.)

(2) Who makes the decision to permit reentry into the building following a search in which no bomb is found? The Bomb Scene Officer who is in control of the operation. (DLE Police do NOT order reentry to a building.)

(3) How will evacuation be signaled? Establish a signal for evacuation and proceed according to the preestablished evacuation plan.

(4) If evacuation is ordered, what procedures will be followed? Evacuation teams should be designated to guide the occupants out of the area. Alternate evacuation routes must be provided, preferably the same routes used in case of fire.

(5) Who will be part of the evacuation team? These people should be designated before the incident and thoroughly trained. Areas through which evacuation will proceed should be searched and cleared before evacuation. These include areas inside and outside the threatened building. Public areas are the most likely places for a bomb to be located and are the usual avenues of exit. The evacuation team should be able to control the evacuation and eliminate panic that could lead to injuries.

(6) To what area do you evacuate the occupants? Occupants should be evacuated to an area at east 300 feet away from the threatened area. It must be emphasized that the 300 foot figure is a minimum. Greater distances are encouraged, if at all possible. In any case, evacuees should be instructed to take cover and shelter from possible fragmentation.

(7) What are the responsibilities of the occupants during evacuation? The occupants should open all doors and windows. This will reduce the shock effect of the bomb. Electrical units should be unplugged to reduce chance of detonation and to reduce noise for an audio check. Then they should proceed calmly, following the orders of the evacuation team.

10. Any information released to the public and/or media will be through the Public Affairs Office only.

11. AFTER ACTION REPORT: The BSO will prepare an After Action Report concerning any bomb threat or explosion. The report will be forwarded through the chain of command to the Garrison Commander, with a copy furnished to the Directorate of Law Enforcement, ATTN: Physical Security.

12. REFERENCES:

a. AR 525-13, Countering Terrorism

b. AR 190-13, Army Physical Security Program

c. AR 19-30, Physical Security

d. TC 19-5, Bomb Threat

e. FC 19-106, Bomb Threat